Strategia integrată de informatizare şi transformare digitală a Primăriei Municipiului Bistrița

Aprilie 2023

Conținut

STADIUl ACTUAL SUB ASPECTUL NEVOILOR DE DIGITALIZARE EXISTENTE LA NIVELUL PROCESELOR ADMINISTRATIEI PUBLICE LOCALE.

STADIUL ACTUAL AL DIGITALIZARII PRIN SERVICII ONLINE OFERITE CETATENILOR.

I. Nevoi existente in domeniul *Gestiunii si Mentenanței Datelor*

I.1 Nevoile de dotare suplimentară cu **echipamente/accesorii/tehnica de calcul/senzoristica/ solutii tehnologice inovative** aferente digitalizării **proceselor si subproceselor de *Gestiune si Mentenanță a Datelor*** din cadrul administratiei publice locale a Municipiului Bistrița

Nevoile exprimate de catre personalul reprezentant al domeniului se refera mai ales la următoarele echipamente considerate a fi necesare:

- creșterea capacității de stocare a Datastorage-urilor (echipamente de stocare date) din cadrul Centrului de date existent (achiziție hard diskuri pentru completare);
- echipamente de stocare electronică a datelor ca parte a unor procese automatizate pentru arhivarea electronică.

I.2 Nevoi de **digitalizare/informatizare/softuri** pentru domeniul proceselor şi subproceselor de ***Gestiune si Mentenanță a Datelor*** din cadrul administratiei publice locale a Municipiului Bistrița

Nevoile exprimate de catre personalul reprezentant al domeniului se refera mai ales la următoarele:

- nevoia implementarii soluției de server de fișiere;
- nevoia implementarii soluției de arhivare electronică (software arhivare electronică).

I.3 Nevoi organizatorice avute in vederea optimizarii **proceselor si subproceselor de *Gestiune si Mentenanță a Datelor*** din cadrul administratiei publice locale a Municipiului Bistrița

Nevoile exprimate de catre personalul reprezentant al domeniului se referă la următoarele:

- în primul rând: măsuri privind reorganizarea centrului de date existent;
- implementarea noului centru de date (soluție container) cu funcție de rezilienta datelor.

II. Proiecte aflate în derulare aferent nevoilor existente in domeniul *Gestiunii si Mentenanței Datelor*

II.1 **Proiecte de digitalizare/inovare/optimizare a proceselor si subproceselor de *Gestiune si Mentenanță a Datelor*** aflate in derulare:

- configurare server de fișiere pe soluție Windows Server 2019;
- creșterea automatizării proceselor de backup.

II.2 **Proiecte de digitalizare/inovare/optimizare a proceselor si subproceselor de *Gestiune si Mentenanță a Datelor*** necesare pentru a fi demarate (pe termen scurt, mediu si lung):

Pe termen scurt și mediu se consideră că sunt necesare următoarele:

- adoptare de soluții software noi
- upgrade asupra soluțiilor la interfețe web și integrarea softurilor existente.

Din ianuarie 2023 s-a demarat un upgrade al soluțiilor financiar-contabile la interfață web.

Pe termen lung: este necesară începerea proceselor de proceduralizare a arhivei electronice.

III. Nevoi existente în domeniul *Coordonare Serviciul relații publice, comunicare*

III.1 Nevoile de dotare suplimentară cu **echipamente/accesorii/ tehnica de calcul/senzoristica/solutii tehnologice inovative** aferente digitalizării **proceselor si subproceselor de *Coordonare Servicii Relații Publice, Informatică, Registratură Generală*** din cadrul administratiei publice locale a Municipiului Bistrița.

Nevoile exprimate de catre personalul reprezentant al domeniului se refera mai ales la următoarele echipamente/măsuri considerate a fi necesare în vederea digitalizării:

- schimbarea soluției de telefonie existente în soluție bazată pe IP;
- implementarea soluțiilor de scanare a documentelor și roboți software de interpretare a datelor scanate (automatizarea înregistrării documentelor);
- implementarea semnăturii electronice.

III.2 Nevoi de **digitalizare/informatizare/softuri** pentru domeniul proceselor şi subproceselor de ***Coordonare Servicii Relații Publice, Informatică, Registratură Generală*** din cadrul administratiei publice locale a Municipiului Bistrița

Nevoile exprimate de catre personalul reprezentant al domeniului se refera mai ales la următoarele:

- creșterea performanței și securității sistemului de poștă electronică;
- implementarea unei palete complete de servicii electronice pentru cetățeni.

III.3 Nevoi organizatorice avute in vederea optimizarii **proceselor si subproceselor de *Coordonare Servicii Relații Publice, Informatică, Registratură Generală*** din cadrul administratiei publice locale a Municipiului Bistrița

Nevoile exprimate de către personalul reprezentant al domeniului se referă la următoarele:

- actualizarea și modernizate procedurilor existente și crearea unora noi.

IV. Proiecte aflate în derulare aferent nevoilor existente in domeniul proceselor de *Coordonare Servicii Relații Publice, Informatică, Registratură Generală*

IV.1 Proiecte de digitalizare/inovare/optimizare a proceselor si subproceselor de *Coordonare Servicii Relații Publice, Informatică, Registratură Generală* aflate in derulare:

- *"Implementarea de proceduri simplificate pentru reducerea burocrației pentru cetățeni la nivelul ,umicipiului Bistrița în domenii de activități cu competență partajată asistență socială și urbanism", COD SIPOCA 1231 / MYSMIS 154519* în cadrul acestuia se vor implementa un număr de servicii electronice pentru cetățeni din domeniul asistenței sociale și urbanism.
- Achiziționarea a două totemuri (ecrane interactive) pentru afișarea informațiilor de importanță pentru cetățeni.

IV.2 Proiecte de digitalizare/inovare/optimizare a proceselor si subproceselor de *Coordonare Servicii Relații Publice, Informatică, Registratură Generală* necesare pentru a fi demarate (pe termen scurt, mediu şi lung):

Nevoile exprimate în acest sens de catre personalul reprezentant al domeniului se refera la următoarele:

- Proiecte menite a realiza creșterea gradului de integrare a aplicațiilor existente în vederea îmbunătățirii proceselor

- Proiecte focalizate pe crearea de noi servicii electronice pentru cetățeni, pentru a se asigura pe termen scurt si mediu o paleta completa a acestor servicii.

V. Situația actuală a serviciilor online/digitale pentru cetățeni

Prin implementarea proiectului "***Fundamentarea deciziilor și măsuri pentru simplificarea procedurilor administrative pentru cetățeni la nivelul UAT Municipiul Bistrița***" cod SIPOCA 687, s-au introdus soluții moderne de gestiune a serviciilor publice pentru cetățeni.

Platforma de servicii online pentru cetățeni este un sistem integrat complex care oferă utilizatorului o interacțiune facilă și directă cu Primăria Bistrița pentru toate serviciile online oferite de către municipalitate.

In stadiul actual al implementării, sunt disponibile următoarele servicii online:

1. Aplicație de plăți online de pe dispozitive mobile pentru impozite și taxe locale;
2. Aplicație informatică pentru eliberarea online de certificate de atestare fiscală;
3. Aplicație informatică pentru depunerea și consultarea online a declarațiilor pentru impozite și taxe locale;
4. Aplicație informatică de consultare online a "dosarului personal" cu documentele emise de autoritatea fiscală locală;
5. Aplicație informatică pentru depunerea online a petițiilor;
6. Aplicație informatică care permite consultarea/vizualizarea online a istoricului interacțiunii cetățeanului cu autoritatea locală;
7. Aplicație informatică de tip GIS pentru semnalarea online, de către cetățeni a defecțiunilor și altor avarii apărute la diversele dotări publice existente - IReport;
8. Aplicație informatică de tip GIS pentru informare online cu privire la diferite aspecte ale vieții publice – consultări, sondaje, chestionare publice;
9. Aplicație informatică pentru introducerea conceptului de "bugetare participativă".

În plus față de funcționalitățile prevăzute prin clauzele contractuale, s-au mai implementat şi următoarele servicii online suplimentare:

10. Plata online a impozitelor, taxelor și amenzilor;
11. Stadiul cererii depuse – consultare stare documente depuse la Primăria Bistrița;
12. Plată autorizații acces – plată online pentru obținere autorizații de acces în oraș, a mjloacelor de transport de tonaj greu;
13. Programări acte de identitate;
14. Programări pt radierererea/evidența mijloacelor de transport;
15. Urbanism – consultare documente de urbanism ;
16. Parcări online – consultare stare locuri de parcare de reședință din municipiul Bistrița
17. Colectare și epurare – registru evidență sisteme individuale de colectare și epurare.

Prin proiectul "*Implementarea de proceduri simplificate pentru reducerea birocrației pentru cetățeni la nivelul municipiului Bistrița în domenii de activitate cu competență partajată asistență socială și urbanism*", cod SIPOCA 1231, MySMIS 154519, se vor completa serviciile online cu următoarele 19 servicii:

A. **Servicii de depunerea online a cererilor de asistență socială – integrate cu aplicația utilizată de DAS, pentru** :

1. Depunere online a documentelor aferente obținerii ajutorului social, conform Legii nr. 416/2001 privind venitul minim garantat, cu modificările și completările ulterioare, Art. 10;
2. Depunere online a documentelor aferente obținerii alocației pentru susținerea familie, conform Legii nr. 277/2010 privind alocația pentru susținerea familiei, cu modificările și completările ulterioare, Art. 10;
3. Depunere online a documentelor aferente obținerii ajutorului pentru încălzirea locuinței, conform Legii nr.226/2021 privind stabilirea măsurilor de protecție socială pentru consumatorul vulnerabil de energie (OUG nr.70/2011 privind masurile de protecție socială în perioada sezonului rece, cu modificările și completările ulterior, Art. 16 – abrogată);
4. Depunere online a documentelor aferente obținerii stimulentelor educaționale (tichete de grădiniță), conform Legii nr. 248/2015 privind stimularea participării în învățământul preșcolar a copiilor provenind din familiile defavorizate;
5. Depunere online a documentelor aferente obținerii ajutorului de urgență / înmormântare, conform Legii nr. 416/2001 privind venitul minim garantat, cu modificările și completările ulterioare / H.C.L.;
6. Depunere online a documentelor aferente obținerii drepturilor lunare pentru persoanele cu handicap, conform Legii nr. 448/2006 privind protecția și promovarea drepturilor persoanelor cu handicap cu modificările și completările ulterioare, Art.39 și Art.42;
7. Depunere online a documentelor aferente obținerii alocației de stat pentru copii
8. Depunere online a documentelor aferente obținerii indemnizației pentru creștere copil
9. Depunere online a documentelor aferente acordării suplimentului pentru energie
10. Înscrierea online a copiilor la creșă
11. Vizualizare a fișei personale conținând istoricul serviciilor și beneficiilor sociale de care a beneficiat o persoană
12. Planificare a Anchetelor Sociale și notificarea electronică a persoanelor din gospodăria unde se va realiza ancheta.

B. **Servicii de depunere online a documentațiilor de urbanism – sistemul informatic utilizat pentru Urbanism, respectiv Circuitul Intern al Documentelor, pentru:**

1. Depunerea documentației pentru eliberarea certificatelor de urbanism și calculul, respectiv plata taxelor aferente eliberării certificatelor de urbanism
2. Depunerea documentației pentru prelungirea valaibilității certificatelor de urbanism
3. Înștiințarea începerii lucrărilor de construcție / desființare
4. Înștiințarea finalizării lucrărilor de construcție / desființare
5. Obținerea certificatelor de nomenclatură stradală
6. Publicarea on-line a listei Autorizațiilor de construire / desființare și listei certificatelor de urbanism emise
7. Informarea prin SMS a cetățenilor cu privire la documentele de Urbanism proprii.

VI. Stadiul actual al digitalizării proceselor din Administrația Publică a Municipiului Bistrița, prin prisma aplicațiilor informatice existente şi utilizate la ora actuală în departamentele/serviciile/compartimentele şi birourile Primăriei Municipiului Bistrița

Harta Proceselor Administrației Publice din Primia Municipiului Bistrița este ilustrată în Fig. 1, după cum urmează:

Tip de proces	Detaliere subprocese aferente procesului principal								
Procese de management	*Procese de programare*	*Procese de realizare a strategiilor*	*Procese de evaluare*						
	Departament: Serviciul Managementul Proiectelor & Serviciul Implementare Proiecte cu fonduri externe nerambursabile								
Procese pimare	***Dezvoltarea facilitatilor, oferirea de produse si servicii***	***Managementul si mentenanta spatiului public*** (*reparatii, mentenanta*)	***Taxe*** (*determinarea, impunerea, colectarea taxelor*)	***Operarea facilitatilor publice*** (*vanzare de produse si servicii culturale, sportive; inchirierea spatiilor si bunurilor publice; gestiunea cladirilor municipalitatii; vanzarea proprietatii publice imobiliare*)	***Mentinerea sigurantei publice si protejarea proprietatii publice*** (*monitorizare, detectia si evaluarea riscurilor, impunerea sanctiunilor*)	***Urmarirea efectelor livrarii serviciilor*** (*colectarea opiniilor cetatenilor, gestiunea plangerilor, medierea conflictelor sau apelurilor la o decizie, urmarirea proactiva a consecintelor actiunilor masurilor si serviciilor livrate*)			
	Departament: Direcția Asistență Socială	Departament: Serviciul Monumente Istorice & Direcția Admin. Piețe	Departament: Serviciul urmărire încasări	Departament: Direcția Patrimoniu	Departament: Serviciul Poliția Locală	Departament: Serviciul constatare şi impunere			
Procese suport	***Gestiunea si mentenanta datelor***	***Gestiunea documentelor si arhivelor***	***Resurse agricole***	***Realizarea platilor***	***Receptia serviciilor, lucrarilor, produselor***	***Gestiunea achizitiilor si contractarii***	***Alocarea resurselor umane***	***Coordonare servicii administrație publică***	***Coordonare servicii relații publice***
	Departament: Compartimentul Tehnologia Informației	Departament: Serviciul Juridic şi Evidența Documentelor	Departament: Compartimentul Registru Agricol	Departament: Compartimentul Buget şi Execuție Bugetară	Departament: Direcția Tehnică	Departament: Serviciul Achiziții Publice	Departament: Biroul Resurse Umane	Departament: Administrator Public Secretar General	Departament: Direcția Servicii Publice

Fig. 1 Harta Proceselor Administrației Publice din Primia Municipiului Bistrița

Aferent acestor procese, aplicatiile informatice si tehnologii digitale care sunt utilizate în prezent în cadrul Primăriei Mun. Bistrița sunt următoarele:

VI.1 Aplicatiile informatice si tehnologiile digitale care sunt utilizate aferent *Proceselor Suport* de *Gestiune si Mentenanta Datelor* din cadrul departamentelor/ serviciilor/compartimentelor Primariei Bistrita si a Serviciilor Subordonate - *Poliția Locală – str.Piața Centrală nr.2*

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departa mente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabi litate (3)	Istoric (4)	Mentenanta asigurata (Da/ Nu)	BD la care este conectat sistemul/ aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
1	CID – circuitul intern al documentelor	Toate compartimentele care sunt în lan-ul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2, L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Tărpiului nr.2,	L	Apache / PHP / MySQL	Pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal cetățeni	2017		CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.	..\5.Caiete de sarcini\Caiet sarcini CID.doc	..\4.Manuale de utilizare\CID manual de utilizare.pdf
2	Lexexpert – aplicație de legislație	Toate compartimentele	L		Pe server propriu în centrul de date PMB	Indeco Soft Baia Mare		1995					

3	Portal PMB – www.primariabistrita.ro	Toate compartimentele și Cetățenii	L	Apache / PHP / MySQL / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu următoarele module: CID, ImpoTax, Urbanism	2020		Portal, Impozite-Bistrita, CID	Asigură servicii electronice către cetățeni asigurând digitalizarea completă a procesului de la cetățean la inspectorul care prelucrează solicitarea în aplicația din backend sau procese complet automatizate fără a mai fi nevoie de un inspector (eliberarea certificatelor de atestare fiscală)	..\5.Caiete de sarcini\Caiet de Sarcini portal 2020 POCA.pdf	..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf
4	Parcari – aplicatie online	Orice utilizator din rețea inclusiv Poliția locală/ Piața Centrală nr.2	L	Laravel (PHP), Vue.js, MySQL, PostgreSQL, MS SQL	Virtual Appliance (Server al institutiei)	GREEN OVEN SRL	GeCON	2015	Da	GeCON	Parcari – aplicatie online vizualizare si rezervare parcare rezidentiala – pe portalul PMB - https://parcari.primariabistrita.ro/		
5	Buget – modul care gestionează veniturile și cheltuielile și execuția bugetară.	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, Contab, Dars, GestBug, GeCon, MiFix, Invest, Acon, ResUm, CID	2006	Da	Buget_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea. Integrat cu sistemul eFactura.		..\4.Manuale de utilizare\Buget_2006-Manual de utilizare.pdf
6	Cassa – modul care înregistrează și urmărește operațiile de încasări sau plăți făcute prin casa	Birou contabilitate Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu modulul de Buget, Contab și ImpoTax	2006	Da	Cassa	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Cassa-Manual de utilizare.pdf
7	Contab – modulul este un instrument de urmărire și analiză a activității instituției prin gestiunea tuturor înregistrarilor contabile	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, ImpoTax, Contab, Dars, GestBug, GeCon, MiFix, Invest, ResUm	2006	Da	Contab_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Contab2006-Manual de utilizare.pdf

8	Dars – modul instrument pentru generare dări de seamă	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Dars_2006	Generează automat toate situațiile financiare pe baza datelor prelucrate în restul modulelor din pachetul financiar contabil		..\4.Manuale de utilizare\Dars2006-Manual de utilizare.pdf
9	eCubAdmin - centru de management unitar al tuturor modulelor care definesc produsul eCUB	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu toate modulele din pachetul financiar contabil	2006	Da	Nucleu	Gestionează utilizatorii și drepturile lor pentru modulele din pachetul financiar contabil. Asigură mecanismul de backup automat al bazelor de date într-o locație din rețea după un program configurabil.		
10	Gestbug – generează situații economice	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Gestbugue	Generează automat toate situațiile economice necesare gestionării materialelor și a obiectelor de inventar (intrări, ieșiri, inventare, etc)		
11	ListOP – listări ordine plată	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget	2006	Da	Nucleu	-		
12	MiFix – gestionează mijloacele fixe din direcție	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	MiFix	Generează automat toate situațiile economice necesare gestionării mijloacelor fixe. (intrări, ieșiri, inventare, reevaluare, etc)		..\4.Manuale de utilizare\MiFix-Manual de utilizare.pdf
14	ResUm – gestionează personalul din direcție, salarizarea	Birou contabilitate/ Poliția locală/ Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	ResUm	Gestionează resursele umane, asigură calculul salariului și generează raportările stabilite de legislație.		..\4.Manuale de utilizare\ResUm-manual de utilizare.pdf

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul
(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului
(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)
(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins
(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

VI.2 Aplicatiile informatice si tehnologii digitale care sunt utilizate aferent *Proceselor Suport* de *Gestiune si Mentenanta Datelor* din cadrul departamentelor/serviciilor/compartimentelor Primariei Bistrita - *Aparatul Primarului* - toate aplicațiile folosite în 2022

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
1	Acon – modul care asigură suportul informatic necesar procesului de atribuire a contractelor de achiziție publică	Serviciul achiziții/Gh.Șincai nr.2	L	Visual Fox Pro 9 / MSSQL 2014	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget și Investiții	2013	Da	Acon	Listare situații cu informații corelate din modulele de Buget și Investiții	..\5.Caiete de sarcini\Specificatii tehnice Acon.pdf	..\4.Manuale de utilizare\Acon-Manual de utilizare.pdf	
2	AgroRegis – aplicație de evidență a Registrului agricol	Compartiment registru agricol/Gh.Șincai nr.2	L	Microsoft Silverlight / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Circuit Intern al Documentelor și modulul de Impozite și Taxe Locale	2017	Da	Indb	Vizualizarea situațiilor comparative cu modulul ImpoTax și listarea tuturor documentelor necesare în activitatea cu contribuabilii.	..\5.Caiete de sarcini\Caiet de sarcini AgroRegis.pdf	..\4.Manuale de utilizare\AgroRegis - Manual de utilizare.pdf	
3	Buget – modul care gestionează veniturile și cheltuielile și execuția bugetară.	Compartiment buget și executare bugetară/Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, Contab, Dars, GestBug, GeCon, MiFix, Invest, Acon, ResUm, CID	2006	Da	Buget_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea. Integrat cu sistemul eFactura.		..\4.Manuale de utilizare\Buget_2006-Manual de utilizare.pdf	

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
4	Cassa – modul care înregistrează și urmărește operațiile de încasări sau plăți făcute prin casa	Direcția economică/Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu modulul de Buget, Contab și ImpoTax	2006	Da	Cassa	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Cassa-Manual de utilizare.pdf	
5	Contab – modulul este un instrument de urmărire și analiză a activității instituției prin gestiunea tuturor înregistrarilor contabile	Compartiment contabilitate/ Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, ImpoTax, Contab, Dars, GestBug, GeCon, MiFix, Invest, ResUm	2006	Da	Contab_ 2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Contab2006-Manual de utilizare.pdf	
6	Dars – modul instrument pentru generare dări de seamă	Direcția economică/Piața Centrală nr.6Die	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Dars_2006	Generează automat toate situațiile financiare pe baza datelor prelucrate în restul modulelor din pachetul financiar contabil		..\4.Manuale de utilizare\Dars2006-Manual de utilizare.pdf	
7	eCubAdmin - centru de management unitar al tuturor modulelor care definesc produsul eCUB	Compartiment tehnologia informației, Indeco Soft	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu toate modulele din pachetul financiar contabil	2006	Da	Nucleu	Gestionează utilizatorii și drepturile lor pentru modulele din pachetul financiar contabil. Asigură mecanismul de backup automat al bazelor de date într-o locație din rețea după un program			

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
8	Gestbug – generează situații economice	Compartiment buget și executare bugetară/Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Gestbug ue	Generează automat toate situațiile economice necesare gestionării materialelor și a obiectelor de inventar (intrări, ieșiri, inventare, etc)			
9	ListOP – listări ordine plată	Direcția economică/Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget	2006	Da	Nucleu	-			
10	MiFix – gestionează mijloacele fixe	Direcția economică/Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	MiFix	Generează automat toate situațiile economice necesare gestionării mijloacelor fixe. (intrări, ieșiri, inventare, reevaluare, etc)		..\4.Manuale de utilizare\MiFix-Manual de utilizare.pdf	
11	ResUm – gestionează personalul din instituție, salarizarea	Compartiment financiar salarizare și Biroul resurse umane/Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	ResUm	Gestionează resursele umane din instituție, asigură calculul salariului și generează raportările stabilite de legislație.		..\4.Manuale de utilizare\ResUm-manual de utilizare.pdf	
12	CID – circuitul intern al documentelor	Toate compartimentele care sunt în lan-ul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2,	L	Apache / PHP / MySQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal	2017	Da	CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea	..\5.Caiete de sarcini\Caiet sarcini CID.pdf	..\4.Manuale de utilizare\CID manual de utilizare.pdf	

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
		L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Tărpiului nr.2,					cetățeni				lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.			
13	Urbanism	Direcția Arhitect Șef - Piața Centrală nr.6	L	Apache / PHP / MySQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: CID și portal cetățeni	2017	Da	CID	Asigură gestiune registrelor de urbanism și publicarea lor automată în portalul cetățeni.	..\5.Caiete de sarcini\Caiet de sarcini_Urbanism.pdf	..\4.Manuale de utilizare\Urbanism manual de utilizare.pdf	
14	ImpoTax – evidență taxe și impozite	Direcția Venituri/Al. Odobescu nr.17	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Contab, Cassa, CID, AgroRegis, ghiseul.ro, GlobalPay, Portal cetățeni	2013	Da	Impozite -Bistrita	Gestionează automat următoarele procese: gestionează masa impozabilă la nivelul UAT, debitare (după formule și moduri de debitare stabilite de Codul Fiscal sau configurabile),	..\5.Caiete de sarcini\Caiet de sarcini Impotax.pdf	..\4.Manuale de utilizare\Impotax - ManualDeUtilizare.pdf	

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
											încasări și calcul automat de dobânzi după reguli stabilite de Codul fiscal sau configurabile pe fiecare tip de venit, asigură procesul de urmărire și executare silită			
15	Invest	Direcția Tehnică/Gh. Țincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Acon și Contab	2013	Da	Invest	Gestionează lista obiectivelor de investiții asigurând listarea situațiilor necesare corelând informațiile cu cele din Buget și Acon		..\4.Manuale de utilizare\Invest-Manual de utilizare.pdf	
16	Juris – evidență dosare	Serviciul juridic și evidență documente/Piața Centrală nr.2	L	- app server: node + js - client: js + react - baza de date: PostgreSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu: portal.just.ro	2017	Da	Indb	gestionează procesele/ cauzele din cadrul instituției.	..\5.Caiete de sarcini\Caiet de sarcini Juris.pdf	https://doc.juris.indecosoft.net/	
17	Stare civila – evidență registre căsătorii, nașteri, decese	Serviciul stare civilă/ Piața Centrală nr.2	L	Tehnologie web și platformă IBM Lotus Domino 7	pe server propriu in centrul de date PMB	Sobis Sibiu		2015?	Da		-			

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
18	LEX EXPERT – legislația Romîniei și a U.E., Jurisprudență, etc.	Utilizatorii din rețeaua locală de calculatoare a PMB	L	Delphi	Pe server propriu în centrul de date PMB	COMPANIA DE INFORMATICĂ NEAMȚ	Se pot exporta documente in orice editor Windows (Word, Excel etc.)	2001/2022	DA		Neaplicabil		..\4.Manuale de utilizare\Manual Lex.pdf	Mare
19	Portal PMB – www.primariabistrita.ro	Toate compartimentele PMB și Cetățeni	L	Apache / PHP / MySQL / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu următoarele module: CID, ImpoTax, Urbanism	2020	Da	Portal, Impozite-Bistrita, CID	Asigură servicii electronice către cetățeni asigurând digitalizarea completă a procesului de la cetățean la inspectorul care prelucrează solicitarea în aplicația din backend sau procese complet automatizate fără a mai fi nevoie de un inspector (eliberarea certificatelor de atestare fiscală)	..\5.Caiete de sarcini\Caiet de Sarcini portal 2020 POCA.pdf	..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf	
20	Parcari – aplicatie online	Direcția Patrimoniu/Gh. Șincai nr.2	L	Laravel (PHP), Vue.js, MySQL, PostgreSQL, MS SQL	Virtual Appliance (Serverul institutiei)	GREEN OVEN SRL	GeCON	2015	Da	GeCON	Parcari – aplicatie online vizualizare si rezervare parcare rezidentiala pe portalul PMB - https://parcari.primariabistrita.ro/	..\5.Caiete de sarcini\Specificatii parcari 2015.pdf		
21	WinDoc Deviz 5 – calcul devize de lucrări	Direcția tehnică/Gh.Șincai nr.2	L	Apache/ MySQL	pe mașină virtuală din centrul de date	Softmagazin Brașov		2010 2013	Nu	windoc	-		https://deviz.ro/ghid-devize.php	Este utilizat doar pt verificare devize

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
22	Taiden- aplicație de conferință și votare - Aplicația este folosită în cadrul ședințelor de Consiliu local (înregistrează vot, audio și video)	Sala de ședințe	L		Pe server fizic din sala de ședințe	Gerom Internațional București		2015	Da cu Loyal Center Bistrița		-			
23	Software ArcGIS desktop 10.5	Serviciul Cadastru/ Seviciul Urbanim/ Direcția Servicii Publice	L	MSSQL	Pe server propriu în centrul de date PMB	ESRI ROMANIA	Permite interogarea, editarea bazelor de date SISDIEBDU -GIS, baza de date Cadastru General, baza de date Sistem de centralizare al bazelor de date cadastru	2008-2017	Nu	SQL baza de date SISDIEBDU SQL baza de date Cadastru General SQL baza de date Sistem de centralizare al bazelor de date cadastru	Furnizare din bazele de date geospaţiale ale serviciului, a informaţiilor necesare pentru diverse proiecte derulate de Municipiul Bistrita, dar şi suport pentru serviciile din cadrul PMB sau alte instituţii (ex. Direcţia judeţeană de Statisticã)	_	_	Maxim
24	Software ArcGIS Sever Basic Enterprise	Compartimentul Tehnologia Informației	L	MSSQL	_	ESRI ROMANIA		2009	Nu	Nu este cazul	_			
25	Aplicație plug-in la ArcGIS, denumită ArcCadastru	Serviciul Cadastru	L	MSSQL	Conectare la baza de date SQL a	ESRI ROMANIA	Permite conexiunea la BD SISDIEBDU	2009	Nu	SQL baza de date SISDIEBDU	Gestionează baza de date SISDIEBDU Generare Fișa bunului Imobil			Maxim

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
					SISDIE BDU,stocată pe server propriu în centrul de date PMB Pe PC-urile/staţiile de lucru ale funcţionarilor din cadrul Serviciului Cadastru									
26	Aplicaţie plug-in la ArcGIS, denumită CadGenBIS	Serviciul Cadastru	L (kit instalare, cod sursă, certificat de calitate, certificat de garanţie, fişa tehnică)	MSSQL	Conectare la baza de date SQL a Cadastrului General, stocată pe server propriu în centrul de date PMB Pe PC-urile/staţiile de	IMPRUVEMENT TIME SRL	Permite, interogarea, introducerea de date, editatrea importul exportul fişiere CGXML, generarea de rapoarte-documente tehnice ale cadastrului Interoperabilitate cu software E-	2018-2022	Da	SQL baza de date Cadastru General	Gestionează baza de date a Cadastrului General Generare documente tehnice ale Cadastrului Generare fişierelor CGXML Importul de fişiere CGXML Editări multi-user, interogări, importuri/exporturi			Maxim

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
					lucru ale persoanelor cu atribuţii în acest sens din cadrul Serviciului Cadastru		Terra al Agenţiei Naţionale de Cadastru							
27	Aplicaţie plug-in la ArcGIS, denumită CadVeGIS	Serviciul Cadastru	L (kit instalare, cod sursă, certificat de calitate, certificat de garanţie, fişa tehnică)	MSSQL	Conectare la baza de date SQL a Sistemului de centralizare al bazelor de date cadastru, stocată pe server propriu în cen-trul de date PMB Pe PC-urile/staţiile de lucru ale funcţionarilor din cadrul Serviciului	IMPROVEMENT TIME SRL	Permite, interogarea, introducerea de date, editatrea importul exportul fişiere SHP, DXF, DWG, generarea de rapoarte-Fişe specifice Registrului Local al Spaţiilor verzi (Fişa spaţiului verde, Fişă arbore, Fişă teren degradat) -Fişe cămine edilitare (apă, canalizare, electricitate, gaz, Hidrant)	2018-2022	Da	SQL baza de date Sistem de centralizare al bazelor de date cadastru	Gestionează baza de date a Sistemului de centralizare al bazelor de date cadastru Generarea de rapoarte -Fişe specifice Registrului Local al Spaţiilor verzi (Fişa spaţiului verde, Fişă arbore, Fişă teren degradat) -Fişe cămine edilitare (apă, canalizare, electricitate, gaz, Hidrant) Editări multi-user, interogări, importuri/exporturi			Maxim

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
					Cadastru		Interoperabilitate cu alte baze de date GIS							
28	Soft antivirus ESET Endpoint Security – protejare stații și servere	Instalat pe toate stațiile	L					2009	Nu		-			
29	Eset Security Management Center - soft pt managementul centralizat al stațiilor	Compartimentul tehnologia informției	L	Tehnologie web/MS SQL	Pe server propriu in centrul de date PMB (mașină virtuală)	ESET Romînia		2015	Nu		-			

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul

(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului

(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)

(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins

(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

Toate aplicațiile care au ca și limbaj de dezvoltare Visual Fox Pro 9 vor fi migrate gratuit de producător într-un sistem integrat nou dezvoltat în Angular și care va folosi ca sistem de gestiune a bazelor de date Microsoft SQL Server. În acest sistem de prelucrarea informațiilor este optimizată și vor exista automatizări noi care vor simplifica și mai mult operațiile efectuate de utilizator. Aplicațiile unde numele este colorat în roșu sunt în curs de transfer pe noul sistem și va fi operațional începând cu ianuarie 2023.

VI.3 Aplicatiile informatice si tehnologii digitale care sunt utilizate aferent *Proceselor Suport* de *Gestiune si Mentenanta Datelor* din cadrul departamentelor/ serviciilor/compartimentelor Primariei Bistrita si a Serviciilor Subordonate - *Direcția Asistență Socială – str.Dornei nr.12*

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii / localizare (in ce locatii/departamente / entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizo-rul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul/ aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
1	Cid_dmss – aplicație Registrul intern al documentelor (circuitul documentelor)	Direcția de asistență socială	L		Pe server propriu în centrul de date PMB	Indeco Soft Baia Mare		2018	Da	CID	Asigură urmărirea circulației electronice a documentelor intrate în DAS, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare.		
2	Lexexpert – aplicație de legislație	Toate compartimentele	L		Pe server propriu în centrul de date PMB	Indeco Soft Baia Mare		1995	Nu				
3	Portal – www.primariabistrita.ro	Toate compartimentele	L		Pe server propriu în centrul de date PMB			2021	Nu				
4	Încălzire – aplicație evidență acordare ajutoare de încălzire	Direcția de asistență socială	L	Apache/ MySQL	Pe server propriu în centrul de date PMB	Costin Dumitriu			Da				
5	AsiSoc- aplicație prestări sociale	Direcția de sistență socială / strada Dornei	L	Apache / PHP / MySQL	Pe server propriu în centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de CID		Da	Asisoc	Asigură gestiunea, evidența și raportările pentru majoritatea prestărilor sociale oferite de direcție.		
3	Buget – modul care gestionează veniturile și	Compartiment buget și executare	L	Visual Fox Pro 9	pe server propriu in centrul de date	Indeco Soft Baia	Integrare cu modulele: Cassa,		Da	Buget_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații		..\4.Manuale de utilizare\Buget_2006-Manual de utilizare.pdf

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii / localizare (in ce locatii/departamente / entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizo-rul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul/ aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
	cheltuielile și execuția bugetară.	bugetară/Piața Centrală nr.6		/MSSQL	PMB	Mare	Contab, Dars, GestBug, GeCon, MiFix, Invest, Acon, ResUm, CID				de la acestea. Integrat cu sistemul eFactura.		
4	Cassa – modul care înregistrează și urmărește operațiile de încasări sau plăți făcute prin casa	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu modulul de Buget, Contab și ImpoTax		Da	Cassa	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Cassa-Manual de utilizare.pdf
5	Contab – modulul este un instrument de urmărire și analiză a activității instituției prin gestiunea tuturor înregistrarilor contabile	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, ImpoTax, Contab, Dars, GestBug, GeCon, MiFix, Invest, ResUm		Da	Contab_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Contab2006-Manual de utilizare.pdf
6	Dars – modul instrument pentru generare dări de seamă	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix		Da	Dars_2006	Generează automat toate situațiile financiare pe baza datelor prelucrate în restul modulelor din pachetul financiar contabil		..\4.Manuale de utilizare\Dars2006-Manual de utilizare.pdf
7	eCubAdmin - centru de management unitar al tuturor	Compartiment tehnologia informației	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu toate modulele din pachetul		Da	Nucleu	Gestionează utilizatorii și drepturile lor pentru modulele din pachetul financiar contabil. Asigură mecanismul de backup		

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii / localizare (in ce locatii/departamente / entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizo-rul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul/ aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
	modulelor care definesc produsul eCUB	, Indeco Soft					financiar contabil				automat al bazelor de date într-o locație din rețea după un program configurabil.		
8	Gestbug – generează situații economice	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix		Da	Gestbugue	Generează automat toate situațiile economice necesare gestionării materialelor și a obiectelor de inventar (intrări, ieșiri, inventare, etc)		
9	ListOP – listări ordine plată	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget		Da	Nucleu	-		
10	MiFix – gestionează mijloacele fixe	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab		Da	MiFix	Generează automat toate situațiile economice necesare gestionării mijloacelor fixe. (intrări, ieșiri, inventare, reevaluare, etc)		..\4.Manuale de utilizare\MiFix-Manual de utilizare.pdf
11	ResUm – gestionează personalul din instituție, salarizarea	Direcția asistență socială/ Dornei nr.12	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab		Da	ResUm	Gestionează resursele umane din instituție, asigură calculul salariului și generează raportările stabilite de legislație.		..\4.Manuale de utilizare\ResUm-manual de utilizare.pdf

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul

(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului

(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)

(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins

(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

VI.4 Aplicatiile Aplicatiile informatice si tehnologii digitale care sunt utilizate aferent *Proceselor Suport* de *Gestiune si Mentenanta Datelor* din cadrul departamentelor/serviciilor/compartimentelor Primariei Bistrita si a Serviciilor Subordonate - *Direcția Patrimoniu – Str.Gh. Șincai nr.2*

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departa mente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabi litate (3)	Istoric (4)	Mentenanta asigurata (Da/Nu)	BD la care este conectat sistemul/ aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
1	CID – circuitul intern al documentelor	Toate compartimentel e care sunt în lan-ul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2, L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Târpiului nr.2,	L	Apache / PHP / MySQL	Pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal cetățeni	2017		CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.	..\5.Caiete de sarcini\Caiet sarcini CID.doc	..\4.Manuale de utilizare\CID manual de utilizare.pdf
2	Lexexpert – aplicație de legislație	Toate compartimentel e	L		Pe server propriu în centrul de date PMB	Indeco Soft Baia Mare		1995					

3	Portal PMB – www.primariabistrita.ro	Toate compartimentele și Cetățenii	L	Apache / PHP / MySQL / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu următoarele module: CID, ImpoTax, Urbanism	2020		Portal, Impozite-Bistrita, CID	Asigură servicii electronice către cetățeni asigurând digitalizarea completă a procesului de la cetățean la inspectorul care prelucrează solicitarea în aplicația din backend sau procese complet automatizate fără a mai fi nevoie de un inspector (eliberarea certificatelor de atestare fiscală)	..\5.Caiete de sarcini\Caiet de Sarcini portal 2020 POCA.pdf	..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf
4	GeCon – gestionare contracte	Direcția Patrimoniu/Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu	Indeco Soft Baia Mare	Integrare cu modulele: Contab și Cassa	2010	Da	ImpoziteGeCon-Bistrita	Gestionează automat următoarele procese: debitare (după formule și moduri de debitare configurabile), încasări și calcul automat de dobânzi după reguli configurabile pe fiecare tip de venit.		..\4.Manuale de utilizare\GeCon - Manual de utilizare.pdf
5	Parcari – aplicatie online	Direcția Patrimoniu/Gh. Șincai nr.2/cetățenii	L	Laravel (PHP), Vue.js, MySQL, PostgreSQL, MS SQL	Virtual Appliance (Server al institutiei)	GREEN OVEN SRL	GeCON	2015	Da	GeCON	Parcari – aplicatie online vizualizare si rezervare parcare rezidentiala – pe portalul PMB - https://parcari.primariabistrita.ro/		
6	Buget – modul care gestionează veniturile și cheltuielile și execuția bugetară.	Direcția Patrimoniu/ Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, Contab, Dars, GestBug, GeCon, MiFix, Invest, Acon, ResUm, CID	2006	Da	Buget_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea. Integrat cu sistemul eFactura.		..\4.Manuale de utilizare\Buget_2006-Manual de utilizare.pdf
7	Cassa – modul care înregistrează și urmărește operațiile de încasări sau plăți făcute prin casa	Direcția Patrimoniu/ Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu modulul de Buget, Contab și ImpoTax	2006	Da	Cassa	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Cassa-Manual de utilizare.pdf

8	Contab – modulul este un instrument de urmărire și analiză a activității instituției prin gestiunea tuturor înregistrarilor contabile	Direcția Patrimoniu/Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, ImpoTax, Contab, Dars, GestBug, GeCon, MiFix, Invest, ResUm	2006	Da	Contab_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Contab2006-Manual de utilizare.pdf
9	Dars – modul instrument pentru generare dări de seamă	Direcția Patrimoniu/ Gh. Țincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Dars_2006	Generează automat toate situațiile financiare pe baza datelor prelucrate în restul modulelor din pachetul financiar contabil		..\4.Manuale de utilizare\Dars2006-Manual de utilizare.pdf
10	eCubAdmin - centru de management unitar al tuturor modulelor care definesc produsul eCUB	Compartiment tehnologia informației, Indeco Soft	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu toate modulele din pachetul financiar contabil	2006	Da	Nucleu	Gestionează utilizatorii și drepturile lor pentru modulele din pachetul financiar contabil. Asigură mecanismul de backup automat al bazelor de date într-o locație din rețea după un program configurabil.		
11	Gestbug – generează situații economice	Direcția Patrimoniu/ Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Gestbugue	Generează automat toate situațiile economice necesare gestionării materialelor și a obiectelor de inventar (intrări, ieșiri, inventare, etc)		
12	ListOP – listări ordine plată	Direcția Patrimoniu/ Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget	2006	Da	Nucleu	-		
13	MiFix – gestionează mijloacele fixe din direcție	Direcția Patrimoniu/ Gh.Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	MiFix	Generează automat toate situațiile economice necesare gestionării mijloacelor fixe. (intrări, ieșiri, inventare, reevaluare, etc)		..\4.Manuale de utilizare\MiFix-Manual de utilizare.pdf
14	ResUm – gestionează personalul din	Compartiment financiar salarizare și	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de	Indeco Soft Baia Mare	Integrare cu modulele: Buget,	2006	Da	ResUm	Gestionează resursele umane din instituție, asigură calculul		..\4.Manuale de utilizare\ResUm-manual de

	direcție, salarizarea	Biroul resurse umane/Piața Centrală nr.6			date PMB		Contab				salariului și generează raportările stabilite de legislație.		utilizare.pdf

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul
(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului
(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)
(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins
(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

VI.5 Aplicatiile informatice si tehnologii digitale care sunt utilizate aferent *Proceselor Suport* de *Gestiune si Mentenanta Datelor* din cadrul departamentelor/ serviciilor/compartimentelor Primariei Bistrita si a Serviciilor Subordonate - *Direcția Piețe Târguri și Oboare – Piața Decebal*

Nr. Crt	Nume (denumirea aplicatiei/tehnologiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
1	CID – circuitul intern al documentelor	Toate compartimentele care sunt în lan-ul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2, L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Tărpiului nr.2,	L	Apache / PHP / MySQL	Pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal cetățeni	2017		CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.	..\5.Caiete de sarcini\Caiet sarcini CID.doc	..\4.Manuale de utilizare\CID manual de utilizare.pdf	

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
2	LEX EXPERT – legislația Romîniei și a U.E., Jurisprudență, etc.	Utilizatorii din rețeaua locală de calculatoare a PMB	L	Delphi	Pe server propriu în centrul de date PMB	COMPANIA DE INFORMATICĂ NEAMȚ	Se pot exporta documente in orice editor Windows (Word, Excel etc.)	2001/2022	DA		Neaplicabil		..\4.Manuale de utilizare\Manual Lex.pdf	Mare
3	Portal PMB – www.primariabistrita.ro	Toate compartimentele și Cetățenii	L	Apache / PHP / MySQL / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu următoarele module: CID, ImpoTax, Urbanism	2020		Portal, Impozite-Bistrita, CID	Asigură servicii electronice către cetățeni asigurând digitalizarea completă a procesului de la cetățean la inspectorul care prelucrează solicitarea în aplicația din backend sau procese complet automatizate fără a mai fi nevoie de un inspector (eliberarea certificatelor de atestare fiscală)	..\5.Caiete de sarcini\Caiet de Sarcini portal 2020 POCA.pdf	..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf	
4	Buget – modul care gestionează veniturile și cheltuielile și execuția bugetară.	Compartiment buget și executare bugetară/Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, Contab, Dars, GestBug, GeCon, MiFix, Invest, Acon, ResUm, CID	2006	Da	Buget_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea. Integrat cu sistemul eFactura.		..\4.Manuale de utilizare\Buget_2006-Manual de utilizare.pdf	

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departa mente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnolo gii (1)	Deploy ment (2)	Furnizoru l	Interoperabi litate (3)	Istoric (4)	Mente nanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
5	Cassa – modul care înregistrează și urmărește operațiile de încasări sau plăți făcute prin casa	Direcția economică/Gh. Șincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu modulul de Buget, Contab și ImpoTax	2006	Da	Cassa	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Cassa-Manual de utilizare.pdf	
6	Contab – modulul este un instrument de urmărire și analiză a activității instituției prin gestiunea tuturor înregistrarilor contabile	Compartiment contabilitate/ Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, ImpoTax, Contab, Dars, GestBug, GeCon, MiFix, Invest, ResUm	2006	Da	Contab_ 2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Contab2006-Manual de utilizare.pdf	
7	Dars – modul instrument pentru generare dări de seamă	Direcția economică/Piața Centrală nr.6Die	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Dars_20 06	Generează automat toate situațiile financiare pe baza datelor prelucrate în restul modulelor din pachetul financiar contabil		..\4.Manuale de utilizare\Dars2006-Manual de utilizare.pdf	
8	eCubAdmin - centru de management unitar al tuturor modulelor care definesc produsul eCUB	Compartiment tehnologia informației, Indeco Soft	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu toate modulele din pachetul financiar contabil	2006	Da	Nucleu	Gestionează utiliza-torii și drepturile lor pentru modulele din pachetul financiar contabil. Asigură me-canismul de backup automat al bazelor de date într-o locație din rețea după un pro-gram configurabil.			

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
9	Gestbug – generează situații economice	Compartiment buget și executare bugetară/Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Gestbug ue	Generează automat toate situațiile economice necesare gestionării materialelor și a obiectelor de inventar (intrări, ieșiri, inventare, etc)			
10	ListOP – listări ordine plată	Direcția economică/Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget	2006	Da	Nucleu	-			
11	MiFix – gestionează mijloacele fixe	Direcția economică/Piața Centrală nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	MiFix	Generează automat toate situațiile economice necesare gestionării mijloacelor fixe. (intrări, ieșiri, inventare, reevaluare, etc)		..\4.Manuale de utilizare\MiFix-Manual de utilizare.pdf	
12	ResUm – gestionează personalul din instituție, salarizarea	Compartiment financiar salarizare și Biroul resurse umane/Piața Centrală nr.6	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	ResUm	Gestionează resursele umane din instituție, asigură calculul salariului și generează raportările stabilite de legislație.		..\4.Manuale de utilizare\ResUm-manual de utilizare.pdf	
13	GeCon – gestionare contracte	Direcția Patrimoniu/Gh. Țincai nr.2	L	Visual Fox Pro 9 /MSSQL	pe server propriu	Indeco Soft Baia Mare	Integrare cu modulele: Contab și Cassa		Da	Impozite GeCon-Bistrita	Gestionează automat următoarele procese: debitare (după formule și moduri de debitare configurabile), încasări și calcul			

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare	Grad satisfactie in utilizare
											automat de dobânzi după reguli configurabile pe fiecare tip de venit.			

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul

(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului

(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)

(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins

(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

VI.6 Aplicatiile informatice si tehnologii digitale care sunt utilizate aferent *Proceselor Suport de Gestiune si Mentenanta Datelor* din cadrul departamentelor/serviciilor/compartimentelor Primariei Bistrita si a Serviciilor Subordonate - *Direcția Servicii Publice – str.Liviu Rebreanu nr.2-4*

Nr. Crt	Nume (denumirea aplicatiei/tehnologiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deploym ent (2)	Furnizo-rul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
1	CID – circuitul intern al documentelor	Toate compartimentele care sunt în lan-ul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2, L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Tărpiului nr.2,	L	Apache / PHP / MySQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal cetățeni	2017	Da	CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.	..\5.Caiete de sarcini\Caiet sarcini CID.doc	..\4.Manuale de utilizare\CID manual utilizare.pdf
2	LEX EXPERT – legislația Romîniei și a U.E., Juris-prudență, etc.	Utilizatorii din rețeaua locală de calculatoare a PMB	L	Delphi	Pe server propriu în centrul de date PMB	COMPANIA DE INFORMATICĂ NEAMȚ	Se pot exporta documente in orice editor Windows (Word, Excel etc.)	2001/2022	DA		Neaplicabil		..\4.Manuale de utilizare\Manual Lex.pdf
3	Portal – www.primariabistrita.ro	Toate compartimente-le	L		Pe server propriu în centrul de date PMB	Indeco Soft Baia Mare		2021					..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf

Nr. Crt	Nume (denumirea aplicatiei/tehnologiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizo-rul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
4	Buget – modul care gestionează veniturile și cheltuielile și execuția bugetară.	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, Contab, Dars, GestBug, GeCon, MiFix, Invest, Acon, ResUm, CID	2006	Da	Buget_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea. Integrat cu sistemul eFactura.		..\4.Manuale de utilizare\Buget_2006-Manual de utilizare.pdf
5	Cassa – modul care înregistrează și urmărește operațiile de încasări sau plăți făcute prin casa	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu modulul de Buget, Contab și ImpoTax	2006	Da	Cassa	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Cassa-Manual de utilizare.pdf
6	Contab – modulul este un instrument de urmărire și analiză a activității instituției prin gestiunea tuturor înregistrarilor contabile	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Cassa, ImpoTax, Contab, Dars, GestBug, GeCon, MiFix, Invest, ResUm	2006	Da	Contab_2006	Pune la dispoziție informații către toate modulele enumerate la integrare și primește informații de la acestea.		..\4.Manuale de utilizare\Contab2006-Manual de utilizare.pdf
7	Dars – modul instrument pentru generare dări de seamă	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Dars_2006	Generează automat toate situațiile financiare pe baza datelor prelucrate în restul modulelor din pachetul financiar contabil		..\4.Manuale de utilizare\Dars2006-Manual de utilizare.pdf

Nr. Crt	Nume (denumirea aplicatiei/tehnologiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta*	Tehnologii (1)	Deployment (2)	Furnizor-ul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigurata (Da/ Nu)	BD la care este conectat sistemul / aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
8	eCubAdmin - centru de management unitar al tuturor modulelor care definesc produsul eCUB	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrat cu toate modulele din pachetul financiar contabil	2006	Da	Nucleu	Gestionează utilizatorii și drepturile lor pentru modulele din pachetul financiar contabil. Asigură mecanismul de backup automat al bazelor de date într-o locație din rețea după un program configurabil.		
9	Gestbug	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab, MiFix	2006	Da	Gestbug ue	Generează automat toate situațiile economice necesare gestionării materialelor și a obiectelor de inventar (intrări, ieșiri, inventare, etc)		
10	ListOP	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulul de Buget	2006	Da	Nucleu	Listare ordine de plată după diferite criterii		
11	MiFix	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	MiFix	Generează automat toate situațiile economice necesare gestionării mijloacelor fixe. (intrări, ieșiri, inventare, reevaluare, etc)		..\4.Manuale de utilizare\MiFix-Manual de utilizare.pdf
12	ResUm	Direcția Servicii Publice/L. Rebreanu 2-4	L	Visual Fox Pro 9 /MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Buget, Contab	2006	Da	ResUm	Gestionează resursele umane din instituție, asigură calculul salariului și generează raportările stabilite de legislație.		..\4.Manuale de utilizare\ResUm-manual de utilizare.pdf

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul

(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului

(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)

(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins

(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

VI.7 Aplicatiile informatice si tehnologii digitale care sunt utilizate aferent *Proceselor Suport* pentru *Coordonare servicii relații publice, informatică, registratură generală* din cadrul departamentelor/serviciilor/compartimentelor Primariei Bistrita si a Serviciilor Subordonate - Direcția Comunicare/ Serviciul Relații Publice, Comunicare

Nr. Crt	Nume (denumirea aplicatiei/tehno-logiei de digitalizare si specificarea obiectivului pentru care este utilizata)	Care sunt utilizatorii/ localizare (in ce locatii/departa mente/ entitati subordonate ruleaza aplicatia)	Flag licentiere (L/F) L=exista licenta pentru softul respectiv F= soft care nu necesita licenta	Tehnologii (1)	Deployment (2)	Furnizorul	Interoperabilitate (3)	Istoric (4)	Mentenanta asigu-rata (Da/ Nu)	BD la care este conectat sistemul/ aplicatia (5)	Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)	Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)	Link la Manualul de Utilizare
1	CID – circuitul intern al documentelor	Toate compartimentele care sunt în lan-ul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2, L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Tărpiului nr.2,	L	Apache / PHP / MySQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal cetățeni	2017	Da	CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.	..\5.Caiete de sarcini\Caiet sarcini CID.doc	..\4.Manuale de utilizare\CID manual de utilizare.pdf
2	Portal PMB – www.primariabistrita.ro	Toate compartimentele/ Cetățeni	L	Apache / PHP / MySQL / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu următoarele module: CID, ImpoTax, Urbanism	2020	Da	Portal, Impozite-Bistrita, CID	Asigură servicii electronice către cetățeni asigurând digitalizarea completă a procesului de la cetățean la inspectorul care prelucrează solicitarea în aplicația din backend sau procese complet automatizate fără a mai fi nevoie de un inspector (eliberarea certificatelor de atestare fiscală)	..\5.Caiete de sarcini\Caiet de Sarcini portal 2020 POCA.pdf	..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf

3	**LEX EXPERT – legislația Romîniei și a U.E., Jurisprudență, etc.**	**Utilizatorii din rețeaua locală de calculatoare a PMB**	**L**	**Delphi**	**Pe server propriu în centrul de date PMB**	**COMPANIA DE INFORMATICĂ NEAMȚ**	**Se pot exporta documente in orice editor Windows (Word, Excel etc.)**	**2001/2022**	**DA**		**Neaplicabil**		**..\4.Manuale de utilizare\Manual Lex.pdf**
Nr. Crt	**Nume (denumirea aplicatiei/tehnologiei de digitalizare si specificarea obiectivului pentru care este utilizata)**	**Care sunt utilizatorii/ localizare (in ce locatii/departamente/ entitati subordonate ruleaza aplicatia)**	**Flag licentiere (L/F) L=*exista licenta pentru softul respectiv* F= *soft care nu necesita licenta***	**Tehnologii (1)**	**Deployment (2)**	**Furnizorul**	**Interoperabilitate (3)**	**Istoric (4)**	**Mentenanta asigurata (Da/ Nu)**	**BD la care este conectat sistemul/ aplicatia (5)**	**Evidentiere functionalitati de tip SMART (considerate a fi inovative si/sau adecvate pentru cresterea eficientei activitatilor in departamentele in care se utilizeaza)**	**Link la Caietul de Sarcini in baza caruia s-a efectuat achizitia (daca exista un astfel de Caiet de Sarcini)**	**Link la Manualul de Utilizare**
1	CID – circuitul intern al documentelor	Toate compartimentele care sunt în lanul PMB: Piața Centrală nr.6, Piața Centrală nr.2, Gh. Șincai nr.2, L.Rebreanu 2-4, N.Titulescu nr.3, Al. Odobescu nr.17A, D.Gherea nr.14, Piața Decebal, V. Babeș nr.28 și 37, Tărpiului nr.2,	L	Apache / PHP / MySQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu modulele: Urbanism, ImpoTax, AgroRegis, iReport Bistrița, Portal cetățeni	2017	Da	CID	Asigură urmărirea circulației electronice a documentelor intrate în instituție, ieșite din instituție și interne. Pentru toate aceste tipuri de documente asigură și arhivarea lor în format electronic prin scanare direct din aplicație sau atașare. Este integrat cu emailul oficial al instituției asigurând preluarea automată a solicitărilor primite prin el și răspunsul către cetățeni / instituții direct din CID. Asigură preluarea sesizărilor din iReport Bistrița și trimiterea răspunsurilor. Asigură preluarea petițiilor din Portalul pentru cetățeni și răspunsul către petițiile respective.	..\5.Caiete de sarcini\Caiet sarcini CID.doc	..\4.Manuale de utilizare\CID manual de utilizare.pdf
2	Portal PMB – www.primariabistrita.ro	Toate compartimentele / Cetățeni	L	Apache / PHP / MySQL / MSSQL	pe server propriu in centrul de date PMB	Indeco Soft Baia Mare	Integrare cu următoarele module: CID, ImpoTax, Urbanism	2020	Da	Portal, Impozite-Bistrita, CID	Asigură servicii electronice către cetățeni asigurând digitalizarea completă a procesului de la cetățean la inspectorul care prelucrează solicitarea în aplicația din backend sau procese complet automatizate fără a mai fi nevoie de un inspector (eliberarea certificatelor de atestare fiscală)	..\5.Caiete de sarcini\Caiet de Sarcini portal 2020 POCA.pdf	..\4.Manuale de utilizare\Manual portal WEB - Adaugare articole si documente.pdf

3	LEX EXPERT – legislația Romîniei și a U.E., Jurisprudență, etc.	Utilizatorii din rețeaua locală de calculatoare a PMB	L	Delphi	Pe server propriu în centrul de date PMB	COMPANIA DE INFORMATICĂ NEAMȚ	Se pot exporta documente in orice editor Windows (Word, Excel etc.)	2001/2022	DA		Neaplicabil		..\4.Manuale de utilizare\Manual Lex.pdf

(1) Tehnologii: include: limbaje (Java, .NET, PHP …), sisteme de baze de date (MS SQL, MySQL, MongoDB etc), respectiv alte caracteristici tehnologice specifice, care pot fi relevante pentru audit, daca e cazul
(2) Deployment (echipamentele de calcul pe care ruleaza) : pe statii individuale de lucru, pe server in custodia institutiei, pe serverele furnizorului
(3) Interoperabilitate (cu ce aplicatii este direct interfatata, ce poate exporta, ce poate importa; scurta descriere)
(4) anul de cand sunt in functiune, respectiv anul cand s-au actualizat sau extins
(5) In cazul in care este vorba de mai multe baze de date, se precizeaza toate; in cazul in care aplicatia nu este conectata la BD, se specifica "*Nu este cazul*"

VII. DEETALII SUPLIMENTARE PRIVIND STADIUL ACTUAL AL DIGITALIZARII PROCESELOR ADMINISTRATIEI PUBLICE DIN PRIMARIA MUNICIPIULUI BISTRITA

Constatare pozitivă generală: toți funcționarii publici ai Primăriei au semnături electronice, primite de la STS.

Privitor la GIS:

Incă din 2004 s-a început crearea unei baze de date GIS, cu ajutorul firmei GeoTop, sistemul fiind finalizat în anul 2016 şi cuprinzând şi mărirea de intravilan.

Pentru extravilan, există o bază de date cu punerile în posesie conform legii 165.

Actualmente, se lucrează cu un strat importat din ETERRA (atât pentru intravilan cât şi pentru extravilan), cu date atât în mod grafic cât şi alfanumeric. Se foloseşte ARGIS versiunea desktop 10.5.1, existând nouă licențe individuale, două licențe concurente plus o licența de server.

Problema cea mai mare este aceea că trebuie rezolvată neapărat interoperabilitatea Bazelor de Date GIS – ceea ce s-a semnalat deja din 1992.

- Lipsa de actualitate şi lipsa de integrare a soft-urilor pentru sistemele GIS este reflectată inclusiv prin faptul că cele 12 licențe ARGIS desktop existente, sunt neactualizate din 2015.
- Foarte important este de asemenea faptul că nu există proceduri/interfețe de interacțiune directă cu celelalte instituții implicate în gestiunea resurselor GIS.

Toate aceste probleme urmează a fi rezolvate prin proiectul descris în Fişa de Proiect întitulată «***GIS pentru gestiunea informațiilor de urbanism, colectarea şi accesibilitatea acestora***», care se află în secțiunea dedicată Fişelor de Proiect.

Privitor la Procesul de Achiziții:

Procedura de achiziții decurge conform reglementărilor, dar în afara interacțiunii cu SEAP, nu există altă platformă digitalizată care să asiste procesul.

La intrare, procesul are Referatele însoțite de Note Explicative şi Documentele Tehnice aferente (Caiet de Sarcini, Specificații Tehnice etc).

La ieşire, Contractul de achiziții se înregistrează în Registrul de achiziții manual, se trece mai apoi In modulul de achiziții al platformei INDECO.

Facturile merg mai întâi la departamentul economic, după care factura în original vine înapoi la Achiziții.

Planul de achiziții este ținut în Excel, existând şi un alt fişier Excel în care se consemnează stadiul achizițiilor aflate în derulare.

In această manieră, procedura este greoaie şi are multe redundanțe, ca atare se constată nevoia unei platforme software de asistare a acestui proces, care sa fie integrată cu platformele de digitalizare ale celorlalte procese ale administrației publice locale a Municipiului Bistrița.

Privitor la Procesul de Management/Alocare Resurse Umane:

Există un program (RESUM) realizat de firma INDECO, care gestionează Baza de Date cu personalul Primăriei Municipiului Bistrița.

Gestiunea concediilor se face şi în paralel in Excel, pentru a se acoperi perioadele în care RESUM nu este funcțional, de aceea se constată faptul că partea de procesare digitalizată a cererilor de concediu este deficitară

Pentru Contractele de Muncă se foloseşte REVISAL; se mai lucrează şi cu portalul AJOFM de la nivel național.

Pentru declarațiile de avere şi interese, se lucrează cu platforma EDAI disponibilă la nivel național.

Sistemul de pontaj automat este gata de dat în folosință, urmând a fi instalat în 21 locații din Primăria Municipiului Bistrița.

Se constată faptul ca majoritatea activităților din departamentul de Resurse Umane au evidențe ținute inclusiv în tabele Excel, comunicarea între acest departament şi celelalte departamente interne/ organizații externe se derulează prin email-uri.

In ceea ce priveşte evidența digitalizată a gradului de instruire a personalului din Primăria Bistrița, este şi aceasta deficitară într-o oarecare măsură, anumite date despre nivelul de instruire fiind stocate în mod static în baza de date a sistemului RESUM, dar procesul de instruire continuă şi evaluare continuă a gradului de instruire nu are un suport digitalizat capabil a urmări în mod dinamic întregul proces.

Pentru digitizarea dosarelor de personal şi pentru digitalizarea întregului proces de management/ alocare a resurselor umane din Primăria Bistrița, este nevoie deci de o platformă dedicată, integrată şi ca atare interoperabilă cu platformele de digitalizare ale celorlalte procese ale administrației publice locale a Municipiului Bistrița.

Privitor la Procesul de Management al Patrimoniului

Gestionarea patrimoniul Primăriei Municipiului Bistrița se referă la următoarele categorii:

- Închirieri de locuințe din fondul locativ vechi
- Închirieri de locuințe sociale
- Locuințe ANL
- Sedii de partide politice
- Asociații/Fundații
- Concesiuni / inclusiv pășuni care se află în proprietatea primăriei (există suprafețe de pajişti care sunt ale municipiului); Ocolul Silvic – reunit cu Livezile, este subordonat Consiliului Local.

Toate contractele de acest tip sunt urmărite prin intermediul unui soft numit GeCon, care are in spate o Bază de Date în care sunt înregistrate toate aceste obiective de patrimoniu.

In plus, toate parcările de pe teritoriul Municipiului Bistrița sunt gestionate tot prin GeCon. Există 10 000 de locuri pentru parcări rezidențiale şi 1200 locuri pentru parcări cu plată. Sunt definite 11 zone, etapizate din punctul de vedere al termenului de expirare a abonamentelor, toate aceste condiționalități fiind procesate inclusiv prin intermediul unei aplicații mobile numită Parcări Online, care are şi facilități de desenare cu ACAD şi este interoperabilă cu GeCon, în sensul de a se putea actualiza situația parcărilor după expirarea termenelor de plată a abonameentelor.

De asemenea, tot în acest context, este pregătită funcționalitatea de rezervare de la distanță a locurilor de parking, plata abonamentului facându-se tot în context GeCon, prin mecanismul GlobalPay furnizat de firma SYBIT.

Privitor la Procesul de Registratură şi Circulație a documentelor

Există un program de registratură, prin intermediul căruia se dau automat numere de înregistrare pentru cererile depuse la toate compartimentele Primăriei Municipiului Bistrița.

Toate documentele circulă deocamdată în format fizic, iar în format electronic unele dintre ele circulă pe email, ca atare un pas important de făcut în acest domeniu este acela de a se pune la punct o platformă software pentru circuitul documentelor în format electronic, integrată şi ca atare interoperabilă cu platformele de digitalizare ale tuturor celorlalte procese ale administrației publice locale a Municipiului Bistrița.

Privitor la Procesele aferente Serviciului de Urbanism

Deşi există în momentul de față posibilitatea de a se lucra în acest domeniu cu platforma RENNS (Registrul Electronic Național de Nomenclatură Stradală), nu sunt încărcate toate datele urbanistice în RENNS, spre exemplu sunt multe străzi care nu au denumire proprie, numerele de case fiind extinse de la străzile care au nume. Este evidentă deci necesitatea implementării şi în acest domeniu a unei platforme software, care să asiste gestionarea completă şi integrată a resurselor urbanistice, care să fie de asemenea interoperabilă cu platformele de digitalizare ale tuturor celorlalte procese ale administrației publice locale a Municipiului Bistrița.

In acest sens, platforma software pentru urbanism va trebui să permită vizualizarea inclusiv a datelor de la toate serviciile publice (Apă, Canal etc), în plus să permită consultarea şi actualizarea PUG-ului, cu funcționalități pentru eliberarea online de avize, aprobări, certificate şi alte documente de urbanism. De asemenea, pentru toate construcțiile este important să se digitizeze Cartea Construcției, pentru a putea fi stocată în format electronic în baza de date integrată de urbanism. La fel, este necesară integrarea şi interoperabilitatea cu celelalte procese.

Privitor la Procesele de Management

Digitalizarea tuturor proceselor Administrației Publice a Municipiului Bistrița, va permite finalmente şi implementarea unui Dashboard (Tablou de Bord) pentru asistarea proceselor de management, operabil de către managementul de vârf şi cel mediu, cât şi de către toți funcționarii publici din Primărie care sunt responsabili de procese în baza unor drepturi de acces ierarhizate, care să permită:

- accesul online la traseul documentelor transpuse în mod obligatoriu în format electronic,
- interacțiunea online între echipele diverselor servicii/compartimente şi
- furnizarea tuturor funcționalitățile caracteristice unei platforme suport pentru decizii.

De mare importanța este şi posibilitatea de grupare, prin intermediul unei astfel de platforme, a solicitărilor cetățenilor pe tipuri de probleme, cât şi generarea de atenționări şi alarmări privind iminența unor depăşiri de termene în rezolvarea acestora, după caz.

VIII Analiză și diagnostic asupra stadiului de digitalizare a proceselor administrației publice din Primăria Municipiului Bistrița

Analiza nivelului existent de digitalizare a proceselor organizaționale din cadrul Primăriei Municipiului Bistrița s-a realizat prin discuții directe cu reprezentanți ai compartimentelor din cadrul primăriei. Analiza urmărește identificarea aplicațiilor informatice care susțin procesele organizaționale, atât cele derulate în relația cu cetățenii și alte entități deservite (companii, asociații și fundații, etc.) prin serviciile publice, cât și activitățile suport derulate în cadrul instituției.

Analiza preliminară a stadiului digitalizării în cadrul administrației publice locale a Primăriei Municipiului Bistrița a fost structurată pe următoarele arii:

- Aplicațiile informatice utilizate - Informații privind funcționalitatea, furnizorii, licențierea, accesul la date. Informații privind acoperirea informatică a activității, gradul de satisfacție dat de aplicațiile curente, problemele aplicațiilor;
- Activitatea direcției sau serviciului – pentru fiecare direcție/serviciu din cadrul Primăriei Municipiului Bistrița, au fost colectate informații legate de tipuri de procese, documente utilizate, informații utilizate, de unde sunt colectate și unde sunt transmise, provocările și dificultățile specifice în activitate, comunicarea cu celelalte structuri din primărie și din instituțiile subordonate;
- Modul ideal în care cei implicați văd că ar trebui să se deruleze activitatea și comunicarea;
- Ideile concrete pe care le au reprezentanții direcțiilor și serviciilor privind pașii care se pot face și aplicațiile care ar trebui implementate pentru a îmbunătăți activitatea, inclusiv prin informatizare;
- Proiecte de informatizare care sunt în curs de implementare sau care sunt deja definite și pregătite pentru a fi implementate.

Sistemele informatice existente acoperă o serie de funcții operaționale de bază. Există activități importante unde informatizarea este foarte slabă sau inexistentă (cum ar fi gestiunea proiectelor, achizițiile publice). În cadrul compartimentelor mai bine informatizate (venituri, resurse umane, etc.), există în continuare activități care nu au suport digital și sistemele existente necesită îmbunătățiri.
În ceea ce privește nivelul de integrare a sistemelor informatice, acesta este scăzut, astfel încât există multe cazuri în care informațiile nu pot fi preluate dintr-un sistem în altul, în anumite cazuri chiar impunând cetățenilor obligația transferului fizic al unor documente.

Per ansamblu personalul este deschis la ideea de informatizare și își dorește un nivel mai ridicat de suport informatic, atât pentru activitatea internă, derulată în și între compartimentele instituției, cât și pentru a reduce efortul și disconfortul cetățenilor care încă în anumite situații sunt nevoiți să își asume personal transferul de informații, pe suport fizic pe hârtie, între departamente ale Primăriei în condițiile lipsei interoperabilității adecvate.
Totuși, nivelul general de expunere a personalului instituției la tendințele actuale este relativ scăzut în ce privește e-guvernarea, transformarea digitală, securitatea cibernetică.

Situația existentă la nivelul direcțiilor și departamentelor cheie se prezintă după cum urmează. Structura si denumirile departamentelor Primăriei Municipiului Bistrița sunt cele aprobate si functionale la nivelul anului 2022.

Direcția Economică

Activitățile de programare și execuție bugetară sunt informatizate parțial, încă din 2006. Aplicațiile principale care asistă procesele contabile și cele legate de colectarea taxelor sunt oferite de același furnizor (Indeco Software din Baia Mare). Aceste aplicații sunt încă sub formă de sisteme desktop, fiecare dintre ele instalate local, conectate la un server central pe care sunt stocate datele. A fost discutată cu furnizorul necesitatea de evoluție înspre aplicații web și este prevăzută transpunerea acestui set de aplicații la un sistem web integrat, “SIGMA”, însă calendarul de implementare nu este deocamdată clar definit, urmărindu-se ca în cursul anului 2023 să se avanseze în această direcție.
Setul de aplicații furnizat de INDECO include suportul pentru execuția bugetară, contabilitate, gestiune, mijloace fixe, resurse umane, registratură (sistemul CID - Circuitul Intern al Documentelor), impozite și taxe, registrul agricol. Aceste aplicații sunt încă slab integrate între ele și nu sunt interoperabile cu celelate sisteme ale primăriei. Furnizorul este deschis la dialog însă rezervat la a accepta extinderi ale funcționalității sistemelor actuale mai ales în perspectiva trecerii la o nouă versiune integrată într-un viitor încă neclar definit.
Direcția economică evidențiază o listă consistentă de lipsuri în informatizare și în capacitatea de gestiune integrată a informațiilor și documentelor, printre care se remarcă următoarele
Ar fi nevoie de integrarea unor mijloace de plată mai flexibile, prin card sau numerar, pentru încasările impozitelor și taxelor și a plăților de valoare mică necesare pentru primirea de către cetățeni a unor servicii. O posibilă variantă văzută de instituție este instalarea unor automate de plată și integrarea lor digitală cu sistemul de gestiune taxe și impozite
Pentru colectarea unor taxe sunt integrate atât aplicația națională ghișeul.ro cât și serviciul globalpay, fiecare cu atuuri specifice. Ar fi fost ideală utilizarea unui singur sistem dar deocamdată nici unul dintre sisteme nu este suficient de flexibil

Se resimte foarte puternic negativ lipsa acoperirii informatice a proceselor de achiziție publică, a execuției planului anual de achiziții și posibilitatea de urmărire a acestuia în relație cu planificarea bugetară. Această lipsă duce la o dublare a activității de introducere de date, atât la direcția economică, cât și la serviciul achiziții, cu riscuri de introducere greșeli sau de lipsă a unor date.
Lipsește corelarea informatică cu direcția de investiții, astfel încât unele activități trebuie dublate, cum sunt de exemplu cele legate de urmărirea financiară a derulării contractelor cu furnizorii. Se resimte foarte acut lipsa interconectării informaționale între activitățile specifice derulării investițiilor, a derulării achizițiilor și a execuției bugetare, deși toate aceste activități folosesc aceleași informații și datele, inclusiv modificarea acestora, ar trebui să fie accesibile în timp real. Lipsa acestor corelări informaționale cu departamentul proiecte pentru urmărirea realizării achizițiilor și plăților în derularea proiectelor finanțate din bani europeni induce risc semnificativ de întârzieri și discrepanțe care pot conduce la corecturi financiare impuse municipalității. Se resimte ca fiind foarte utilă posibilitatea de a suprapune harta colectării impozitelor cu planurile de urbanism astfel încât să se genereze un suport direct, inclusiv vizual, de analiză privind colectarea taxelor în funcție de zonă
Printre cele mai stringente probleme, frecvent ridicate de către managementul departamentelor din cadrul primăriei de-a lungul timpului dar care încă își așteaptă rezolvarea este asigurarea unui suport adecvat pentru procesul de planificare bugetară, astfel încât necesitățile financiare previzionate de către fiecare departament să poată fi colectate într-un mod unitar, standardizat, în timp scurt, să existe posibilitatea de analiză și aprobare a solicitărilor de bugetare, într-un mod eficient și transparent, și să se poată realiza o consolidare a acestor cereri într-un plan comun care să poată fi apoi urmărit și să se constituie ca suport pentru procesele de achiziție ulterioară, iar departamentele care au generat cererile să poată urmări starea propunerilor lor, inclusiv forma în care acestea au fost aprobate. Din perspectiva impactului și a presiunii interne, acest aspect, digitalizarea procesului de planificare bugetară în relația cu departamentele, este printre cele mai stringente, iar furnizorul actual al sistemelor informatice financiare nu are încă în plan o soluție în acest sens
Ar fi utilă introducerea unui sistem de inventariere bazat pe coduri de bare citibile cu aplicații dedicate, astfel încât să poată fi urmărit mai ușor inventarul, inclusiv localizarea și schimbarea locației unor piese de inventar

Serviciul Achiziții Publice

Nivelul de informatizare este foarte scăzut, fiind limitat la suportul oferit de sistemele informatice din zona financiară pentru gestiunea financiară a contractelor atribuite și corelarea acestora cu facturile primite.
Se resimte ca fiind necesară o mai bună gestiune a contractelor, cu un suport informatic adecvat, pentru a putea corela informațiile pe tot ciclul de viață a relației contractuale, inclusiv de exemplu

pentru a adăuga actele adiționale. Deocamdată contractele sunt înscrise manual într-un registru fizic. Ar trebui să existe o gestiune unitară și complet informatizată, care să permită accesarea informației privind clauzele, cantitățile, valorile, termenele calendaristice de către toate departamentele care trebuie să fie implicate în derularea contractelor, inclusiv a departamentelor care sunt beneficiare sau responsabile de implementare, fiecare pe baza unor drepturi de acces stabilite și controlate.

Redactarea referatelor de necesitate se realizează printr-o abordare tradițională, pe baza unui șablon în Word distribuit departamentelor, care este completat de fiecare solicitor, apoi este printat și transmis în format fizic. Procesul de creare, completare, transmitere, aprobare a referatelor nu este digitalizat, ceea ce duce la neînțelegeri, întârzieri și probleme de exemplu dacă referatele conțin informație incompletă sau insuficient de clară, trebuie să se reia fizic tot parcursul, cei care au generat referatele nu știu care este starea lor, dacă au fost aprobate, în ce stadiu se află la cine sau în ce birou, iar uneori documentele fizice se pot pierde fără a exista o urmă a existenței lor. Se întâmplă foarte frecvent să se trimită înapoi spre compartimente referate care nu sunt completate corespunzător. Ar fi un avantaj major dacă referatele ar fi generate și transmise printr-o aplicație informatică, dar percepția până acum a fost că astfel de aplicații dedicate ar fi costisitoare.

Șefii de departamente și managementul dețin semnături electronice și ar fi posibil ca acest proces să fie digitalizat, inclusiv cu folosirea semnării electronice (oferite de STS), dar deocamdată lipsește un astfel de suport, se poate în cel mai bun caz folosi transmiterea prin email de la o persoană la alta dar acest mecanism nu oferă trasabilitate și certitudine, nu e sigur dacă mailul a ajuns, nu se știe dacă documentul a fost descărcat, procesat și transmis mai departe.

La nivelul personalului există un nivel semnificativ de rezistență la digitalizarea activităților de achiziție, trecerea la o formă digitală de gestiune fiind percepută de unele persoane implicate ca fiind generatoare de efort suplimentar.

Planul anual al achizițiilor este ținut într-un fișier Excel, care nu poate fi partajat între mai multe persoane, este ținut doar de șeful biroului achiziții publice, care colectează de la fiecare coleg informațiile pentru a actualiza PAAP-ul. Pentru evidențierea achizițiilor efectuate se realizează câte un fișier Excel în fiecare săptămână. Nu este nici o corelație informatică între PAAP și datele despre achizițiile realizate.

Nu există posibilitatea urmăririi plăților realizate de către direcția economică pentru achizițiile efectuate. Facturile sunt colectate de la furnizori de către contabilitate, iar compartimentul achiziții le primește ulterior. Ar fi util dacă facturile ar putea fi primite de achiziții și ar putea fi corelate informatic printr-o aplicație cu pozițiile din plan și cu achizițiile efectuate de la furnizori.

Biroul Resurse Umane

Activitatile departamentului sunt partial informatizate prin aplicatia Resum realizata de INDECO.

S-a implementat un sistem de pontaj electronic bazat pe cartele, care include si un sistem de raportare, pentru 21 de locatii fizice ale municipalitatii, inclusiv pentru serviciile care au personalitate juridica proprie. Se mentine in continuare și forma de raportare traditionala bazata pe semnarea olografa a pontajelor. Procesul de pontare ar trebui in viitor unificat intr-o forma complet digitala.

Raman in continuare activitati importante care nu sunt informatizare.

Cererile de concediu se primesc in continuare pe hartie. Gestiunea concediilor se face intr-un fisier Excel pentru luna curenta si se raporteaza doar retroactiv in aplicatia Resum, dupa ce se inchide luna anterioara si se primeste acceptul din partea contabilitatii, astfel incat poate sa existe intarzieri si necorelatii chiar pana in data de 15 a lunii urmatoare.

Gestiunea delegatiilor, incluzand planificarea si raportarea deplasarilor, nu poate fi realizata informatic in timp real si nu se poate tine evidenta disponibilitatii efective a personalului in momentul in care deplasarile se realizeaza ci doar la sfarsitul lunii, cand se introduc retroactiv situatiile privind pontajele in relatie cu ordinele de deplasare.

Documentele se trimit prin email, fluxul documentar al compartimentului nu este inclus in aplicatia de management a fluxului de documente la nivelul primariei.

Ar fi necesar ca toata comunicarea realizata prin documente intre compartimentel institutiei sa se realizeze printr-un sistem unitar de management al documentelor. Utilizarea mailului pentru aceste schimburi nu este optima deoarece nu se poate realiza trasabilitatea, e greu sa se reconstituie schimbul de informatii ulterior, nu se stie cand ajunge informatia la destinatar.

Se resimte a fi foarte utila posibilitatea ca personalul sa isi poata vedea situatia la zi prin accesarea unui sistem informatic, sa poata sa transmita cereri de concedii, sa isi poata vedea salariul, fisa de pontaj, situatia concediului (de exemplu cate zile libere mai are ramase in an). Ar fi foarte util sa se poata gestiona informatic formulare prin care se pot colecta informatii si feedback pe anumite teme din cadrul personalului, sau sa se poata realiza testele necesare pe anumite teme impuse de cadrul legislativ precum protectia muncii sau integritatea.

Ar fi nevoie ca urmarirea instruirii continue a personalului sa poata fi gestionata digital, astfel incat sa poata fi introduse toate studiile, cursurile, certificarile, diplomele obtinute de personal, perioadele de instruire, temele instruirilor, asa incat sa se poata realiza rapoarte rapide si sa se poata face o planificare eficienta. Astfel Dosarul Profesional care ar putea fi tinut electronic intr-un sistem al cupinde atat datele privind activitatile trecute si cele planificate cat si documentele scanate aferente pentru fiecare persoane. Acum dosarul profesional este tinut in fisiere Word, gestiunea este dificila si nu este posibila realizarea de analize, rapoarte si cautari pe grupuri de personal, pe departament sau pe institutie.

Este nevoie de o aplicatie de gestiune a concursurilor, care sa cuprinda toate activitatile legate de derularea concursurilor, de la primirea dosarelor de concurs, verificarea si urmarirea procesului de selectie si evaluare, rezolutiile in urma evaluarilor, comunicarea cu candidatii si

notificarea lor privind rezultatele, respectiv publicarea rezultatelor, fara a necesita efort uman semnificativ ca si pana acum.
Ar trebui ca tot schimbul de informatii specifice resurselor umane in relatia cu institutiile subordonate sa se deruleze printr-un sistem informatic unitar, nu prin email, pentru a se putea asigura trasabilitatea si a putea fi urmarote informatiile, inclusiv de exemplu evidenta usoara unitara la zi a incadrarii personalului in toate subordonatele pentru a se putea verifica usor acoperirea posturilor in relatie cu numarul maxim legal.

Serviciul Juridic şi Evidenţă Documente

Activitatile juridice sunt partial informatizate, printr-o aplicatie furnizata de Indeco, prin care se acopera evidenta cauzelor, litigiilor si gestiunea generala a documentelor.
Comunicarea cu celelalte compartmente se realizeaza in general prin email.
Problema cea mai grava este lipsa unei arhive electronice si trecerea la gestiunea complet electronica a documentelor, intr-un mod centralizat, si prioritar digitizarea arhivei documentare fizice.
Primaria are peste 2000 de metri liniari de documente, volum asupra caruia trebuie realizata o analiza comprehensiva, care nu a fost inca facuta, pentru a determina ce anume este obligatoriu de digitizat conform cadrului de reglementare, respectiv ce ar trebui digitizat din perspectiva oportunitatii. De asemenea va trebui implementata si o evidenta a procedului de arhivare fizica si a procesului de distrugere controlata conform normelor in vigoare.
Trebuie realizata o definire standardizata a ciclului de viata a documentelor care intra sau se genereaza in institutie, in format fizic sau electronic, cu un sistem de etichetare unitar, cu posibilitatea de sortare, filtrare, cautare, alocare in arhiva in functie de caracteristici specifice, care de asemenea trebuie sa fie definite.
Rezolvarea acestei probleme privind arhiva este stringenta si trebuie sa fie prioritara.
Deocamdata in cadrul serviciului activeaza trei persoane specializate ca arhivar, tin evidenta exclusiv in fisiere Word si Excel si folosesc sistemul de circuit al documentelor implementat in primarie. In fiecare an se adauga peste 120.000 de documente care intra intr-un fel sau altul sau sunt create in institutie, crescand permanent complexitatea si dificultatile de gestiune a arhivei.

Direcţia Patrimoniu

Un interes special este acordat gestiunii celor peste 10.000 de parcari de resedinta, alaturi de cele 1.200 de parcari cu plata din zona centrala.
Gestiunea parcarilor de resedinta este gestionata prin doua aplicatii distincte, Gecon (oferit de Indeco), prin care se urmaresc platile, si Sybit, prin care se identifica locurile de parcare libere nealocate si neplatite, pe baza unei harti interactive.

Fluxul functional este in continuare nefinalizat deoarece lipseste posibilitatea de selectare si rezervare a locului de parcare, desi din punct de vedere tehnic aceasta functie este dezvoltata, insa nu este data in folosinta deoarece trebuie proiectat un flux de lucru care sa nu discrimineze intre cetatenii care completeaza cererile online sau in persoana la primarie si sa evite eventuale riscuri de desincronizare a celor doua moduri de lucru.
Ar fi necesara digitalizarea unitara a eliberarii chitantelor si autorizatiilor emise, inclusiv cu stocarea lor automata in arhiva electronica (deocamdata inexistenta), astfel incat sa se poata realiza interogari si verificari in relatie cu persoana fizica sau juridica platitoare.
Documentele generate ar putea fi eliberate electronic, semnate electronic cu sigiliul institutiei, directia fiind pregatita in acest sens deoarece detine 5.000 de semnaturi de tip sigiliu, achizitionate de la compania Certsign. Este insa nevoie de implementarea unui flux informatic de gestiune a acestor documente, ideal conectat direct in viitoarea aplicatie de arhiva electronica.
Deocamdata, se foloseste un registru fizic de intrari-iesiri, pe hartie, cu semnaturi olografe.
Semnaturile sigiliu sunt folosite deocamdata pentru eliberarea certificatelor fiscale in format electronic. Acest mecanism se poate extinde in viitor si pentru a te servicii oferite cetatenilor.

Secretar general

Este necesara digitalizarea unitara a gestiunii nomenclaturii stradale si a relatiei acesteia cu evidenta populatiei. Este nevoie de o evidenta informatica care sa permita verificari diverse, cum ar fi de exemplu numarul de kilometri ai tramei stradale, inclusiv numarul de strazi private, gestiunea unitara a populatiei celor 22 de comune arondate, posibilitatea de localizare rapida pe baza de nume de strada si numar.

Nivelul de interoperabilitate intre sistemele din cazul primariei este foarte scazut, ceea ce duce la obligarea cetateanului de a duce informatii si documente intre un compartiment si altul, in loc ca personalul din structura institutiei sa poata accesa si reutiliza informatia. Acest lucru se resimte in relatia cu registrul agricol, cu utilitatile, cu urbanismul.

Nu au mai fost realizate de foarte mult timp programe de instruire a personalului pentru utilizarea eficienta a calculatorului, a internetului si a aplicatiilor cum ar fi suita de tip office, browserele web, sistemele de teleconferinta si alte aplicatii uzuale utile, si respectiv utilizarea si aplicarea semnaturilor electronice. Aceasta lipsa face ca personalul sa nu fie uniform instruit, sa existe lacune semnificative in abilitatile de lucru cu instrumente digitale, situatie care duce la scadere de performanta, timpi indelungati in realizarea unor sarcini si riscuri, inclusiv legate de securitatea cibernetica.

La nivelul primariei ar trebui sa existe posibilitatea acordata unor roluri cu responsabilitate larga, cum ar fi secretarul general, primarul, administratorul public, de a accesa si vizualiza rapid informatii relevante care se colecteaza si genereaza, eventual sub forma unor tablouri de bord care sa sprijine si luarea unor decizii. Printre cele mai importante informatii care ar trebui sa poata fi accesate astfel, dar deocamdata nu este posibil, sunt documentele depuse de cetean incluzand petitiile si termenele de rezolvare ale lor, planul achizitiilor publice incluzand detaliile cantitative si valorice pentru fiecare pozitie si situatia realizarii achizitiilor, inclusiv situatia calendarelor de derulare a procedurilor competitive si a termenelor actiunilor impuse conform legii pentru a se genera avertizari si a se preveni depasirea termenelor legale. De ademenea este nevoie de un sistem de urmarire a executiei lucrarilor contractate si de administrare a receptiilor. Este nevoie de un sistem integrat de management al investitiilor, incepand de la tema de proiectare, continutul caietului de sarcini, atribuirea lucrarii, gestiunea contractului, raportarile in cursul implementarii, si gestiunea electronica a cartii constructiei pentru fiecare lucrare realizata, respectiv fiecare obiectiv de investitie aflat in gestiunea institutiei.

Lipseste o gestiune unitara informatica a serviciilor publice, a starii retelelor, a lucrarilor efectuate si planificate. Acestea ar trebui sa fie disponibile in mod unitar.

Ar fi foarte utila implementarea unui sistem de urmarire a neconformitatilor urbane, incluzand un sistem de management al incidentelor cu un mecanism de raportare care sa fie disponibil cetatenilor, si de asemenea de gestiune a problemelor urbane care trebuie rezolvate si care sunt identificate si urmarite de catre personalul institutiei.

Serviciul Audit Intern

Activitatea este foarte slab informatizata, folosind sistemul de circuit intern al doccumentelor doar pentru a inregistra documentele finale ale rapoartelor de audit.
Pe de o parte activitatea efectiva de planificare, executie si raportare in cadrul proceselor de audit nu este digitalizata, pe de alta parte eficienta acestor activitati este mult redusa de lipsa accesibilitatii informatiei primare relevante, intr-o forma electronica, auditabila direct.
Următoarele activități ar beneficia semnificativ de informatizare:

- Procesul de evaluare a riscurilor, incluzand analiza de impact si probabilitatea de aparitie, pe o scara de la 1 la 3, cu posibilitatea de generare a matricii riscurilor pentru fiecare proiect de audit

- Urmarirea informatica a intregului flux de audit, cu posibilitatea adaugarii direct in aplicatia de gestiune a auditului a documentelor de lucru si corelarea acestora cu obiectivele si activitatile proiectului de audit.

- Gestiunea dosarelor permanente pentru fiecare structura auditata si gestiunea corelata a tuturor dosarelor de audit rezultate din proiectele de audit distincte realizare in relatie cu respectiva structura organizationala

- Circuit complet al documentelor care sa permita auditabilitatea ciclului de viata a fiecarui document, prin interograrea specifica pe baza de tip de document, numar de exemplare, destinatia documentului, unde se arhiveaza, cine le intocmeste, cine le avizeaza, cine le aproba.

- Accesibilitatea informatica a informatiilor economice, legate de planificarea si executia bugetara, contabilitate, planificarea si executia achizitiilor. Acest lucru se poate realiza inclusiv prin alocarea unor drepturi pentru un tip de utilizator special (de tip auditor) in sistemele deja existente, si trebuie avute in vedere pentru sistemele care vor fi implementate in viitor. In acest moment, orice informatie economica se transmite in format fizic sau scanat, cu intarziere mare, ceea ce extinde foarte mult calendarul proceselor de audit si induce riscuri semnificative legate de lipsa corelarii informatiei, de completitudinea acesteia sau inclusiv de greseli umane de transcriere a valorilor economice. Pentru achizitiile publice, trebuie asigurat accesul la dosarul electronic al fiecarei achizitii, treubie sa se poata verifica in mod complet cine a generat o informatie sau un document, cine a aprobat, cine si cand a modificat o informatie.

- In relatia cu activitatile de urbanism, nu exista trasabilitate privind procesul de emitere a autorizatiilor de constructie, incluzand activitatile realizate in cadrul primariei si momentele in care acestea au avut loc.

Din cauza lipsei accesului la informatii si a lipsei digitalizarii si trasabilitatii informatice serviciul de audit poate in fapt sa realizeze doar circa 30% din toate misiunile pe care nominal ar trebui sa le realizeze in cursul unui an calendaristic, reducand foarte mult eficienta proceselor de audit, capacitatea de urmarire a implementarii masurilor evidentiate prin rapoartele de audit si posibilitatea ca aceste activitati sa aiba impactul pozitiv scontat.

Analiza SWOT a digitalizării Primăriei Municipiului Bistrița

Puncte tari	Puncte slabe
• Digitalizarea este considerată o prioritate de către conducerea instituției. Digitalizarea, asigurarea securității cibernetice, educația digitală a personalului beneficiază de suport managerial; • Se derulează în mod consecvent proiecte care vizează digitalizarea unor activități și situația se îmbunătățește continuu • La nivelul conducerii departamentelor și serviciilor există deschidere și susținere pentru accelerarea informatizării și se manifestă un nivel bun de proactivitate prin contribuția cu idei privind prioritățile de digitalizare și modul concret în care aplicațiile viitoare ar trebui să funcționeze	• Nu exista ghiduri, arhitecturi și modele la nivel național aplicabile direct pentru transformarea digitală a administrației, astfel încât Municipiul Bistrița trebuie să identifice și să aplice propria abordare; • Nivelul actual de digitalizare și interoperabilitatea sistemelor din cadrul Primăriei Municipiului Bistrița este scăzut. Sistemele actuale trebuie extinse; • Nivelul actual de pregătire a personalului per ansamblu pentru utilizarea instrumentelor digitale și pentru asigurarea securității cibernetice este redus
Oportunități	**Amenințări**
• Disponibilitatea fondurilor accesibile pentru implementarea proiectelor de transformare digitală a administrației; • Context european favorabil, care susține necesitatea și oportunitatea digitalizării administrației publice, inclusiv prin obligarea guvernelor țărilor membre să implementeze proiecte suport (de exemplu Punctul de Contact Unic Electronic);	• Digitalizarea trebuie continuată într-o manieră sistematică și coordonată, pentru a asigura informatizarea completă, interoperabilitatea și posibilitatea susținerii principiului „o singură dată” (once-only), care precizează că o informație furnizată o dată de către cetățean trebuie să fie reutilizată direct de către orice alt serviciu din cadrul Primăriei Municipiului Bistrița fără a i se solicita cetățeanului acea informație încă o dată. În lipsa unei coordonări coerente, efectele digitalizării vor fi sub optimal; • Pregătirea și implementarea proiectelor trebuie să urmeze un set de reguli și ghiduri, privind asigurarea drepturilor de exploatare și evitarea situației de client captiv;

Linii Prioritare De Acțiune

În vederea sprijinirii procesului de transformare evolutivă, identificăm următoarele linii majore de acțiune:

- Identificarea proiectelor noi care ar trebui implementate pentru a asigura optimizarea prin digitalizare a instituției și a relației cu cetățenii;
- Identificarea îmbunătățirilor care trebuie aduse sistemelor informatice existente pentru o mai bună acoperire a activității, pentru asigurarea interoperabilității, a accesului la informații, a unui nivel sporit de utilitate pentru cetățeni și funcționari;
- Identificarea unor măsuri, proceduri, programe care sunt de natură să îmbunătățească procesele de implementare, exploatare, mentenanță sau înlocuire a sistemelor informatice, să reducă riscurile de securitate, de captivitate față de furnizor sau de pierderi și corecții financiare.

Prin analiza realizată, au fost identificate proiectele de digitalizare a activității Primăriei Municipiului Bistrița și a interacțiunii dintre instituție și cetățeni, prioritizate după cum urmează:

- Sistem informatic de planificare bugetară pentru a asigura participarea tuturor compartimentelor, colectarea necesităților, trasabilitatea procesului de aprobare, consolidarea planului bugetar
- Implementarea arhivei electronice, digitizarea arhivei fizice, asigurarea gestiunii complete și standardizate a documentelor, atât a celor deja existente cât și a celor viitoare, cu asigurarea posibilităților de căutare, filtrare, sortare, corelare, auditare a operațiilor realizate pe aceste documente (cine și când a generat, aprobat, actualizat, transmis fiecare document)
- Reimplementarea întregii suite de aplicații aferente activității economice, resurselor umane, registraturii, sub forma unui sistem web cu componente integrate și cu informație structurată standardizată și accesibilă tuturor celor care trebuie să o utilizeze
- Implementarea unui sistem unitar de management a proceselor de achiziție, cu focus pe gestiunea planului anual al achizițiilor publice, în forma unei aplicații web accesibile tuturor celor care au nevoie de informații, inclusiv serviciului de audit intern, asigurând standardizarea modului în care se colectează referatele de necesitate, a aprobării lor, a dialogului cu compartimentele pentru completarea sau corectarea referatelor, a urmăririi

execuției achizițiilor, a gestiunii contractelor după atribuire și a corelării cu facturile primite de la furnizori

- Implementarea unui sistem de gestiune și urmărire a implementării investițiilor, integrat cu activitățile de achiziție, incluzând managementul tuturor activităților pornind de la planificare, realizarea caietelor de sarcini, atribuire, gestiunea contractelor de lucrări, urmărirea recepțiilor, urmărirea garanțiilor, consolidarea informației în cartea constructiei

- Extinderea aplicațiilor pentru resurse umane sau implemetarea unei aplicații noi care să asigure în mod integrat susținerea tuturor activităților, inclusiv gestiunea concediilor, gestiunea delegațiilor, gestiunea învățării continue, gestiunea concursurilor

- Sistem informatic de gestiune a proceselor de audit intern, incluzând toate activitățile, inclusiv planificarea, realizarea rapoartelor, urmărirea implementării rapoartelor

- Implementarea unui sistem de inventariere bazat pe coduri de bare și incluzând verificarea și actualizarea periodică a locației obiectelor de inventar

- Realizarea înregistrării directe bazată pe harta interactivă a rezervării locului de parcare și a depunerii actelor, pe baza unei proceduri care să evite defavorizarea persoanelor care nu au abilități sau posibilități în a utiliza sistemul informatic

- Extinderea eliberării documentelor în format electornic cu sigiliul electronic al instituției, inclusiv prin integrarea realizării semnăturilor la nivel de server

- Program general de instruire continua si periodica a personalului pentru îmbunătățirea abilităților de lucru cu sistemele informatice și dezvoltarea capacității de prevenție a pericolelor legate de securitatea cibernetică

IX Analiză şi diagnostic privind stadiul actual al infrastructurii IT din Primăria Municipiului Bistrița

Rolul acestei analize este oglindirea cât mai fidelă a realității în vederea facilitării unor decizii manageriale raționale, bazate pe fapte. Situația generală a infrastructurii IT a primăriei Bistrița este relativ precară în acest moment: chiar dacă sistemul a funcționat până în prezent cu defecțiuni punctuale, apariția oricărei defecțiuni majore va duce la o serie de reacții în cascadă care vor rezulta în indisponibilitatea serviciilor pentru o perioadă de timp cuprinsă între ore sau săptămâni, în funcție de componentele infrastructurii IT afectate și de scenariul analizat.

Analiza inițială a relevat lipsa unei strategii coerente de investiții în infrastructura IT și a unei strategii de utilizare a infrastructurii IT definită de ținte / nevoi de business pe termen mediu și lung. Infrastructura IT a primăriei Bistrița are în compoziția sa atât echipamente perimate din punct de vedere tehnic, cât și echipamente la zi, dar care nu sunt armonizate în infrastructura globală.

Mecanismele și cauzele fundamentale care au dus la prezenta situație pot fi rezumate succint: alocarea sarcinii de a proiecta, implementa și administra & efectua mentenanță unui departament intern sufocat deja de activități zilnice diverse. De asemenea, subfinanțarea departamentului a creat premisele dezvoltării unor sisteme și soluții pe bază de software gratis (i.e. de tip open source) si fără suport. Subdimensionarea departamentului IT intern a condus la prioritizarea deciziilor pe termen scurt ceea ce a favorizat puternic soluționarea ad-hoc a problemelor legate de IT. Majoritatea soluțiilor IT implementate se opresc la nivel de minimă funcționalitate, cu lacune seriose în documentare, stimulate de apariția perpetuă a unor situații noi care reclamau atenția personalului IT.

În plus, această abordare a condus la încorporarea în infrastructura IT a primăriei Bistrița a unor soluții tehnice foarte diverse. În contextul administrării și mentenanței unei infrastructuri IT, diversitatea soluțiilor tehnice nu este un avantaj, ci este o piedică semnificativă, dată fiind complexitatea suplimentară introdusă de nevoia de a se sincroniza soluții tehnice care au limitări sau care nu se suprapun și ale căror ciclu de viață și de mentenanță sunt distincte. Toate considerentele menționate au rezultat gradual în agilitate scăzută și risc crescut.

Recomandarea de bază a echipei CLUJ IT este migrarea aplicațiilor critice pe o infrastructura cloud moderna într-un centru de date modern în cadrul primăriei Bistrița sau la un furnizor specializat în astfel de servicii.

Activitățiile fundamentale de administrare & mentenanță IT pot fi efectuate de către departamentul IT al primăriei Bistrița, anumite activități din cadrul mentenanței putând fi externalizate către un furnizor (ales în baza unor criterii clare și având niște ținte de peformanță măsurabile, stipulate clar în contract). În acest context menționăm diferența dintre focalizarea anterioară pe reducerea costurilor și focalizarea recomandată în strategia prezentă pe prevenția costurilor evitabile.

Recomandăm ca în cel mai scurt timp să se realizeze investițiile necesare în infrastructura critică cuplate cu achiziționarea serviciilor de suport de la furnizorii agreați și asigurarea creșterii resursei umane (i.e. personal calificat care să aibă expertiza necesară, dar și timpul necesar pentru a le putea întreține).

În final, reiterăm că situația relevată de analiză indică faptul că abordarea prezentă în cadrul instituției este deficitară. Reexaminarea principiilor de bază și a valorilor care fundamentează strategia IT trebuie să constituie punctul de plecare în revitalizarea infrastructurii IT.

X. Diagnoza privind vulnerabilitatea din punctul de vedere al securității cibernetice

1. Situația actuală

Sistemul de securitate cibernetică din Primăria Bistrița prezintă atât puncte forte, cât și zone de îmbunătățit.

În ceea ce privește utilizarea acceptabilă a sistemelor informaționale, există proceduri de utilizare a stațiilor de lucru și modalități de acces stabilit, precum și soluții antivirus pentru serverele Windows. Cu toate acestea, aceste proceduri nu sunt întotdeauna aplicate corect de către personalul din Primărie.

De asemenea, există 5 mașini fizice suport pentru procesele de virtualizare care folosesc ca sistem de operare platforma de virtualizare Proxmox; pe aceste mașini suport funcționează un număr de aproximativ 30 mașini virtuale, majoritatea cu sistem de operare Windows Server dar și cu sisteme de operare Linux, mașini virtuale care asigură servicii precum: poșta electronică, consola de securitate antivirus, aplicații dedicate – gestiunea documentelor, portalul WEB și serviciile electronice, aplicațiile de contabilitate, etc.

În ceea ce privește managementul conturilor, acesta nu este realizat prin intermediul unui sistem Active Directory pentru sistemul de operare Windows, din cauza barierei reprezentate de personalul din compartimentele instituției (această soluție ar introduce restricții și reguli noi) și a lipsei de capacitate de administrare din partea compartimentului de specialitate subdimensionat pînă în luna septembrie 2022. Instalarea acestui sistem este planificată probabil pentru anul viitor.

În ceea ce privește soluțiile antivirus, sunt prezente pe toate stațiile de lucru), iar accesul cu memory stick-uri și CD-ROM-uri este restricționat. De asemenea, rezistența umană la respectarea regulilor stricte și lipsa unei intervenții efective în cazul detectării malware prin intermediul consolei ESET reprezintă probleme în implementarea acestor soluții.

Politica de utilizare și securitate acceptabilă a dispozitivelor mobile deținute nu există în prezent, iar aparatele mobile și laptop-urile nu mai ajung la departamentul de IT pentru instalare antivirus. De asemenea, nu există politici interne în acest sens, însă există soluții precum Knox oferite de Orange pentru mobile.

Politica de birou curat nu este clar definită prin proceduri și reguli interne, existând abateri privind afișarea parolelor la loc vizibil și transmiterea acestora între angajați. Angajații nu sunt conștienți de riscul la care expun sistemele din Primărie prin ignorarea regulilor de securitate a accesului la date.

Politica de servicii electronice pentru cetățeni se bazează pe 2 mașini virtuale Linux și o mașină virtuală Windows Server pe care rulează aplicația de impozite și taxe, administrate de către furnizorul INDECO, care oferă soluții de servicii către cetățeni.

Politica de e-mail se bazează pe o soluție ”open source” Zimbra, care oferă backup automat. Până în prezent, nu a fost necesară cumpărarea de licențe. E-mail-urile sunt utilizate pe baza unei adrese instituționale, evitându-se utilizarea adreselor personale. Există 464 de casete de e-mail și autentificarea se realizează prin intermediul unui sistem cu doi factori.

În ceea ce privește politica de firewall se bazează în principal pe o soluție router dedicat SonicWALL NSA 3700 precum și un router de backup. Acesta livrează ultimele alerte în cazul atacurilor cibernetice.

Remarcabil este faptul că Primăria municipiului Bistrița este conectată la rețeaua națională de date operată de STS prin intermediul a patru conexiuni de fibră optică care conectează centrul de date al primăriei cu centrul de date din municipiu al STS.

Este important să se asigure o gestionare adecvată a hardware-ului și suporturilor electronice la sfârșitul vieții lor în utilizare. Schimbarea anuală a 10% din parcul de calculatoare este o abordare adecvată pentru menținerea sistemelor actualizate și în siguranță. Backup-ul în caz de incidente poate ajuta la protejarea informațiilor importante. Distrugerea fizică a hardware-ului și suporturilor electronice după casare este esențială pentru protejarea informațiilor confidențiale și pentru prevenirea accesului neautorizat. Formatarea hardware-ului înainte de distrugere poate ajuta la eliminarea completă a informațiilor stocate.

Disponibilitatea unui centru de date pentru backup poate ajuta la gestionarea incidentelor de securitate, dar este important să se dezvolte și să se implementeze proceduri adecvate de răspuns la incidente pentru a se asigura că toate problemele sunt abordate într-un mod eficient și coordonat.

Recepția la nivel de instituții subordonate poate crea probleme privind controlul și managementul centralizat al achizițiilor în tehnologia informației. Este important să se dezvolte o formă centralizată de achiziție și recepție pentru a se asigura că toate achizițiile sunt efectuate în mod adecvat și conform cu regulile și procedurile de securitate. Interesele diverșilor factori pot crea bariere în administrarea adecvată a achizițiilor IT și este important să se acorde o atenție suplimentară acestei probleme.

În cadrul celor 21 de imobile analizate, 19 dintre ele beneficiază de servicii de intranet, în timp ce 2 imobile sunt considerate nesemnificative. Conectarea la Internet se realizează prin intermediul unui centru de date central. Aproximativ 70% din conexiunile de calculatoare sunt asigurate prin fibra optică a Primăriei, în timp ce restul de 30% folosesc fibră optică închiriată. Accesul la Internet este restricționat pentru anumite țări, precum China și Rusia, iar accesul la filme este, de asemenea, limitat. Cookie-urile reprezintă o sursă potențială de malware, iar configurarea corectă a browserelor este esențială pentru a preveni riscurile de securitate. Se estimează că 50% din traficul de date este rezultatul descărcărilor.

În prezent, nu există reguli scrise privind gestionarea jurnalelor de log. Acestea sunt păstrate doar când este posibil, în special pe routere. Log-urile nu se regăsesc pe stațiile de lucru, dar sunt disponibile pentru suportul de virtualizare. În ceea ce privește sistemele noi, este nevoie de o politică de securitate și de formalizarea protocoalelor pentru a asigura o gestionare adecvată a log-urilor.

Nu există o semnătură de confidențialitate și nici măsuri de păstrare în siguranță a datelor membrilor. Datele se regăsesc la liber pe stațiile de lucru și pot fi exportate, ceea ce crește riscul de scurgeri de date (ex. GIS).

Nu există un VPN implementat, deși acesta ar fi necesar pentru a facilita tele-munca. O soluție de Open VPN ar permite două conexiuni simultane.

Dispozitivele personale pot fi conectate la Wi-Fi-ul securizat al organizației. Conexiunea este permisă doar pentru laptopuri și telefoane mobile.

Parolele se schimbă la intervale de 3 luni și trebuie să conțină între 8 și 12 caractere. Totuși, în prezent, nu există o soluție de protecție a parolelor implementată în organizație.

Monitorizarea poștei electronice este o măsură importantă de securitate. Implementarea unei politici de centralizare a upgrade-urilor pentru sistemul Office, folosind un server Microsoft, ar consolida securitatea și ar facilita managementul actualizărilor.

Pentru a proteja împotriva accesului neautorizat, este esențial să se asigure controlul accesului fizic prin camere video, sisteme de control al accesului și dispozitive de recunoaștere a amprentelor.

Fără un server de fișiere, este important să se considere adoptarea soluțiilor cloud computing. Utilizarea Nextcloud și a Office în departamentul de IT, împreună cu o rețea de centre de date pentru interoperabilitate și stocare de 4T și SSD, poate aduce beneficii de securitate și eficiență operațională.

Este crucial să se asigure securitatea serverului prin aplicarea unor politici și protocoale de securitate riguroase, precum și actualizarea constantă a sistemelor și aplicarea patch-urilor de securitate.

O politică de utilizare acceptabilă a rețelelor sociale ar trebui să fie implementată pentru a preveni abuzurile și potențialele riscuri de securitate. O politică de atenționare ar trebui să fie dezvoltată pentru a informa angajații despre riscurile asociate cu utilizarea rețelelor sociale.

Monitorizarea zilnică a centrului de date este esențială, dar trebuie să se efectueze și audituri regulate pe stațiile de lucru pentru a identifica și remedia eventualele probleme de securitate.

În loc de o abordare oportunistă, este important să se dezvolte și să se implementeze o practică de evaluare a vulnerabilităților atât pentru echipamente, cât și pentru sisteme. Acest lucru va permite identificarea și remedierea rapidă a punctelor slabe.

Este important ca Primăria să colaboreze îndeaproape cu firma INDECO pentru a se asigura că securitatea și funcționarea site-ului web sunt optimizate. Un raport lunar poate ajuta la monitorizarea performanței și a securității site-ului.

Implementarea unei politici de securitate pentru configurarea stațiilor de lucru și actualizarea periodică a acesteia este crucială pentru a preveni vulnerabilitățile și riscurile de securitate.

Este important să se mențină o rețea Wi-Fi securizată și să se monitorizeze în mod constant performanța și securitatea acesteia. Implementarea unor protocoale de criptare și autentificare puternice poate contribui la protejarea rețelei wireless împotriva accesului neautorizat și a atacurilor cibernetice.

În cazul în care telecommuting devine o opțiune pentru angajați, trebuie să se dezvolte și să se implementeze o politică adecvată pentru a asigura securitatea datelor și a informațiilor atunci când se lucrează de la distanță.

Dacă se adoptă tehnologia IoT în viitor, este crucial să se evalueze și să se abordeze riscurile de securitate specifice asociate cu utilizarea dispozitivelor IoT conectate în rețea.

Este esențial să se dezvolte și să se furnizeze instruire în domeniul securității cibernetice pentru personal, pentru a crește conștientizarea și a recunoaște diferite tipuri de atacuri cibernetice.

Verificarea periodică a securității și performanței serverului virtualizat este esențială pentru a preveni vulnerabilitățile și pentru a asigura disponibilitatea constantă a resurselor. Implementarea unor politici și protocoale de securitate adecvate, precum și monitorizarea activității serverelor virtualizate, va contribui la menținerea unui mediu sigur și eficient pentru operațiunile organizației.

În cazul în care se adoptă soluții de cloud computing, trebuie să se dezvolte și să se implementeze o politică de securitate adecvată pentru a proteja datele și informațiile stocate în cloud.

De asemenea, este important să se adopte o politică de securitate a informațiilor și să se obțină certificări precum ISO 27001 pentru a asigura respectarea standardelor internaționale în materie de protecție a datelor și a informațiilor confidențiale.

Din perspectiva celor mai bune practici de securitate cibernetică, există mai multe puncte slabe în sistemul de securitate cibernetică din Primăria Bistrița. Acestea includ:

1. Managementul conturilor - Nu există implementarea unui sistem de management al conturilor prin intermediul Active Directory, ceea ce poate crește riscul de acces neautorizat și de compromitere a conturilor (notă: Active Directory (AD) este un serviciu de director de rețea dezvoltat de Microsoft, care oferă funcții de gestionare a identității și a accesului într-o rețea. Active Directory este utilizat pentru a gestiona utilizatorii, grupurile, computerele și alte obiecte într-o rețea, precum și pentru a controla accesul la resursele din rețea, cum ar fi aplicațiile și fișierele. Active Directory permite administrarea centralizată a identităților și a accesului într-o rețea, ceea ce poate crește eficiența și securitatea.)
2. Politica de utilizare și securitate acceptabilă a dispozitivelor mobile - Lipsește o politică clară și un sistem de protecție antivirus pentru dispozitivele mobile, ceea ce poate duce la compromiterea acestora prin intermediul malware-ului sau a atacurilor cibernetice.
3. Politica de birou curat - Lipsește o politică clară privind regulile de securitate și procedurile pentru un birou curat, ceea ce poate duce la compromiterea sistemelor prin intermediul accesului neautorizat sau a afișării parolelor la loc vizibil.
4. Accesibilitatea serviciilor electronice - Serviciile electronice oferite cetățenilor sunt în administrarea partajată între furnizorul acestor soluții și compartimentul de specialitate al primăriei, ceea ce poate conduce la apariția unor probleme privind accesibilitatea și utilizarea acestora.
5. Protecția firewall - Deși există un router dedicat care deservește firewall-ul și un router de backup, acestea pot fi compromise prin intermediul atacurilor cibernetice, ceea ce poate duce la probleme privind securitatea sistemelor. Este critic să se implementeze soluții robuste de securitate pentru a proteja firewall-ul și router-ul de backup împotriva amenințărilor cibernetice. Acest lucru poate fi realizat prin intermediul unor măsuri precum implementarea unei soluții anti-malware, configurarea setărilor firewall-ului pentru a bloca accesul neautorizat, monitorizarea constantă a activităților din rețea și realizarea de backup-uri regulate ale sistemelor. Prin implementarea acestor soluții de securitate puternice, se poate asigura protecția sistemelor și siguranța informațiilor.

6. Gestionarea hardware-ului și a suporturilor electronice: Este esențial să se implementeze proceduri stricte de eliminare a echipamentelor vechi și a dispozitivelor de stocare. Un proces clar de distrugere a datelor și a echipamentelor ar reduce riscul de scurgeri de date și acces neautorizat.
7. Backup și răspuns la incidente: Este crucial să se dezvolte și să se implementeze proceduri de răspuns la incidente și să se asigure backup-uri regulate ale datelor pentru a proteja informațiile importante și a menține continuitatea afacerii.
8. Controlul și managementul centralizat al achizițiilor în tehnologia informației: Dezvoltarea unei strategii centralizate de achiziție și recepție poate preveni utilizarea neadecvată a echipamentelor și a resurselor IT.
9. Gestionarea accesului la Internet și securitatea browserelor: Implementarea de politici de securitate și monitorizarea traficului web poate reduce riscul de malware și alte amenințări cibernetice. De asemenea, este esențial să se asigure că toate browser-urile sunt configurate în mod corespunzător.
10. Gestionarea jurnalelor (log-urilor): Dezvoltarea și implementarea unei politici de gestionare a jurnalelor de log pentru toate sistemele și dispozitivele, inclusiv stațiile de lucru, poate ajuta la identificarea și soluționarea problemelor de securitate în timp util.
11. Protejarea informațiilor confidențiale ale membrilor: Implementarea măsurilor de securitate, precum criptarea datelor și restricționarea accesului la informații sensibile, poate reduce riscul de scurgeri de date.
12. Implementarea unui VPN: Implementarea unui VPN securizat și stabil este esențială pentru a asigura confidențialitatea și integritatea datelor în cazul tele-muncii.
13. Securitatea dispozitivelor personale (BYOD): Dezvoltarea și implementarea unei politici clare de securitate pentru dispozitivele personale conectate la rețea poate reduce riscurile de securitate asociate cu utilizarea acestora.
14. Gestionarea parolelor: Implementarea unei soluții de gestionare a parolelor, precum un sistem de management al parolelor, poate crește securitatea și reduce riscul de acces neautorizat. De asemenea, politici de securitate mai stricte privind lungimea și complexitatea parolelor sunt recomandate.
15. Lipsa unei politici de centralizare a upgrade-urilor pentru sistemul Office, care poate crea incoerențe în securitate și poate expune organizația la riscuri.
16. Insuficiența măsurilor de control al accesului fizic, care poate permite accesul neautorizat la echipamente și date sensibile.
17. Absența unui server de fișiere sau a unei soluții de cloud computing, care poate cauza probleme de stocare, accesibilitate și securitate a datelor.
18. Lipsa auditurilor pe stațiile de lucru, care poate duce la neidentificarea vulnerabilităților sau a problemelor de securitate.
19. Abordarea oportunistă în evaluarea vulnerabilităților, în locul unei practici de testare și evaluare sistematică și riguroasă.
20. Lipsa unei politici de utilizare acceptabilă a rețelelor sociale și a unei politici de atenționare, care poate crește riscul de abuz și de probleme de securitate asociate cu utilizarea rețelelor sociale.
21. Absența instruirii personalului în domeniul securității cibernetice, ceea ce reduce conștientizarea și capacitatea de a recunoaște și preveni atacuri cibernetice.
22. Lipsa unei politici de securitate cloud computing și a unei politici de securitate a informațiilor, precum și absența certificării ISO 27001, care arată o posibilă lipsă de conformitate cu standardele internaționale în materie de protecție a datelor și a informațiilor confidențiale.

2. Analiza SWOT

Analiza SWOT detaliată pentru Primăria Bistrița în problema securității cibernetice:

Puncte forte (Strengths):

1. Proceduri de utilizare a stațiilor de lucru și modalități de acces stabilite.
2. Soluții antivirus pentru serverele Windows.
3. Circa 30 mașini virtuale protejate prin sistemantivirus și firewall pe 5 mașini suport de virtualizare cu sistem de operare Linux (Proxmox).
4. Existența și utilizarea a 8 domenii înregistrate pe Primăria municipiului Bistrița care permit o adresare instituțională pentru servicii precum e-mail, WEB, etc.
5. Firewall asigurat de echipament de tip router dedicat și router de backup.
6. 70% din conexiunile de calculatoare asigurate prin fibra optică a Primăriei.
7. Accesul restricționat la internet pentru anumite țări și limitarea accesului la filme.

Puncte slabe (Weaknesses):

1. Necorespunzătoarea aplicare a procedurilor de utilizare a stațiilor de lucru de către personal.
2. Lipsa unui sistem Active Directory pentru managementul conturilor.
3. Rezistența umană la respectarea regulilor stricte și lipsa unei intervenții efective în cazul detectării malware.
4. Lipsa unei politici de utilizare și securitate acceptabilă a dispozitivelor mobile.
5. Politica de birou curat nu este clar definită și există abateri privind gestionarea parolelor.
6. Lipsa regulilor scrise privind gestionarea jurnalelor de log.
7. Lipsa unei semnături de confidențialitate și măsuri de păstrare în siguranță a datelor membrilor.
8. Fără VPN implementat, în ciuda nevoii pentru facilitarea tele-muncii.
9. Lipsa unei soluții de protecție a parolelor implementată în organizație.
10. Utilizarea dispozitivelor personale conectate la Wi-Fi-ul securizat al organizației.
11. Lipsa unei politici de utilizare acceptabilă a rețelelor sociale.

Amenințări (Threats):

1. Rezistența umană la respectarea regulilor stricte de securitate și lipsa unei intervenții efective în cazul detectării malware.
2. Lipsa unei politici de utilizare și securitate acceptabilă a dispozitivelor mobile.
3. Riscul la care expun sistemele din Primărie prin ignorarea regulilor de securitate a accesului la date de către angajați.
4. Scurgeri de date din cauza lipsei de măsuri de păstrare în siguranță a datelor membrilor.
5. Lipsa unui VPN implementat, care ar putea expune organizația la atacuri cibernetice.
6. Accesul dispozitivelor personale la Wi-Fi-ul securizat al organizației, care ar putea permite intruziunile în rețea.
7. Lipsa unei soluții de protecție a parolelor implementată în organizație.
8. Cookie-urile care reprezintă o sursă potențială de malware.
9. Riscurile asociate cu utilizarea rețelelor sociale în absența unei politici de utilizare acceptabilă.
10. Vulnerabilități și riscuri de securitate datorate lipsei unei politici de securitate pentru configurarea stațiilor de lucru și actualizarea periodică a acesteia.

11. Riscurile de securitate specifice asociate cu utilizarea dispozitivelor IoT conectate în rețea, în cazul în care acestea sunt adoptate în viitor.

Oportunități (Opportunities):

1. Implementarea unui sistem Active Directory pentru sistemul de operare Windows, care ar îmbunătăți managementul conturilor.
2. Dezvoltarea unei politici de utilizare și securitate acceptabilă a dispozitivelor mobile, pentru a proteja informațiile și a preveni riscurile de securitate.
3. Implementarea unui VPN pentru a facilita tele-munca și a securiza conexiunile la distanță.
4. Dezvoltarea și implementarea unei politici de utilizare acceptabilă a rețelelor sociale pentru a preveni abuzurile și potențialele riscuri de securitate.
5. Implementarea unor protocoale de criptare și autentificare puternice pentru a proteja rețeaua wireless împotriva accesului neautorizat și a atacurilor cibernetice.
6. Dezvoltarea și implementarea unei politici adecvate pentru a asigura securitatea datelor și a informațiilor atunci când se lucrează de la distanță (telecommuting).
7. Evaluarea și abordarea riscurilor de securitate specifice asociate cu utilizarea dispozitivelor IoT conectate în rețea, în cazul în care acestea sunt adoptate în viitor.
8. Furnizarea instruirii în domeniul securității cibernetice pentru personal, pentru a crește conștientizarea și a recunoa ște riscurile asociate cu securitatea informațiilor.
9. Implementarea unei soluții de protecție a parolelor pentru a asigura gestionarea sigură și eficientă a parolelor în organizație.
10. Colaborarea cu experți în securitate cibernetică și instituții guvernamentale pentru a beneficia de cele mai recente recomandări și tehnologii disponibile în domeniu.
11. Implementarea unei soluții de backup și de recuperare a datelor pentru a asigura continuitatea activității în cazul unui incident de securitate sau a unei pierderi de date.
12. Evaluarea periodică a infrastructurii și a practicilor de securitate pentru a identifica și aborda rapid eventualele vulnerabilități.
13. Utilizarea și implementarea instrumentelor de monitorizare și analiză a rețelei pentru a detecta și preveni potențialele atacuri cibernetice.
14. Dezvoltarea și promovarea unei culturi organizaționale care să pună accent pe securitatea informațiilor și protecția datelor personale ale membrilor.

3. Plan de acțiune pentru securitatea cibernetică a Primăriei Bistrița

Etapa 1: Abordarea slăbiciunilor și amenințărilor

1. Crearea unui comitet de securitate cibernetică responsabil cu implementarea și monitorizarea planului de acțiune.
2. Asigurarea accesului la tehnologii și resurse adecvate pentru a aborda vulnerabilitățile existente în sistemul IT al Primăriei.
3. Dezvoltarea și implementarea unui program de formare pentru angajații Primăriei cu privire la practicile de securitate cibernetică și protecția datelor.
4. Implementarea unei politici de securitate a informațiilor, cu proceduri și reguli specifice pentru protejarea datelor și a sistemelor informatice.
5. Crearea unei linii de comunicare directă între cetățeni și Primărie pentru raportarea incidentelor de securitate cibernetică.

Etapa 2: Consolidarea punctelor forte și exploatarea oportunităților

6. Utilizarea expertizei interne și a parteneriatelor cu instituții publice și private pentru dezvoltarea de proiecte digitale prioritare în domeniul securității cibernetice.
7. Implementarea unui sistem de e-guvernare pentru a facilita accesul cetățenilor la serviciile și informațiile publice, asigurând în același timp securitatea și confidențialitatea datelor.
8. Stimularea colaborării cu alte primării, organizații și instituții pentru a împărtăși bunele practici și a dezvolta soluții comune pentru problemele de securitate cibernetică.
9. Promovarea inițiativelor de securitate cibernetică în comunitate pentru a crește gradul de conștientizare și a reduce riscurile asociate cu utilizarea tehnologiei.
10. Monitorizarea și evaluarea continuă a eficacității măsurilor de securitate cibernetică implementate, pentru a se asigura că Primăria Bistrița rămâne protejată în fața amenințărilor emergente.

Pentru a asigura succesul acestui plan de acțiune, este esențial ca Primăria Bistrița să aloce resursele financiare și umane necesare și să monitorizeze în mod constant progresul în atingerea obiectivelor stabilite.

4. Recomandări pentru digitalizare

Adoptarea cu prioritate a măsurilor/rezultatelor obținute în urma implementării proiectelor fanion. Recomandări de abordare a noilor oportunități și nevoi de digitalizare pentru Primăria Bistrița:

1. Digitalizarea serviciilor publice (prioritate înaltă, etapa 1)
    - Crearea unei arhive electronice.
    - Integrarea unui sistem de semnătură electronică pentru a facilita procesul de aprobare a documentelor.
2. Crearea unui portal de date deschise (prioritate medie, etapa 2)
    - Adaptarea portalului online existent astfel încât să ofere acces la datele publice ale Primăriei într-un format deschis și ușor de utilizat.
    - Organizarea de hackathoane și concursuri pentru a implica comunitatea locală în dezvoltarea de aplicații și servicii bazate pe aceste date deschise.
3. Implementarea unui sistem de monitorizare a infrastructurii urbane (prioritate medie, etapa 3)
    - Instalarea de senzori IoT (Internet of Things) în infrastructura urbană (iluminat stradal, trafic, managementul deșeurilor, etc.) pentru a colecta și analiza date în timp real.
    - Dezvoltarea de aplicații și servicii pentru a permite cetățenilor să raporteze probleme legate de infrastructură și pentru a facilita managementul resurselor și intervenția rapidă a echipei de întreținere.
4. Îmbunătățirea comunicării și transparenței (prioritate înaltă, etapa 1)
    - Dezvoltarea unei aplicații mobile și a unui site web actualizat pentru Primăria Bistrița, care să permită cetățenilor să acceseze informații și să comunice direct cu primăria.
    - Implementarea unui sistem de notificare prin SMS și e-mail pentru a ține cetățenii informați despre evenimentele și deciziile locale.
5. Promovarea inovației și colaborării în comunitate (prioritate medie, etapa 2)
    - Crearea unui centru de inovație și colaborare, unde autoritățile locale, întreprinderile, organizațiile non-profit și cetățenii să poată lucra împreună pentru a dezvolta soluții digitale la problemele locale.
    - Organizarea de evenimente, workshop-uri și cursuri pentru a încuraja învățarea digitală și a cultiva competențele digitale în rândul angajaților și cetățenilor.

6. Îmbunătățirea capacității de răspuns în situații de urgență (prioritate înaltă, etapa 2)
    - Integrarea unui sistem digital de management al situațiilor de urgență, care să permită coordonarea eficientă a resurselor și comunicarea rapidă între autorități, serviciile de urgență și cetățeni.
    - Dezvoltarea unei aplicații mobile pentru raportarea și monitorizarea situațiilor de urgență de către cetățeni.
7. Digitalizarea procesului de urbanism și dezvoltare (prioritate medie, etapa 3)
    - Implementarea unei soluții digitale pentru gestionarea și monitorizarea proiectelor de urbanism și dezvoltare, care să faciliteze colaborarea între diferitele departamente ale Primăriei și să asigure transparența procesului pentru cetățeni.
    - Crearea unei platforme online pentru consultarea publică și colectarea feedback-ului cetățenilor privind proiectele de dezvoltare urbană.
8. Crearea unui sistem de e-guvernare (prioritate înaltă, etapa 1)
    - Implementarea unui sistem de e-guvernare care să permită cetățenilor să participe activ la procesul de luare a deciziilor și să-și exprime opiniile privind problemele locale.
    - Integrarea unui sistem de vot electronic pentru a facilita participarea cetățenilor în alegerile locale și în consultările publice.
9. Evaluarea riscurilor de securitate cibernetică și identificarea vulnerabilităților (prioritate înaltă, etapa 1)
    - Realizarea unui audit de securitate cibernetică pentru a identifica vulnerabilitățile și a stabili prioritățile în materie de securitate a informațiilor.
10. Crearea unui plan de conformitate cu GDPR (prioritate înaltă, etapa 1)
    - Elaborarea unui plan de conformitate cu GDPR, care să includă procese și proceduri privind colectarea, stocarea, procesarea și ștergerea datelor cu caracter personal.
11. Dezvoltarea unei strategii de securitate cibernetică (prioritate înaltă, etapa 1)
    - Crearea unei strategii de securitate cibernetică care să acopere atât infrastructura IT, cât și componentele digitale ale Primăriei Bistrița, precum și proiectele de digitalizare viitoare.
12. Implementarea unui sistem de management al securității informațiilor (prioritate înaltă, etapa 2)
    - Implementarea unui sistem de management al securității informațiilor (SMSI) bazat pe standarde internaționale, cum ar fi ISO/IEC 27001, pentru a gestiona riscurile de securitate și a proteja informațiile și serviciile digitale ale Primăriei.
13. Îmbunătățirea conștientizării privind securitatea cibernetică și formarea personalului (prioritate înaltă, etapa 1)
    - Implementarea unui program de formare și conștientizare în domeniul securității cibernetice pentru angajații Primăriei Bistrița, pentru a-i ajuta să înțeleagă riscurile și să-și îmbunătățească comportamentul în privința securității informațiilor.
14. Stabilirea unui protocol de reacție la incidente de securitate (prioritate înaltă, etapa 2)
    - Crearea unui protocol de reacție la incidente de securitate cibernetică, care să includă proceduri pentru identificarea, investigarea și remedierea incidentelor, precum și comunicarea cu părțile interesate.
15. Monitorizarea și evaluarea periodică a securității cibernetice și a conformității cu GDPR (prioritate medie, etapa 3)
    - Implementarea unui proces de monitorizare și evaluare periodică a securității cibernetice și a conformității cu GDPR, pentru a asigura un nivel adecvat de protecție în timp și a adapta planurile de acțiune în funcție de evoluția riscurilor și a reglementărilor.

Pentru a asigura succesul acestor recomandări, este important ca Primăria Bistrița să coopereze cu parteneri din sectorul public și privat, să aloce resursele necesare și să mențină un proces de evaluare și ajustare continuă a proiectelor în funcție de nevoile comunității și de evoluția tehnologiei.

5. Indicatori specifici și niveluri de progres

Indicatorii specifici și nivelurile de progres pentru fiecare dintre cele 15 puncte de acțiune menționate anterior sunt:

1. Digitalizarea serviciilor publice
    - Indicator: numărul de servicii publice accesibile online
    - Obiectiv: 80% din serviciile publice disponibile online în termen de 36 luni
2. Crearea unui portal de date deschise
    - Indicator: numărul de seturi de date publicate în format deschis
    - Obiectiv: publicarea a cel puțin 50 de seturi de date în termen de 24 luni
3. Implementarea unui sistem de monitorizare a infrastructurii urbane
    - Indicator: numărul de senzori IoT instalați și zonele acoperite
    - Obiectiv: instalarea a 500 de senzori IoT în zonele-cheie în termen de 24 luni
4. Îmbunătățirea comunicării și transparenței
    - Indicator: numărul de cetățeni înregistrați pe platformele digitale de comunicare
    - Obiectiv: înregistrarea a 60% din populație pe platformele digitale în termen de 24 luni
5. Promovarea inovației și colaborării în comunitate
    - Indicator: numărul de proiecte și parteneriate dezvoltate în cadrul centrului de inovație
    - Obiectiv: dezvoltarea a 10 proiecte și parteneriate în termen de 18 luni
6. Îmbunătățirea capacității de răspuns în situații de urgență
    - Indicator: timpul de răspuns la situațiile de urgență
    - Obiectiv: reducerea timpului de răspuns cu 30% în termen de 18 luni
7. Digitalizarea procesului de urbanism și dezvoltare
    - Indicator: numărul de proiecte de urbanism și dezvoltare gestionate digital
    - Obiectiv: gestionarea digitală a 100% din proiectele de urbanism în termen de 24 luni
8. Crearea unui sistem de e-guvernare
    - Indicator: numărul de cetățeni care participă la procesul de luare a deciziilor prin e-guvernare
    - Obiectiv: implicarea a 40% din populație în procesul de luare a deciziilor în termen de 12 luni
9. Evaluarea riscurilor de securitate cibernetică și identificarea vulnerabilităților
    - Indicator: numărul de vulnerabilități identificate și remediate
    - Obiectiv: identificarea și remedierea a 90% din vulnerabilitățile critice în termen de 6 luni
10. Crearea unui plan de conformitate cu GDPR
    - Indicator: procentul de conformitate cu GDPR
    - Obiectiv: atingerea unui nivel de conformitate de 100% în termen de 36 luni
11. Dezvoltarea unei strategii de securitate cibernetică
    - Indicator: implementarea strategiei de securitate cibernetică
    - Obiectiv: finalizarea și implementarea strategiei de securitate cibernetică în termen de 6 luni

12. Implementarea unui sistem de management al securității informațiilor
    - Indicator: obținerea certificării ISO/IEC 27001
    - Obiectiv: obținerea certificării ISO/IEC 27001 în termen de 18 luni
13. Îmbunătățirea conștientizării privind securitatea cibernetică și formarea personalului
    - Indicator: numărul de angajați care au completat programul de formare
    - Obiectiv: formarea a 100% din angajații Primăriei în termen de 12 luni
14. Stabilirea unui protocol de reacție la incidente de securitate
    - Indicator: timpul de reacție la incidentele de securitate cibernetică
    - Obiectiv: reducerea timpului de reacție la incidentele de securitate cibernetică cu 50% în termen de 12 luni
15. Monitorizarea și evaluarea periodică a securității cibernetice și a conformității cu GDPR
    - Indicator: numărul de audituri și evaluări efectuate
    - Obiectiv: realizarea a cel puțin 2 audituri și evaluări pe an pentru a menține nivelul de protecție și conformitate adecvat

Acești indicatori și niveluri de progres servesc drept repere pentru a măsura succesul inițiativelor de digitalizare și pentru a asigura că se îndeplinesc obiectivele stabilite. Atingerea acestor obiective va contribui semnificativ la modernizarea și îmbunătățirea serviciilor publice, transparența și securitatea în Primăria Bistrița.

6. Analiza conformității sistemului informatic cu cerințele GDPR

Pentru a realiza o analiză a gradului de conformitate a sistemului informatic actual cu cerințele GDPR, este important să luăm în considerare următoarele aspecte cheie:

1. Documentarea proceselor de prelucrare a datelor cu caracter personal:
    - Este important să se înțeleagă modul în care datele cu caracter personal sunt colectate, stocate, procesate și șterse în cadrul sistemului informatic.
    - Asigurați-vă că există un registru de prelucrare a datelor cu caracter personal, care include scopurile prelucrării, categoriile de date personale, beneficiarii datelor și măsurile de securitate aplicate.
2. Evaluarea impactului asupra protecției datelor (EIPD):
    - Ați efectuat EIPD-uri pentru procesele de prelucrare a datelor cu risc înalt pentru drepturile și libertățile persoanelor fizice? Acest lucru este necesar în cazul în care prelucrarea ar putea avea un impact semnificativ asupra drepturilor și libertăților individuale.
3. Măsuri de securitate a datelor:
    - Verificați dacă măsurile de securitate implementate în sistemul informatic sunt adecvate pentru a proteja datele cu caracter personal împotriva accesului neautorizat, pierderii sau distrugerii.
    - Asigurați-vă că se realizează copii de rezervă periodice și că există un plan de recuperare în caz de incidente de securitate.
4. Acordul privind prelucrarea datelor (APD):
    - În cazul în care apelați la subcontractanți pentru a prelucra date cu caracter personal, asigurați-vă că aveți acorduri scrise în loc care să cuprindă clauzele necesare privind protecția datelor.
5. Desemnarea unui responsabil cu protecția datelor (DPO):
    - Ați desemnat un DPO în cadrul organizației dvs.? Acesta trebuie să fie o persoană cu cunoștințe adecvate și experiență în domeniul protecției datelor.

6. Drepturile persoanelor vizate:
    - Asigurați-vă că sistemul informatic vă permite să respectați drepturile persoanelor vizate, cum ar fi accesul la date, rectificarea, ștergerea, restricționarea prelucrării și portabilitatea datelor.
7. Notificarea autorității de supraveghere și a persoanelor vizate în caz de încălcare a securității datelor:
    - Aveți un plan și un proces în loc pentru a raporta incidentele de securitate autorității de supraveghere și persoanelor vizate, dacă este necesar?
8. Transferul internațional de date:
    - Verificați dacă transferurile internaționale de date cu caracter personal sunt efectuate în conformitate cu cerințele GDPR, cum ar fi utilizarea clauzelor contractuale standard sau asigurarea că țările terțe oferă un nivel adecvat de protecție a datelor.
9. Politici și proceduri interne:
    - Asigurați-vă că aveți politici și proceduri interne privind protecția datelor și că acestea sunt actualizate și respectate de personalul organizației. Acestea ar trebui să includă măsuri precum limitarea accesului la date cu caracter personal și instruirea personalului cu privire la obligațiile lor legate de GDPR.
10. Evaluarea periodică a conformității:
    - Implementați un proces de revizuire și evaluare periodică a conformității sistemului informatic cu cerințele GDPR. Acest lucru vă va ajuta să identificați și să remediați eventualele lacune în conformitate.

Pentru a aborda problemele și lacunele identificate în conformitatea cu GDPR la Primăria Bistrița, vă recomandăm să implementați următoarele măsuri:

1. Instruirea și sensibilizarea personalului:
    - Organizați sesiuni de instruire și conștientizare privind GDPR pentru angajați, cu accent pe importanța protecției datelor și consecințele nerespectării regulamentului. Asigurați-vă că instruirea este adaptată la rolul și responsabilitățile fiecărui angajat.
2. Întărirea autorității Ofițerului GDPR (DPO):
    - Revizuiți rolul și responsabilitățile DPO în cadrul organizației și acordați-i autoritatea necesară pentru a monitoriza și a asigura respectarea cerințelor GDPR. DPO ar trebui să aibă acces la resursele necesare și să poată raporta în mod direct conducerii organizației.
3. Documentarea și revizuirea proceselor de prelucrare a datelor:
    - Lucrați împreună cu DPO pentru a documenta și revizui procesele de prelucrare a datelor cu caracter personal în cadrul sistemului informatic. Actualizați registrul de prelucrare a datelor și asigurați-vă că acesta este menținut în mod constant.
4. Implementarea măsurilor de securitate adecvate:
    - Efectuați o evaluare a riscurilor și identificați măsurile de securitate adecvate pentru a proteja datele cu caracter personal. Implementați măsuri tehnice și organizatorice pentru a preveni accesul neautorizat, pierderea sau distrugerea datelor.
5. Revizuirea și actualizarea politicii și procedurilor interne:
    - Colaborați cu DPO pentru a revizui și actualiza politici și proceduri interne privind protecția datelor, asigurându-vă că acestea sunt în conformitate cu GDPR și sunt urmate de întregul personal.
6. Implementarea unui mecanism eficient pentru exercitarea drepturilor persoanelor vizate:

- Asigurați-vă că sistemul informatic permite respectarea drepturilor persoanelor vizate și că există un proces clar pentru gestionarea solicitărilor legate de drepturile individuale.

7. Stabilirea unui plan de notificare a încălcărilor de securitate:
   - Colaborați cu DPO pentru a stabili un plan și un proces de raportare a încălcărilor de securitate către autoritatea de supraveghere și persoanele vizate, în conformitate cu cerințele GDPR.
8. Evaluarea și monitorizarea transferurilor internaționale de date:
   - Verificați toate transferurile internaționale de date și asigurați-vă că acestea sunt efectuate în conformitate cu cerințele GDPR. În cazul în care este necesar, implementați clauze contractuale standard sau alte mecanisme de transfer adecvate pentru a asigura protecția datelor.
9. Monitorizarea și revizuirea periodică a conformității:
   - Stabiliți un proces de monitorizare și revizuire periodică a conformității sistemului informatic cu cerințele GDPR, implicând DPO și alte părți relevante. Acest proces vă va ajuta să identificați și să remediați eventualele lacune în conformitate.
10. Îmbunătățirea comunicării și colaborării între departamente:
    - Promovați o cultură a protecției datelor în cadrul organizației, încurajând comunicarea și colaborarea între departamente în probleme legate de GDPR. Aceasta va ajuta la identificarea și abordarea rapidă a problemelor și va îmbunătăți conformitatea generală.

Implementarea acestor măsuri va ajuta Primăria Bistrița să își îmbunătățească conformitatea cu GDPR și să reducă riscul de sancțiuni și incidente de securitate legate de datele cu caracter personal. Acest proces poate necesita timp și resurse, dar este esențial pentru a proteja drepturile și libertățile persoanelor fizice și pentru a asigura buna funcționare a sistemului informatic în conformitate cu reglementările aplicabile.

Pentru a evalua progresul și a stabili niveluri de progres pentru fiecare dintre cele 10 puncte menționate, propunem utilizarea următorilor indicatori specifici:

1. Pentru instruirea și sensibilizarea personalului, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Numărul de angajați care au participat la sesiuni de instruire și conștientizare privind GDPR. Nivelurile de progres ar putea fi:
  - Sub 50%: nivel scăzut de progres
  - 50-75%: progres mediu
  - Peste 75%: nivel ridicat de progres
- Numărul de angajați care au finalizat cu succes testele de evaluare a cunoștințelor privind GDPR, după sesiunile de instruire. Nivelurile de progres ar putea fi:
  - Sub 50%: nivel scăzut de progres
  - 50-75%: progres mediu
  - Peste 75%: nivel ridicat de progres
- Feedback-ul angajaților referitor la calitatea și utilitatea sesiunilor de instruire. Nivelurile de progres ar putea fi:
  - Feedback negativ predominant: nivel scăzut de progres
  - Feedback mixt: progres mediu
  - Feedback pozitiv predominant: nivel ridicat de progres

2. Pentru întărirea autorității Ofițerului GDPR (DPO), câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Gradul de implicare al DPO în procesele de luare a deciziilor privind protecția datelor. Nivelurile de progres ar putea fi:
  - DPO nu este implicat în mod activ în procesele de luare a deciziilor: nivel scăzut de progres
  - DPO este consultat, dar nu are autoritate de decizie: progres mediu
  - DPO are autoritate de decizie și este implicat activ în procesele de luare a deciziilor: nivel ridicat de progres
- Accesul DPO la resursele necesare pentru a îndeplini rolul și responsabilitățile sale. Nivelurile de progres ar putea fi:
  - DPO nu are acces la resursele necesare: nivel scăzut de progres
  - DPO are acces limitat la resurse, dar poate îndeplini rolul într-o oarecare măsură: progres mediu
  - DPO are acces la resursele necesare și poate îndeplini rolul în mod eficient: nivel ridicat de progres
- Gradul de raportare directă a DPO către conducerea organizației. Nivelurile de progres ar putea fi:
  - DPO nu are posibilitatea de a raporta direct către conducerea organizației: nivel scăzut de progres
  - DPO poate raporta către conducerea organizației, dar există bariere în comunicare: progres mediu
  - DPO poate raporta direct și există o comunicare eficientă între DPO și conducerea organizației: nivel ridicat de progres

3. Pentru documentarea și revizuirea proceselor de prelucrare a datelor, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Gradul de acoperire a proceselor de prelucrare a datelor înregistrate în registru. Nivelurile de progres ar putea fi:
  - Sub 50% din procesele de prelucrare sunt documentate: nivel scăzut de progres
  - 50-75% din procesele de prelucrare sunt documentate: progres mediu
  - Peste 75% din procesele de prelucrare sunt documentate: nivel ridicat de progres
- Gradul de detaliere și exactitate a proceselor de prelucrare a datelor înregistrate în registru. Nivelurile de progres ar putea fi:
  - Procesele de prelucrare sunt documentate în mod sumar și/sau inexact: nivel scăzut de progres
  - Procesele de prelucrare sunt documentate în mod detaliat și precis: nivel ridicat de progres
- Gradul de actualizare a registrelor de prelucrare a datelor. Nivelurile de progres ar putea fi:
  - Registrele de prelucrare a datelor nu sunt actualizate în mod regulat: nivel scăzut de progres
  - Registrele de prelucrare a datelor sunt actualizate în mod regulat, dar nu în timp real: progres mediu
  - Registrele de prelucrare a datelor sunt actualizate în timp real: nivel ridicat de progres
- Gradul de implicare a DPO în procesul de revizuire și actualizare a registrelor de prelucrare a datelor. Nivelurile de progres ar putea fi:

- DPO nu este implicat în procesul de revizuire și actualizare a registrelor de prelucrare a datelor: nivel scăzut de progres
- DPO este consultat în procesul de revizuire și actualizare a registrelor de prelucrare a datelor: progres mediu
- DPO este implicat activ în procesul de revizuire și actualizare a registrelor de prelucrare a datelor: nivel ridicat de progres

4. Pentru implementarea măsurilor de securitate adecvate, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Gradul de implementare a măsurilor de securitate identificate în urma evaluării riscurilor. Nivelurile de progres ar putea fi:
  - Implementarea măsurilor de securitate este în stadiu incipient: nivel scăzut de progres
  - Implementarea măsurilor de securitate este în curs de desfășurare: progres mediu
  - Implementarea măsurilor de securitate este finalizată: nivel ridicat de progres
- Gradul de adecvare al măsurilor de securitate implementate. Nivelurile de progres ar putea fi:
  - Măsurile de securitate implementate sunt ineficiente sau nu sunt adecvate pentru a proteja datele cu caracter personal: nivel scăzut de progres
  - Măsurile de securitate implementate sunt parțial adecvate, dar mai sunt necesare îmbunătățiri: progres mediu
  - Măsurile de securitate implementate sunt adecvate pentru a proteja datele cu caracter personal: nivel ridicat de progres
- Gradul de documentare și monitorizare a măsurilor de securitate implementate. Nivelurile de progres ar putea fi:
  - Măsurile de securitate implementate nu sunt documentate sau monitorizate în mod regulat: nivel scăzut de progres
  - Măsurile de securitate implementate sunt documentate, dar nu sunt monitorizate în mod regulat: progres mediu
  - Măsurile de securitate implementate sunt documentate și monitorizate în mod regulat: nivel ridicat de progres
- Gradul de implicare a personalului în implementarea și respectarea măsurilor de securitate. Nivelurile de progres ar putea fi:
  - Personalul nu este implicat sau nu respectă măsurile de securitate implementate: nivel scăzut de progres
  - Personalul este implicat, dar nu respectă întotdeauna măsurile de securitate implementate: progres mediu
  - Personalul este implicat și respectă măsurile de securitate implementate în mod constant: nivel ridicat de progres

5. Pentru revizuirea și actualizarea politicii și procedurilor interne, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Gradul de actualizare a politicii și procedurilor interne în concordanță cu GDPR. Nivelurile de progres ar putea fi:
  - Politica și procedurile interne nu au fost actualizate în concordanță cu GDPR: nivel scăzut de progres

    - Politica și procedurile interne au fost actualizate, dar nu sunt în totalitate conform cu GDPR: progres mediu
    - Politica și procedurile interne sunt în totalitate actualizate și conforme cu GDPR: nivel ridicat de progres
- Gradul de accesibilitate și claritate a politicii și procedurilor interne pentru întregul personal. Nivelurile de progres ar putea fi:
    - Politica și procedurile interne nu sunt accesibile sau nu sunt clare pentru întregul personal: nivel scăzut de progres
    - Politica și procedurile interne sunt parțial accesibile și clare pentru întregul personal: progres mediu
    - Politica și procedurile interne sunt complet accesibile și clare pentru întregul personal: nivel ridicat de progres
- Gradul de respectare a politicii și procedurilor interne de către personal. Nivelurile de progres ar putea fi:
    - Personalul nu respectă politica și procedurile interne în mod constant sau deloc: nivel scăzut de progres
    - Personalul respectă politica și procedurile interne, dar cu unele încălcări minore: progres mediu
    - Personalul respectă politica și procedurile interne în mod constant: nivel ridicat de progres
- Gradul de actualizare și revizuire a politicii și procedurilor interne. Nivelurile de progres ar putea fi:
    - Politica și procedurile interne nu sunt actualizate și revizuite în mod regulat: nivel scăzut de progres
    - Politica și procedurile interne sunt actualizate și revizuite în mod regulat, dar nu în totalitate: progres mediu
    - Politica și procedurile interne sunt actualizate și revizuite în mod regulat și în totalitate: nivel ridicat de progres

6. Pentru implementarea unui mecanism eficient pentru exercitarea drepturilor persoanelor vizate, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Timpul necesar pentru a răspunde la solicitările privind exercitarea drepturilor persoanelor vizate. Nivelurile de progres ar putea fi:
    - Timpul de răspuns este foarte lung sau nu este definit în mod clar: nivel scăzut de progres
    - Timpul de răspuns este definit și respectat, dar este prea mare: progres mediu
    - Timpul de răspuns este definit și respectat în mod eficient: nivel ridicat de progres
- Gradul de conformitate al sistemului informatic cu cerințele GDPR privind drepturile persoanelor vizate. Nivelurile de progres ar putea fi:
    - Sistemul informatic nu este configurat pentru a permite exercitarea drepturilor persoanelor vizate: nivel scăzut de progres
    - Sistemul informatic este configurat pentru a permite exercitarea drepturilor persoanelor vizate, dar nu în totalitate: progres mediu
    - Sistemul informatic este configurat pentru a permite exercitarea drepturilor persoanelor vizate în totalitate: nivel ridicat de progres
- Gradul de actualizare și revizuire a procesului pentru gestionarea solicitărilor legate de drepturile individuale. Nivelurile de progres ar putea fi:

- Procesul pentru gestionarea solicitărilor nu este definit sau nu este actualizat în mod regulat: nivel scăzut de progres
- Procesul pentru gestionarea solicitărilor este definit și actualizat în mod regulat, dar există încă probleme semnificative: progres mediu
- Procesul pentru gestionarea solicitărilor este definit și actualizat în mod regulat, iar problemele semnificative sunt rezolvate în mod eficient: nivel ridicat de progres

- Gradul de transparență și claritate a procesului pentru gestionarea solicitărilor legate de drepturile individuale. Nivelurile de progres ar putea fi:
  - Procesul pentru gestionarea solicitărilor nu este clar sau nu este transparent pentru persoanele vizate: nivel scăzut de progres
  - Procesul pentru gestionarea solicitărilor este clar și transparent pentru persoanele vizate, dar există încă probleme minore: progres mediu
  - Procesul pentru gestionarea solicitărilor este clar și transparent pentru persoanele vizate și nu există probleme semnificative: nivel ridicat de progres

7. Pentru stabilirea unui plan de notificare a încălcărilor de securitate, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Timpul necesar pentru a notifica autoritățile și persoanele vizate în cazul unei încălcări de securitate. Nivelurile de progres ar putea fi:
  - Timpul necesar pentru notificare nu este definit sau este prea lung: nivel scăzut de progres
  - Timpul necesar pentru notificare este definit, dar nu este respectat întotdeauna: progres mediu
  - Timpul necesar pentru notificare este definit și este respectat în mod eficient: nivel ridicat de progres
- Gradul de acoperire a planului de notificare a încălcărilor de securitate. Nivelurile de progres ar putea fi:
  - Planul de notificare nu acoperă toate tipurile de încălcări de securitate sau nu este definit în totalitate: nivel scăzut de progres
  - Planul de notificare acoperă majoritatea tipurilor de încălcări de securitate, dar există încă lacune: progres mediu
  - Planul de notificare acoperă toate tipurile de încălcări de securitate și este definit în totalitate: nivel ridicat de progres
- Gradul de implicare a DPO în procesul de notificare a încălcărilor de securitate. Nivelurile de progres ar putea fi:
  - DPO nu este implicat în procesul de notificare a încălcărilor de securitate: nivel scăzut de progres
  - DPO este implicat, dar nu are un rol clar definit în procesul de notificare a încălcărilor de securitate: progres mediu
  - DPO are un rol clar definit în procesul de notificare a încălcărilor de securitate și este implicat activ: nivel ridicat de progres
- Gradul de actualizare și revizuire a planului de notificare a încălcărilor de securitate. Nivelurile de progres ar putea fi:
  - Planul de notificare nu este actualizat sau revizuit în mod regulat: nivel scăzut de progres
  - Planul de notificare este actualizat și revizuit în mod regulat, dar nu în totalitate: progres mediu

- Planul de notificare este actualizat și revizuit în mod regulat și în totalitate: nivel ridicat de progres

8. Pentru evaluarea și monitorizarea transferurilor internaționale de date, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Gradul de acoperire a evaluării transferurilor internaționale de date. Nivelurile de progres ar putea fi:
  - Evaluarea nu acoperă toate transferurile internaționale de date sau nu este definită în totalitate: nivel scăzut de progres
  - Evaluarea acoperă majoritatea transferurilor internaționale de date, dar există încă lacune: progres mediu
  - Evaluarea acoperă toate transferurile internaționale de date și este definită în totalitate: nivel ridicat de progres
- Gradul de conformitate al transferurilor internaționale de date cu cerințele GDPR. Nivelurile de progres ar putea fi:
  - Transferurile internaționale de date nu sunt conform cu cerințele GDPR sau nu sunt analizate în totalitate: nivel scăzut de progres
  - Transferurile internaționale de date sunt conform cu cerințele GDPR, dar nu în totalitate: progres mediu
  - Transferurile internaționale de date sunt conform cu cerințele GDPR în totalitate: nivel ridicat de progres
- Gradul de implementare a clauzelor contractuale standard sau altor mecanisme de transfer adecvate. Nivelurile de progres ar putea fi:
  - Clauzele contractuale standard sau alte mecanisme de transfer adecvate nu sunt implementate sau nu sunt definite în totalitate: nivel scăzut de progres
  - Clauzele contractuale standard sau alte mecanisme de transfer adecvate sunt implementate, dar nu în totalitate: progres mediu
  - Clauzele contractuale standard sau alte mecanisme de transfer adecvate sunt implementate în totalitate: nivel ridicat de progres
- Gradul de actualizare și revizuire a evaluării transferurilor internaționale de date. Nivelurile de progres ar putea fi:
  - Evaluarea transferurilor internaționale de date nu este actualizată sau revizuită în mod regulat: nivel scăzut de progres
  - Evaluarea transferurilor internaționale de date este actualizată și revizuită în mod regulat, dar nu în totalitate: progres mediu
  - Evaluarea transferurilor internaționale de date este actualizată și revizuită în mod regulat și în totalitate: nivel ridicat de progres

9. Pentru monitorizarea și revizuirea periodică a conformității cu cerințele GDPR, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Frecvența și acoperirea evaluărilor periodice de conformitate cu cerințele GDPR. Nivelurile de progres ar putea fi:
  - Evaluările periodice nu sunt efectuate sau sunt efectuate foarte rar: nivel scăzut de progres
  - Evaluările periodice sunt efectuate, dar nu acoperă toate aspectele GDPR: progres mediu

    - Evaluările periodice sunt efectuate și acoperă toate aspectele GDPR: nivel ridicat de progres
- Gradul de implicare a DPO și a altor părți relevante în procesul de monitorizare și revizuire periodică a conformității cu cerințele GDPR. Nivelurile de progres ar putea fi:
    - DPO și alte părți relevante nu sunt implicate sau nu au un rol clar definit în procesul de monitorizare și revizuire periodică a conformității cu cerințele GDPR: nivel scăzut de progres
    - DPO și alte părți relevante sunt implicate în procesul de monitorizare și revizuire periodică a conformității cu cerințele GDPR, dar nu în totalitate: progres mediu
    - DPO și alte părți relevante sunt implicate în mod activ și au un rol clar definit în procesul de monitorizare și revizuire periodică a conformității cu cerințele GDPR: nivel ridicat de progres
- Gradul de identificare și remediere a eventualelor lacune în conformitate. Nivelurile de progres ar putea fi:
    - Eventualele lacune în conformitate nu sunt identificate sau nu sunt remediate: nivel scăzut de progres
    - Eventualele lacune în conformitate sunt identificate, dar nu sunt remediate în totalitate: progres mediu
    - Eventualele lacune în conformitate sunt identificate și remediate în totalitate: nivel ridicat de progres
- Gradul de actualizare și revizuire a procesului de monitorizare și revizuire periodică a conformității cu cerințele GDPR. Nivelurile de progres ar putea fi:
    - Procesul de monitorizare și revizuire periodică a conformității nu este actualizat sau revizuit în mod regulat: nivel scăzut de progres
    - Procesul de monitorizare și revizuire periodică a conformității este actualizat și revizuit în mod regulat, dar nu în totalitate: progres mediu
    - Procesul de monitorizare și revizuire periodică a conformității este actualizat și revizuit în mod regulat și în totalitate: nivel ridicat de progres

10. Pentru îmbunătățirea comunicării și colaborării între departamente în probleme legate de GDPR, câțiva indicatori specifici și nivelurile de progres asociate ar putea fi:

- Gradul de conștientizare a importanței protecției datelor și a cerințelor GDPR în rândul angajaților. Nivelurile de progres ar putea fi:
    - Angajații nu sunt conștienți de importanța protecției datelor și a cerințelor GDPR sau nu sunt instruiți adecvat în această privință: nivel scăzut de progres
    - Angajații sunt conștienți de importanța protecției datelor și a cerințelor GDPR, dar nu sunt instruiți adecvat sau nu sunt implicați în comunicarea și colaborarea în probleme legate de GDPR: progres mediu
    - Angajații sunt conștienți de importanța protecției datelor și a cerințelor GDPR și sunt instruiți adecvat, fiind implicați în comunicarea și colaborarea în probleme legate de GDPR: nivel ridicat de progres
- Gradul de implicare a tuturor departamentelor în procesul de protecție a datelor și de conformitate cu cerințele GDPR. Nivelurile de progres ar putea fi:
    - Unele departamente nu sunt implicate sau nu sunt conștiente de responsabilitățile lor în protecția datelor și conformitatea cu cerințele GDPR: nivel scăzut de progres
    - Toate departamentele sunt implicate, dar implicarea lor este limitată sau nu este eficientă: progres mediu

- Toate departamentele sunt implicate activ în procesul de protecție a datelor și de conformitate cu cerințele GDPR: nivel ridicat de progres
- Gradul de comunicare și colaborare între departamente în probleme legate de GDPR. Nivelurile de progres ar putea fi:
  - Comunicarea și colaborarea între departamente în probleme legate de GDPR este limitată sau ineficientă: nivel scăzut de progres
  - Comunicarea și colaborarea între departamente în probleme legate de GDPR sunt îmbunătățite, dar există încă lacune: progres mediu
  - Comunicarea și colaborarea între departamente în probleme legate de GDPR sunt eficiente și se fac progrese semnificative în soluționarea problemelor: nivel ridicat de progres
- Gradul de dezvoltare a unei culturi a protecției datelor în cadrul organizației. Nivelurile de progres ar putea fi:
  - Organizația nu promovează o cultură a protecției datelor sau nu are o abordare proactivă în ceea ce privește protecția datelor: nivel scăzut de progres
  - Organizația promovează o cultură a protecției datelor, dar aceasta este încă în curs de dezvoltare sau nu este încorporată în toate aspectele organizației: progres mediu
  - Organizația promovează o cultură a protecției datelor, care este încorporată în toate aspectele organizației și este susținută de toți angajații: nivel ridicat de progres.

7. Evaluarea personalului din Primărie în privința cunoștințelor referitoare la GDPR și securitate cibernetică din perspectiva utilizatorului

Evaluarea personalului pe GDPR

A fost selectat un eșantion de 30 persoane pentru evaluare anonimă. S-au prezentat la testul de evaluare 25 persoane. Eroarea statistică în acest caz se referă la discrepanța între valorile estimate dintr-un eșantion și valorile reale ale unei populații, în general, exprimată ca o marjă de eroare. În cazul datelor referitoare la testul GDPR realizat pe angajații Primăriei Bistrița, putem calcula o estimare a erorii statistice utilizând formula standard a erorii standard a mediei:

Eroarea standard a mediei = Deviația standard a eșantionului / radical din dimensiunea eșantionului

În cazul datelor noastre, avem informații limitate, dar putem presupune că scorurile obținute de angajații testați sunt aproximativ distribuite normal și că eșantionul a fost selectat în mod aleatoriu.

Din informațiile furnizate, putem calcula deviația standard a scorurilor testului GDPR în eșantionul de 25 de angajați utilizând o metodă simplificată. Numărul de angajați care au trecut testul (au obținut scoruri la limită) este de 8, iar numărul total de angajați testați este 25. În aceste condiții, putem considera că probabilitatea de a trece testul este de aproximativ 8/25 = 0,32.

Deviația standard poate fi apoi calculată utilizând formula deviației standard pentru o variabilă binară:

Deviația standard = radical din (probabilitatea de succes x probabilitatea de eșec) / dimensiunea eșantionului

În cazul nostru, avem:

Deviația standard = radical din [(0,68 x 0,32) / 25] = 0,093

Astfel, eroarea standard a mediei poate fi calculată utilizând formula de mai sus:

Eroarea standard a mediei = 0,093 / radical din 25 = 0,018

În concluzie, eroarea statistică în acest caz este de aproximativ ± 0,018. Aceasta înseamnă că estimările noastre ale nivelului de cunoștințe GDPR în rândul angajaților pot varia cu cel mult 1,8 puncte (pe o scară de la 0 la 5), cu o anumită probabilitate, în raport cu ceea ce ar fi obținut din întreaga populație a angajaților Primăriei Bistrița.

În urma testului GDPR realizat pe un eșantion de 25 de angajați din Primăria Bistrița, s-au obținut următoarele rezultate: 17 angajați au obținut un scor sub limita de trecere, iar 8 angajați au obținut un scor la limita de trecere. Scorurile se referă la nivelurile de cunoaștere a GDPR-ului, care sunt: sub limită, la limită, peste limită, bine, foarte bine. Deci, pe scara de evaluare de sub limită, la limită, peste limită, bine, foarte bine, nici un test nu a depășit nivelul la limită. Acest lucru indică necesitatea unor măsuri mai conjugate și mai ferme în pregătirea personalului pe probleme de GDPR.

Din totalul de 60 de subiecte, 20 au fost întrebări de tip grilă și 40 au fost întrebări deschise. Din păcate, răspunsurile la întrebările deschise au fost, în mare parte, simpliste sau inexistente, ceea ce indică faptul că angajații nu au o înțelegere clară a modului de procedare în practică cu GDPR-ul.

De asemenea, răspunsurile la întrebările de tip grilă au fost, in general eronate – probabil că multe dintre ele puse la întâmplare, indicând o lipsă de înțelegere a temelor sau o lipsă de interes în a înțelege modul in care GDPR afectează activitatea lor zilnică. Mai mult, neconcordanța între răspunsurile la întrebările de tip grilă și cele deschise indică o lipsă de coerență în modul în care angajații percep și aplică GDPR-ul.

Pe baza acestor rezultate, se poate concluziona ca este nevoie de o mai bună formare și informare a angajaților cu privire la GDPR și modul în care acesta se aplică in cadrul activității lor.

Pentru a aduce angajații la nivelul de cunoștințe necesar pe tema GDPR și pentru a preveni implicarea în probleme legale, următoarele sunt câteva indicații utile:

1. Realizați formare regulată: Asigurați-vă că angajații sunt informați despre GDPR prin formare regulată. Aceasta poate fi realizată prin instruiri sau prezentări periodice, care să abordeze reguli și proceduri în conformitate cu reglementările GDPR.
2. Identificați zonele de risc: Identificați zonele din organizație care sunt cele mai susceptibile de a încălca regulile GDPR și acordați atenție suplimentară acestor zone.
3. Conștientizați angajații despre datele personale: Faceți-i pe angajați conștienți de faptul că datele personale ale cetățenilor, colegilor și partenerilor sunt valoroase și trebuie protejate.
4. Asigurați-vă că există politici și proceduri clare: Asigurați-vă că există politici și proceduri clare pentru protejarea datelor personale și că acestea sunt comunicate în mod regulat angajaților. În plus, acestea trebuie să fie actualizate constant în funcție de schimbările în reglementările GDPR.
5. Implementați tehnologii de securitate adecvate: Implementați tehnologii de securitate adecvate pentru a proteja datele personale ale clienților, colegilor și partenerilor.
6. Conștientizați angajații despre sancțiuni: Faceți-i pe angajați conștienți de sancțiunile severe care pot fi impuse în cazul încălcării regulilor GDPR, inclusiv amenzi financiare semnificative și posibilitatea de a fi acționați în judecată.

7. Implementați un program de conformitate GDPR: Implementați un program de conformitate GDPR care să vă ajute să mențineți în mod constant acoperirea cerințelor GDPR și să reduceți riscul de încălcare.

În concluzie, este important să se asigure că angajații sunt instruiți și conștienți cu privire la regulile și implicațiile GDPR-ului. În plus, organizarea trebuie să implementeze politici și proceduri clare pentru protejarea datelor personale și să se asigure că acestea sunt actualizate în mod constant pentru a fi în conformitate cu schimbările în reglementările GDPR.

Evaluarea personalului în securitate cibernetică

Pentru evaluarea cunoștințelor în securitate cibernetică s-au prezentat la test tot 25 persoane. Asemenea celor precizate în cazul evaluării GDPR, statistic eșantionul poate fi utilizat pentru a generaliza analiza. Eșantionul a fost ales aleator și acoperitor pe toate compartimentele din Primărie. Testul a constat din 70 subiecte, atât de tip grilă, cât și cu răspunsuri deschise. Din cele 25 persoane testate (anonim), 2 au atins un nivel la limită, restul fiind sub limita de trecere.

Următoarele recomandări pot fi utile:

1. Realizarea de instruiri periodice: Primăria ar trebui să implementeze un program de formare continuă, care să includă instruiri periodice și să ofere oportunități de a exersa și aplica cunoștințele dobândite în privința securității cibernetice.
2. Identificarea zonelor de risc: Este important să se identifice zonele din organizație care sunt cele mai susceptibile de a avea vulnerabilități la atacurile cibernetice și să se acorde o atenție suplimentară acestor zone în cadrul programului de formare.
3. Implementarea de politici și proceduri clare: Este important să se implementeze politici și proceduri clare pentru protejarea datelor și a sistemelor informatice împotriva atacurilor cibernetice și să se asigure că acestea sunt comunicate în mod regulat angajaților și sunt actualizate constant în funcție de schimbările în tehnologia și tendințele de securitate cibernetică.
4. Implementarea de tehnologii de securitate adecvate: Este important să se implementeze tehnologii de securitate adecvate, cum ar fi antivirus și firewall, pentru a proteja datele și sistemele informatice împotriva atacurilor cibernetice.
5. Conștientizarea angajaților cu privire la riscurile securității cibernetice: Este important să se informeze angajații despre riscurile și amenințările de securitate cibernetică, precum phishing-ul și malware-ul, și despre cum să recunoască și să evite aceste amenințări.
6. Implementarea unui program de conformitate cu standardele de securitate cibernetică: Este important să se implementeze un program de conformitate cu standardele de securitate cibernetică, cum ar fi ISO 27001, pentru a menține în mod constant acoperirea cerințelor de securitate cibernetică și pentru a reduce riscul de încălcare.

În derularea unei instruiri pentru securitatea cibernetică, următoarele sunt câteva aspecte importante care trebuie luate în considerare:

Stabiliți obiectivele de învățare: Înainte de a începe programul de instruire, trebuie să vă stabiliți obiectivele de învățare. În funcție de nivelul de cunoștințe al angajaților și de nevoile specifice ale organizației, puteți stabili obiectivele de învățare pentru a vă asigura că formarea abordează subiectele relevante și îi ajută pe angajați să-și îmbunătățească cunoștințele și abilitățile în domeniul securității cibernetice.

Asigurați-vă că formarea este interactivă și practică: Pentru a vă asigura că angajații dobândesc cunoștințe și abilități utile, este important ca formarea să fie interactivă și practică. Aceasta poate include exerciții de grup, studii de caz, simulări sau alte activități care să permită angajaților să aplice cunoștințele într-un mod practic și să vadă cum se aplică acestea în situații reale.

Comunicați clar beneficiile formării: Pentru a-i motiva pe angajați să participe și să ia în serios formarea, este important să le comunicați clar beneficiile acestui demers. Aceste beneficii pot include îmbunătățirea abilităților și cunoștințelor de securitate cibernetică, creșterea securității organizaționale și protejarea datelor și a sistemelor împotriva atacurilor cibernetice.

Asigurați-vă că formarea este relevantă și actualizată: Este important să vă asigurați că formarea este relevantă și actualizată, luând în considerare tendințele și schimbările din domeniul securității cibernetice. Acest lucru poate fi realizat prin includerea unor exemple și cazuri relevante pentru organizație, precum și prin actualizarea formării în funcție de evoluțiile tehnologice și schimbările legislative.

Realizați o evaluare a învățării: După încheierea formării, este important să efectuați o evaluare a învățării pentru a vă asigura că obiectivele de învățare au fost îndeplinite și că angajații au dobândit cunoștințe și abilități utile în domeniul securității cibernetice. Această evaluare poate include un test sau o evaluare a competențelor, sau poate fi realizată prin intermediul feedback-ului angajaților și al rezultatelor obținute în urma aplicării cunoștințelor dobândite în activitățile lor de zi cu zi.

Notă: Anexă la acest document sunt testele de evaluare a personalului.

8. Alte aspecte legate de rețea și arhitectura pentru securitate cibernetică

Configurația rețelei din primărie face ca toate dispozitivele și serviciile să fie în același VLAN implicit, ceea ce poate duce la o vulnerabilitate în ceea ce privește securitatea și izolarea între diferitele segmente ale rețelei. De exemplu, un atac prin intermediul unui NVR poate afecta întreaga rețea și cripta. NVR-ul este un dispozitiv utilizat în sistemele de supraveghere video, care înregistrează și stochează imaginile capturate de camerele IP pe rețea. În comparație cu DVR-urile tradiționale, NVR-urile oferă mai multe avantaje, inclusiv o flexibilitate mai mare în ceea ce privește amplasarea și distanța dintre camere, capacitatea de a gestiona camerele IP cu rezoluții mai mari și accesul la înregistrări prin intermediul unui browser web sau a unei aplicații mobile. Acest lucru facilitează gestionarea și monitorizarea sistemelor de supraveghere video la distanță, dar poate crea și vulnerabilități în ceea ce privește securitatea rețelei.

Un scenariu de criză ar putea fi următorul: un hacker reușește să obțină acces la rețeaua primăriei prin intermediul unui dispozitiv vulnerabil, cum ar fi un NVR care nu a fost actualizat cu cele mai recente patch-uri de securitate. Odată ce hacker-ul intră în rețea, poate accesa toate dispozitivele și serviciile din VLAN-ul implicit, inclusiv cele care conțin informații sensibile sau confidențiale, cum ar fi bazele de date ale cetățenilor sau documente ale primăriei.

De exemplu, hacker-ul poate accesa camerele de supraveghere IP care sunt conectate la NVR-ul vulnerabil și poate obține acces la imaginile și înregistrările video stocate pe acesta. Dacă camerele sunt amplasate în zone strategice, cum ar fi birourile primăriei sau spațiile publice, hacker-ul ar putea să obțină informații sensibile, cum ar fi parole, date personale sau informații financiare.

Pentru a proteja rețeaua primăriei împotriva amenințărilor cibernetice, există câteva soluții robuste de securitate cibernetică care pot fi implementate:

1. Segmentarea rețelei - prin segmentarea rețelei în mai multe VLAN-uri, dispozitivele și serviciile pot fi izolate și protejate mai bine împotriva unui atac cibernetic. Segmentarea rețelei poate limita extinderea unui eventual atac și poate proteja împotriva accesului neautorizat la resursele critice.
2. Implementarea autentificării multifactor - implementarea autentificării multifactor (MFA) poate oferi un nivel mai ridicat de securitate prin cererea unui al doilea factor de autentificare, cum ar fi o parolă temporară sau o autentificare cu amprentă digitală. Acest lucru face mai dificilă obținerea accesului neautorizat la dispozitive și servicii din rețea.
3. Actualizarea regulată a dispozitivelor și serviciilor - actualizarea regulată a dispozitivelor și serviciilor din rețea este esențială pentru protejarea împotriva vulnerabilităților de securitate cunoscute. În plus, este important să se implementeze o politică de gestionare a patch-urilor de securitate și să se asigure că dispozitivele și serviciile sunt actualizate în mod regulat.
4. Monitorizarea rețelei - monitorizarea rețelei poate ajuta la detectarea activității suspecte și poate alerta echipa de securitate cu privire la eventuale atacuri. Aceasta poate implica utilizarea unor soluții de monitorizare a traficului de rețea sau a sistemelor de detectare a intruziunilor (IDS).
5. Formarea și educația angajaților - formarea și educația angajaților în ceea ce privește practicile de securitate cibernetică pot fi un pas important în protejarea rețelei primăriei. Angajații ar trebui să fie instruiți să recunoască și să raporteze activitatea suspectă și să ia măsuri pentru a proteja informațiile sensibile și confidențiale.

Implementarea acestor soluții robuste de securitate cibernetică poate ajuta primăria să se protejeze împotriva amenințărilor cibernetice și să protejeze informațiile sensibile ale cetățenilor și ale primăriei.

Detalieri

Segmentarea rețelei conduce la împărțirea rețelei fizice în mai multe sub-rețele logice (VLAN-uri). Fiecare VLAN este izolată de celelalte VLAN-uri, astfel încât dispozitivele și serviciile din fiecare VLAN să nu poată comunica direct cu cele din alte VLAN-uri, decât dacă acest lucru este expres permis.

Acest lucru poate fi realizat prin intermediul switch-urilor de rețea care sunt configurate pentru a crea VLAN-uri diferite. Fiecare VLAN are propriul său identificator unic și poate fi configurată cu setări specifice, inclusiv adrese IP, adrese MAC și politici de securitate. Dispozitivele și serviciile sunt apoi atribuite la VLAN-uri specifice, iar traficul de rețea este limitat numai la aceste VLAN-uri.

Prin segmentarea rețelei în mai multe VLAN-uri, dispozitivele și serviciile pot fi izolate și protejate mai bine împotriva unui atac cibernetic. Dacă o vulnerabilitate este exploatată pe un dispozitiv dintr-o anumită VLAN, atacatorul nu va putea să se extindă la alte dispozitive din alte VLAN-uri. Aceasta poate limita impactul unui atac cibernetic și poate proteja împotriva accesului neautorizat la resursele critice.

Pe lângă securitatea cibernetică, segmentarea rețelei poate oferi și alte beneficii, cum ar fi:

1. Reducerea traficului de rețea - prin segmentarea rețelei în mai multe VLAN-uri, traficul de rețea poate fi redus, deoarece traficul dintr-o VLAN nu va mai interfera cu traficul din alte VLAN-uri.
2. Îmbunătățirea performanței - prin reducerea traficului de rețea și îmbunătățirea fluxului de trafic, performanța rețelei poate fi îmbunătățită.

3. Îmbunătățirea flexibilității - prin segmentarea rețelei în mai multe VLAN-uri, dispozitivele și serviciile pot fi grupate în funcție de nevoile și cerințele specifice ale organizației.

Monitorizarea rețelei implică supravegherea și înregistrarea traficului de rețea, pentru a detecta activitatea suspectă și a alerta echipa de securitate în cazul unui potențial atac cibernetic.

Există mai multe tehnologii și soluții disponibile pentru monitorizarea rețelei, cum ar fi:

1. Monitorizarea traficului de rețea - aceasta implică înregistrarea și analizarea traficului de rețea pentru a detecta activitatea suspectă. Soluțiile de monitorizare a traficului de rețea pot analiza traficul de rețea în timp real și pot alerta echipa de securitate în cazul în care se detectează activitate suspectă.
2. Sisteme de detectare a intruziunilor (IDS) - aceste sisteme monitorizează traficul de rețea în căutarea semnelor de atac cibernetic și pot alerta echipa de securitate în cazul în care se detectează un atac cibernetic. IDS-urile pot utiliza semnături predefinite pentru a detecta atacurile cunoscute sau pot utiliza algoritmi de învățare automată pentru a detecta atacurile noi.
3. Sisteme de prevenire a intruziunilor (IPS) - aceste sisteme sunt similare cu IDS-urile, dar în plus pot bloca traficul suspect sau atacurile cibernetice identificate.
4. Sisteme de analiză a comportamentului utilizatorului - aceste sisteme monitorizează comportamentul utilizatorilor din rețea pentru a detecta activitatea suspectă, cum ar fi accesul neautorizat sau utilizarea neautorizată a resurselor.

În plus, propunem Primăriei Bistrița următoarea arhitectură de securitate cibernetică, împreună cu tehnologiile aferente:

1. Consolidarea firewall-ului de rețea cu module de inteligență artificială - primul pas în protejarea rețelei primăriei este implementarea unui firewall de rețea puternic. Firewall-ul de rețea poate filtra traficul de rețea și poate bloca traficul nedorit sau periculos. Acesta poate fi configurat pentru a permite accesul doar la serviciile autorizate și la utilizatorii autorizați.
2. Segmentarea rețelei - prin segmentarea rețelei în mai multe VLAN-uri, dispozitivele și serviciile pot fi izolate și protejate mai bine împotriva unui atac cibernetic. Segmentarea rețelei poate limita extinderea unui eventual atac și poate proteja împotriva accesului neautorizat la resursele critice.
3. Soluție de autentificare multifactor (MFA) - autentificarea multifactor (MFA) este o soluție de securitate cibernetică puternică care poate proteja împotriva accesului neautorizat la dispozitive și servicii din rețea. Aceasta poate fi configurată pentru a cere un al doilea factor de autentificare, cum ar fi o parolă temporară sau un cod de autentificare primit pe telefonul mobil, înainte de a permite accesul la dispozitiv sau la serviciu.
4. Criptare de date - pentru a proteja datele sensibile și confidențiale, se poate utiliza criptarea de date. Aceasta poate fi implementată la nivelul dispozitivelor și serviciilor din rețea, pentru a proteja datele în tranzit și în repaus.
5. Sisteme de detectare a intruziunilor (IDS) și sisteme de prevenire a intruziunilor (IPS) - aceste sisteme pot detecta și preveni atacurile cibernetice prin monitorizarea traficului de rețea și blocarea traficului suspect sau periculos.
6. Soluții de backup și recuperare a datelor - pentru a asigura disponibilitatea și integritatea datelor, este important să se implementeze soluții de backup și recuperare a datelor.

Acestea pot fi configurate pentru a asigura backup-ul și recuperarea datelor critice în cazul unui incident de securitate cibernetică sau a unei erori umane.

În plus, este important să se asigure că angajații primăriei sunt instruiți și educați în ceea ce privește practicile de securitate cibernetică și să se implementeze o politică de securitate cibernetică robustă și actualizată.

1. Firewall de rețea - un firewall de rețea poate fi implementat utilizând un dispozitiv hardware sau software dedicat, cum ar fi soluțiile de firewall UTM (Unified Threat Management) sau soluțiile de firewall bazate pe cloud. Firewall-ul poate fi configurat pentru a filtra traficul de rețea, în funcție de porturi, protocoale, adrese IP și alte criterii, și pentru a bloca traficul nedorit sau periculos, cum ar fi traficul de spam sau traficul de malware.
2. Segmentarea rețelei - segmentarea rețelei poate fi realizată prin utilizarea tehnologiei VLAN (Virtual Local Area Network), care permite crearea de rețele virtuale separate pe același switch de rețea. În plus, tehnologia SDN (Software-Defined Networking) poate fi utilizată pentru a crea segmente de rețea virtuală mai avansate, care permit o mai mare flexibilitate și scalabilitate.
3. Soluție de autentificare multifactor (MFA) - soluțiile de autentificare multifactor pot fi implementate la nivelul dispozitivelor și serviciilor din rețea, utilizând protocoale standard precum SAML (Security Assertion Markup Language) sau OAuth (Open Authorization). Soluțiile de MFA pot utiliza diferite metode de autentificare, cum ar fi parole temporare, token-uri de securitate, biometrie sau alte tehnologii de autentificare.
4. Criptare de date - criptarea de date poate fi implementată utilizând diverși algoritmi și protocoale de criptare, cum ar fi AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) sau TLS (Transport Layer Security). Criptarea de date poate fi aplicată la nivelul dispozitivelor sau la nivelul serviciilor de rețea, pentru a proteja datele în tranzit sau în repaus.
5. Sisteme de detectare a intruziunilor (IDS) și sisteme de prevenire a intruziunilor (IPS) - soluțiile IDS și IPS pot fi implementate utilizând dispozitive hardware sau software specializate, cum ar fi soluțiile de IDS/IPS bazate pe semnături sau soluțiile de IDS/IPS bazate pe comportament. Acestea pot fi configurate pentru a monitoriza traficul de rețea și a detecta activitatea suspectă, precum traficul de malware, scanarea porturilor sau alte tipuri de atacuri.
6. Soluții de backup și recuperare a datelor - soluțiile de backup și recuperare a datelor pot fi implementate utilizând soluții de stocare backup, soluții de replicare a datelor sau soluții de backup cloud. Acestea pot fi configurate pentru a asigura backup-ul și recuperarea datelor critice în cazul unui incident de securitate cibernetică sau a unei erori umane.

În plus, arhitectura de securitate cibernetică poate include și alte soluții și tehnologii, cum ar fi:

7. Soluții de autentificare pentru rețele VPN (Virtual Private Network) - soluțiile de autentificare pentru rețele VPN pot fi implementate pentru a proteja traficul de rețea între dispozitive și servicii din rețea care comunică prin intermediul unei rețele private virtuale (VPN). Soluțiile de autentificare pentru rețele VPN pot utiliza diferite protocoale, cum ar fi PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec (Internet Protocol Security) sau SSL (Secure Sockets Layer), pentru a asigura autentificarea și criptarea traficului de rețea.
8. Soluții de gestionare a parolelor - soluțiile de gestionare a parolelor pot fi implementate pentru a gestiona și a proteja parolele utilizatorilor și ale dispozitivelor din rețea. Acestea pot include soluții de stocare și gestiune a parolelor, soluții de generare automată a parolelor, soluții de autentificare multifactor și alte tehnologii de protecție a parolelor.

9. Soluții de securitate a e-mailului - soluțiile de securitate a e-mailului pot fi implementate pentru a proteja împotriva atacurilor cibernetice care utilizează e-mailul ca vector de atac. Acestea pot include soluții de filtrare a spamului, soluții de detecție și blocare a malware-ului primit prin e-mail, soluții de criptare a e-mailurilor și alte tehnologii de protecție a e-mailului.
10. Soluții de autentificare a aplicațiilor - soluțiile de autentificare a aplicațiilor pot fi implementate pentru a proteja împotriva accesului neautorizat la aplicațiile din rețea. Acestea pot include soluții de autentificare single sign-on (SSO), soluții de autentificare bazate pe token-uri, soluții de autentificare biometrică și alte tehnologii de autentificare a aplicațiilor.

9. Implementarea senzorilor de securitate cibernetică în rețea

Implementarea senzorilor de securitate cibernetică în rețea poate fi utilă pentru îmbunătățirea securității rețelei și prevenirea atacurilor cibernetice, prin detectarea și identificarea activităților suspecte în timp util.

Implementarea senzorilor de securitate cibernetică în rețea ar însemna instalarea unor dispozitive hardware sau software specializate care să monitorizeze traficul de rețea și să detecteze activitatea suspectă sau periculoasă. Acești senzori pot fi plasați strategic în rețea, astfel încât să poată monitoriza traficul de pe diferite segmente de rețea și să detecteze activitățile anormale care ar putea indica un atac cibernetic.

Senzorii de securitate cibernetică pot fi implementați utilizând diverse tehnologii, cum ar fi IDS (sisteme de detectare a intruziunilor), IPS (sisteme de prevenire a intruziunilor) sau soluții UTM (Unified Threat Management). Aceștia pot fi configurati pentru a monitoriza traficul de rețea în timp real, pentru a detecta comportamente suspecte sau activități neobișnuite, cum ar fi atacuri de tipul DDoS (Distributed Denial of Service), scanări de porturi, tentative de phishing sau alte tipuri de atacuri cibernetice.

Pe baza informațiilor colectate de senzorii de securitate cibernetică, echipa de securitate cibernetică poate lua măsuri de protecție și remediere a incidentelor, cum ar fi blocarea traficului suspect, alertarea administratorilor de sistem sau investigarea incidentului pentru identificarea surselor și a cauzelor atacului.

Implementarea acestor soluții și tehnologii poate ajuta Primăria Bistrița să construiască o arhitectură de securitate cibernetică robustă, care să protejeze informațiile și serviciile critice împotriva atacurilor cibernetice.

Senzorii de securitate cibernetica trebuie sa aibă următoarele specificații:

1. Capacitate de procesare - senzorii trebuie sa fie capabili sa proceseze traficul de rețea in timp real si sa detecteze activitățile suspecte sau periculoase. Capacitatea de procesare poate varia in funcție de viteza si de capacitatea de stocare a senzorilor.
2. Viteza de procesare - senzorii trebuie sa fie capabili sa proceseze traficul de rețea la viteze ridicate, astfel încât sa nu încetinească performanța rețelei. Acest aspect este important pentru a asigura detectarea rapida a amenințărilor cibernetice si pentru a minimiza impactul asupra performantei rețelei.
3. Flexibilitate - senzorii trebuie sa fie configurabili si personalizabili pentru a răspunde la nevoile specifice ale organizației si ale rețelei. Aceasta poate include posibilitatea de a configura si

personaliza politici de securitate, de a ajusta nivelurile de alerta si de a adapta senzorii la diverse scenarii de securitate.

4. Capacitatea de a detecta diverse tipuri de atacuri - senzorii trebuie sa fie capabili sa detecteze si sa identifice diverse tipuri de atacuri, precum atacuri de tipul DDoS, scanări de porturi, tentative de phishing sau alte tipuri de atacuri cibernetice.
5. Tehnologii de analiza si de detecție avansate - senzorii pot utiliza tehnologii avansate de analiza si de detecție, precum inteligenta artificiala, machine learning sau analiza comportamentala, pentru a identifica modele de trafic suspect si pentru a oferi o detecție precisă și eficientă a amenințărilor cibernetice.
6. Integrare cu soluțiile de securitate cibernetică existente - senzorii trebuie sa poată fi integrați cu soluțiile de securitate cibernetica existente, precum soluțiile IDS, IPS sau soluțiile UTM, pentru a oferi o protecție completa si integrata a rețelei.
7. Facilități de gestionare si de raportare - senzorii trebuie sa ofere facilități de gestionare si de raportare, pentru a permite administratorilor de sistem sa monitorizeze starea senzorilor si sa ofere rapoarte de securitate si de incidente cibernetice. Acestea pot include console de management centralizat si interfețe de raportare ușor de utilizat.

Exemple de biblioteci si module Python care pot fi utilizate pentru implementarea senzorilor de securitate cibernetica:

1. Scapy - biblioteca Python pentru manipularea si crearea de pachete de rețea. Aceasta poate fi utilizata pentru a captura, analiza si modifica traficul de rețea, precum si pentru a implementa diverse tehnici de detectare a amenințărilor cibernetice.
2. Suricata - un sistem de detectare a intruziunilor bazat pe retele, care poate fi utilizat pentru a detecta si a preveni atacuri cibernetice. Suricata utilizeaza un motor de detectare de tipul IDS si IPS, si ofera o gama larga de tehnici si reguli de detectare.
3. Bro - un sistem de monitorizare a retelei, care poate fi utilizat pentru a captura si analiza traficul de retea, precum si pentru a detecta si preveni atacuri cibernetice. Bro utilizeaza un motor de detectare de tipul IDS si ofera o gama larga de tehnici si reguli de detectare.
4. Snort - un sistem de detectare a intruziunilor bazat pe retele, care poate fi utilizat pentru a detecta si preveni atacuri cibernetice. Snort utilizeaza un motor de detectare de tipul IDS si ofera o gama larga de tehnici si reguli de detectare.

Implementarea unui senzor de securitate cibernetica este o sarcina complexa si necesita o expertiza tehnica si cunostinte solide in domeniul securitatii cibernetice. Implementarea poate include utilizarea unor biblioteci si module specifice de securitate cibernetica, care pot fi integrate in codul Python. Un exemplu simplu de cod Python pentru implementarea unui senzor de detectare a atacurilor de tipul DDoS, utilizand biblioteca Pyshark si protocolul de detectare a atacurilor DDoS SYN Flood este:

```
import pyshark

capture = pyshark.LiveCapture(interface='eth0')
for packet in capture.sniff_continuously():
    if packet.tcp.flags_syn == '1':
        # detectare SYN Flood attack
        print("Atac SYN Flood detectat!")
```

Acest cod utilizeaza biblioteca Pyshark pentru a captura traficul de retea si a verifica daca fiecare pachet TCP are setat bitul de flag SYN (Synchronize). Daca bitul este setat, senzorul poate identifica un atac DDoS de tipul SYN Flood.

Senzor de detectare a atacurilor de tipul SQL Injection - acest senzor utilizeaza biblioteca PyMySQL pentru a detecta atacurile de tipul SQL Injection pe baza de request-uri de tipul GET si POST, prin analizarea datelor de intrare si detectarea tentativelor de injectare a codului SQL malitios in query-uri. Partea de cod ar putea arata astfel:

```
import pymysql
import re

def detect_sql_injection(query):
    pattern = re.compile(r"\b(select|update|delete|insert|drop|create)\b", re.IGNORECASE)
    if pattern.search(query):
        return True
    return False

def on_request(request):
    query = request.args.get("query", "")
    if detect_sql_injection(query):
        # detectare atac SQL Injection
        print("Atac SQL Injection detectat!")
```

Senzor de detectare a atacurilor de tipul Cross-Site Scripting (XSS) - acest senzor utilizeaza biblioteca Flask pentru a detecta atacurile de tipul XSS pe baza de request-uri de tipul GET si POST, prin analizarea datelor de intrare si detectarea tentativelor de injectare a codului JavaScript malitios in paginile web. Partea de cod ar putea arata astfel:

```
from flask import Flask, request
import re

app = Flask(__name__)

def detect_xss(data):
    pattern = re.compile(r"<script.*?>.*?</script>", re.IGNORECASE | re.DOTALL)
    if pattern.search(data):
        return True
    return False

@app.route("/")
def index():
    name = request.args.get("name", "")
    if detect_xss(name):
        # detectare atac XSS
        print("Atac XSS detectat!")
    return "Hello, " + name + "!"

if __name__ == "__main__":
```

```
app.run()
```

Senzor de detectare a atacurilor de tipul Distributed Denial of Service (DDoS) - acest senzor utilizeaza biblioteca Scapy pentru a detecta atacurile de tipul DDoS prin analizarea traficului de retea si detectarea schimbarilor bruste in ratele de trafic si in pattern-urile de trafic. Partea de cod ar putea arata astfel:

```
import scapy.all as scapy

def detect_ddos():
    pkt = scapy.sniff(count=10, filter="icmp or udp or tcp")
    if len(pkt) > 5:
        # detectare atac DDoS
        print("Atac DDoS detectat!")

while True:
    detect_ddos()
```

Senzor de detectare a atacurilor de tipul Man-in-the-Middle (MitM) - acest senzor utilizeaza biblioteca Scapy pentru a detecta atacurile de tipul MitM, prin analizarea traficului de retea si detectarea schimbarilor bruste in adresele MAC si IP si in pattern-urile de trafic. Partea de cod ar putea arata astfel:

```
import scapy.all as scapy

def detect_mitm():
    pkt = scapy.sniff(count=10, filter="arp or udp or tcp")
    for p in pkt:
        if p.haslayer(scapy.ARP) and p[scapy.ARP].op == 2:
            # detectare atac MitM
            print("Atac MitM detectat!")

while True:
    detect_mitm()
```

Senzor de detectare a atacurilor de tipul Brute-Force - acest senzor utilizeaza biblioteca Flask pentru a detecta atacurile de tipul Brute-Force prin analizarea tentativelor repetate de logare cu combinatii de nume de utilizator si parole incorecte. Partea de cod ar putea arata astfel:

```
from flask import Flask, request
import time

app = Flask(__name__)

def detect_brute_force(username, password):
    attempts = {}
    now = time.time()
    if username in attempts:
        if attempts[username]["count"] > 3 and (now - attempts[username]["last"]) < 60:
```

```
            # detectare atac de tipul Brute-Force
            print("Atac Brute-Force detectat!")
        else:
            attempts[username]["count"] += 1
            attempts[username]["last"] = now
    else:
        attempts[username] = {"count": 1, "last": now}

@app.route("/")
def login():
    username = request.args.get("username", "")
    password = request.args.get("password", "")
    detect_brute_force(username, password)
    return "Hello, " + username + "!"

if __name__ == "__main__":
    app.run()
```

Senzor de detectare a atacurilor de tipul Phishing - acest senzor utilizeaza biblioteca Beautiful Soup pentru a analiza paginile web si a detecta tentativelor de phishing prin analizarea URL-urilor si a textului paginii. Partea de cod ar putea arata astfel:

```
from bs4 import BeautifulSoup
import requests

def detect_phishing(url):
    html = requests.get(url).text
    soup = BeautifulSoup(html, "html.parser")
    text = soup.get_text()
    if "bank" in url and "login" in url and "password" in text:
        # detectare atac de tipul Phishing
        print("Atac de tipul Phishing detectat!")

detect_phishing("http://www.example.com/bank/login.php")
```

Senzor de detectare a atacurilor de tipul Cross-Site Request Forgery (CSRF) - acest senzor utilizeaza biblioteca Flask pentru a detecta atacurile de tipul CSRF prin analizarea headerelor HTTP si detectarea tentativelor de executare a unor actiuni malitioase prin intermediul request-urilor HTTP. Partea de cod ar putea arata astfel:

```
from flask import Flask, request

app = Flask(__name__)

def detect_csrf():
    if request.method == "POST":
        if "Origin" in request.headers and request.headers["Origin"] != "http://www.example.com":
            # detectare atac de tipul CSRF
            print("Atac de tipul CSRF detectat!")
```

```
@app.route("/transfer", methods=["POST"])
def transfer():
    detect_csrf()
    # transferul banilor
    return "Transfer realizat cu succes!"

if __name__ == "__main__":
    app.run()
```

Senzor de detectare a atacurilor de tipul Remote Code Execution (RCE) - acest senzor utilizeaza biblioteca Paramiko pentru a detecta atacurile de tipul RCE prin analizarea conexiunilor SSH si detectarea tentativelor de executare a unor comenzi malitioase prin intermediul acestora. Partea de cod ar putea arata astfel:

```
import paramiko

def detect_rce():
    client = paramiko.SSHClient()
    client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    try:
        client.connect("example.com", username="user", password="pass")
        # executare comanda malitioasa
        stdin, stdout, stderr = client.exec_command("rm -rf /")
        # detectare atac de tipul RCE
        print("Atac de tipul RCE detectat!")
    except:
        pass

while True:
    detect_rce()
```

Senzor de detectare a atacurilor de tipul Malware - acest senzor utilizeaza biblioteca VirusTotal API pentru a detecta si analiza fisierele suspecte prin intermediul serviciului online VirusTotal. Partea de cod ar putea arata astfel:

```
import requests

def detect_malware(file_path):
    url = "https://www.virustotal.com/vtapi/v2/file/scan"
    params = {"apikey": "your_api_key"}
    files = {"file": ("file", open(file_path, "rb"))}
    response = requests.post(url, files=files, params=params)
    scan_id = response.json()["scan_id"]
    url = "https://www.virustotal.com/vtapi/v2/file/report"
    params = {"apikey": "your_api_key", "resource": scan_id}
    response = requests.get(url, params=params)
    if response.json()["positives"] > 0:
        # detectare fisier malitios
```

```
    print("Fisier malitios detectat!")

detect_malware("path/to/file.exe")
```

Machine Learning poate fi folosit pentru a consolida firewall-ul prin crearea unor modele care pot detecta si preveni atacurile cibernetice in timp real. Exemple de algoritmi de Machine Learning care pot fi folositi in acest scop sunt:

1. Random Forest - acest algoritm de tip ensemble poate fi utilizat pentru a detecta atacuri de tipul port scanning sau brute force attacks. Random Forest poate fi antrenat cu un set de date care contine caracteristici specifice ale traficului de retea, cum ar fi numarul de pachete trimise catre un anumit port sau frecventa cu care un anumit IP adrese trimite request-uri catre server. Modelul antrenat poate fi apoi integrat in firewall pentru a detecta si preveni atacurile in timp real.
2. Support Vector Machines (SVM) - acest algoritm poate fi folosit pentru a detecta atacuri de tipul SQL injection sau cross-site scripting (XSS). SVM poate fi antrenat cu un set de date care contine caracteristici specifice ale request-urilor HTTP, cum ar fi lungimea request-ului sau numarul de caractere speciale. Modelul antrenat poate fi apoi integrat in firewall pentru a detecta si preveni atacurile in timp real.
3. Neural Networks - acest algoritm poate fi folosit pentru a detecta atacuri complexe de tipul zero-day, care nu sunt cunoscute si nu sunt detectate de sistemele de securitate clasice. Neural Networks poate fi antrenat cu un set de date care conține caracteristici specifice ale traficului de retea si modele de trafic normal. Modelul antrenat poate fi apoi integrat in firewall pentru a detecta si preveni atacurile in timp real.

Există mai multe tipuri de modele de Neural Networks care pot fi utilizate pentru a detecta atacuri cibernetice în timp real, fiecare cu avantaje și dezavantaje specifice. Exemple de modele potrivite pentru această sarcină sunt:

1. Recurrent Neural Networks (RNN) - aceste modele pot fi utilizate pentru analiza traficului de rețea în timp real, pentru a detecta atacuri cibernetice de tipul zero-day. RNN-urile sunt utile pentru a identifica modele ascunse în traficul de rețea și pentru a detecta anomalii în timp real.
2. Convolutional Neural Networks (CNN) - aceste modele pot fi utilizate pentru analizarea traficului de rețea pentru a detecta atacuri de tipul malware, deoarece aceste atacuri sunt adesea însoțite de diferite tipuri de semnale și modele de trafic de rețea. CNN-urile sunt utile pentru a detecta tipare și structuri în traficul de rețea.
3. Generative Adversarial Networks (GAN) - aceste modele pot fi utilizate pentru a identifica și a înlătura intruziunile de rețea în timp real, prin crearea unui model de trafic normal și compararea acestuia cu traficul în timp real pentru a detecta semnale de atac. GAN-urile sunt utile pentru a genera și valida modele de trafic normal și pentru a detecta semnale de atac și intruziuni în timp real.

Antrenarea acestor modele de Neural Networks necesită seturi mari de date pentru a asigura o performanță optimă.

XI Tinte Măsurabile de Progres

A. Ținte măsurabile pentru maturizarea digitalizării proceselor administrative

1. Existența controalelor de intrare a datelor (*data input controls*), examinabile și evaluabile (*Review and evaluate data input controls*)

2. Existența controalelor asupra fluxurilor de date către și de la sistemele de interfață, examinabile și evaluabile

3. Execuția de procese periodice de „sincronizare" pentru a detecta orice inconsecvență în date, în cazul în care aceleași date sunt păstrate în mai multe baze de date și/sau sisteme

4. Examinarea periodica și evaluarea pistelor de audit prezente în sistem și realizarea de controale periodice asupra acestor teste de audit.

5. Existența posibilității ca sistemele de baze de date utilizate să ofere un mijloc de a urmări o tranzacție sau o bucată de date de la începutul până la sfârșitul procesului activat de sistem.

6. Existența de mecanisme de autentificare a utilizatorului pe baza, cel puțin, a unui identificator unic pentru fiecare utilizator și a unei parole confidențiale, la nivelul aplicațiilor.

7. Existența unui mecanism de securitate/autorizare a sistemelor, cu funcție de administrator cu controale și funcționalități adecvate.

8. Existența in cadrul aplicațiilor a controalelor adecvate pentru parolă.

9. Existența mecanismelor prin care utilizatorii sunt deconectați automat de la aplicații după o anumită perioadă de inactivitate.

10. Existența tehnicilor de criptare pentru a se proteja datele aplicațiilor.

11. Efectuarea de verificări privitor la acordarea corespunzătoare a permisiunilor bazei de date pentru nivelul de autorizare necesar.

12. Efectuarea de verificări privitor la revocarea corespunzătoare a permisiunilor bazei de date pentru nivelul de autorizare necesar.

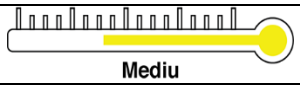
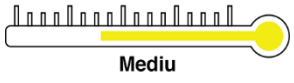
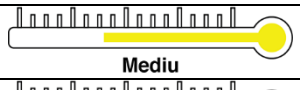
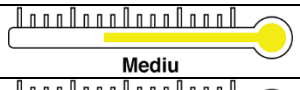
13. Restricționarea permisiunilor pentru directoarele în care sunt instalate baze de date

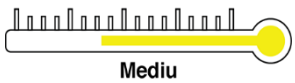
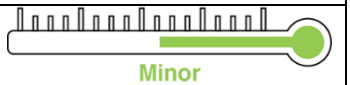
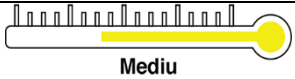
14. Verificarea existenței unor cuvinte de acces ușor de ghicit, caz în care acestea trebuie să fie rapid înlocuite.

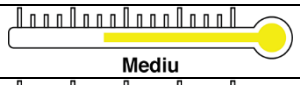
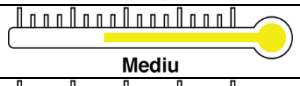
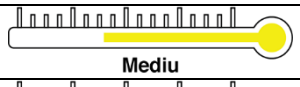
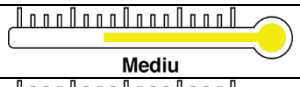
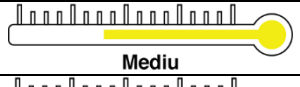
B. Ținte măsurabile pentru maturizarea proceselor de securitate cibernetică

- frecvența cu care se face controlul datelor de intrare
- frecvența backup-urilor de pe server
- siguranța stocării datelor, inclusiv a backup-ului
- nivelul de vulnerabilitate la atacuri cibernetice de tip inginerie socială
- nivelul de vulnerabilitate la atacuri cibernetice de tip „brut force” / DDoS
- frecvența actualizării parolelor
- nivelul de protecție la autentificare
- nivelul de protecție în stocarea parolelor
- gradul de îndeplinire al articolelor GDPR
- capacitatea de recuperare în caz de incidente (timp, calitate, cantitate)
- gradul de instruire nivel 1, 2 și 3 a angajaților din Primărie pe securitate cibernetică, inclusiv frecvența de actualizare a instruirii și instruirea noilor angajați
- frecvența testelor de vulnerabilitate (pentest).

C. Ținte de progres pentru infrastructura IT

1	Proceduri interne de lucru.	
2	Documentație aferentă sistemului IT.	
3	Politici de organizare.	
4	Securitate fizică în sala serverelor	
5	Detecție-stingere incendiu	
6	Climatizare	
7	Monitorizare temperatură	
8	UPS-uri	

19	Cablarea structurată campus	
20	Securitate în LAN	
21	Switch-uri acces	
22	Switch-uri core	
23	Control activitate utilizatori	
24	Wireless	
25	Monitorizare	
26	Active Directory – concluzii generale	

9	Generator	
10	Dulapuri de comunicații	
11	Cablare structurată sală servere	
12	Acces la internet	
13	VPN-uri	
14	Securitate WAN sediu central	
15	Securitate WAN sucursale	
16	Firewall dedicat	
17	Vulnerabilități servicii WAN	
18	DNS	

27	Infrastructură servere fizice	
28	Infrastructură echipamente de stocare	
29	Infrastructură virtualizare	
30	Business continuity	

Nota: Este nevoie ca, in cazul fiecărui indicator dintre cei 18 prin care se măsoara țintele de progres la nivelul infrastructurii hardware a Primăriei Municipiului Bistrița, să se ajunga la starea OK.

XII Recomandări

A. Recomandări privind Evitarea Efectului de „Client Captiv”

În contractele care prevăd achiziția de produse și servicii ITC, în mod special în cele care includ achiziția de componente software (produse) sau dezvoltare de componente software (servicii), exista un risc sporit fata de alte domenii să se instaleze efectul de captivitate ("vendor lock-in") între achizitor și furnizor.

Efectul de captivitate este starea în care beneficiarul de produse sau servicii nu poate exploata, integral sau parțial, produsul sau serviciul achiziționat, respectiv nu poate extinde, modifica, interfață livrabilele achiziționate, sau nu poate accesa și procesa independent informațiile generate de către aplicațiile achiziționate (baze de date, fișiere, etc) fără asistența furnizorului inițial sau fără achiziția unor servicii suplimentare din partea furnizorului inițial, în condiții care limitează atât eficiența operațională, cât și pe cea financiara, și contravine principiului competitivității, datorită obligației de facto de a realiza achizițiile subsecvente de la un singur ofertant.

O alta dimensiune a efectului de captivitate este reprezentată de "captivitatea tehnologica", prin care beneficiarul este limitat în a schimba tehnologia sau componentele tehnologice ale sistemelor achiziționate, chiar dacă poate achiziționa servicii de la mai mulți furnizori. Cazuri clasice, documentate, în aceasta privință, uneori combinate cu captivitatea fata de furnizori, au fost generate de produse SAP, Oracle, Microsoft.

Efectul de captivitate, fie că este urmărit activ de către furnizor, fie că apare accidental datorită neatenției achizitorului la elementele esențiale pe care le vom detalia în continuare, este foarte des întâlnit, atât printre beneficiarii instituții publice cât și în piață privata, și crează pierderi cumulate considerabile, directe de productivitate (prin limitarea capacității de exploatare a produsului/serviciului achiziționat), directe financiare (prin obligația negocierii cu un singur furnizor în condiții dictate de acesta) și de oportunitate (prin blocarea unor dezvoltări ulterioare, limitarea reutilizării datelor, limitarea sau întârzierea interoperabilizarii, etc). De asemenea efectul de captivitate creste probabilitatea că produsele/serviciile achiziționate să aibă un cost de înlocuire ("switching cost") mult mai mare.

La nivelul Uniunii Europene, efectul de captivitate este tratat în studii, ghiduri și recomandări.

În acest sens relevante sunt:

Guidelines for Public Procurement of ICT Goods and Services – Overview of

Procurement Practices (2012)

Guide for the procurement of standards-based ICT — Elements of Good Practice - Against lock-în: building open ICT systems by

making better uşe of standards în public procurement (25.6.2013)

Unele state membre au adoptat în cadrul legislației aplicabile achizițiilor publice reguli mai ferme, care crează obligații, reflectate în caietele de sarcini, contractele de furnizare și procesul de recepție (Olanda, UK, Norvegia etc). Reglementările sunt în general legate de obligativitatea includerii utilizării standardelor deschise că și criteriu de selecție în procedurile de achiziție (nivelul de recomandare fiind deja prezent în strategiile și ghidurile europene), încurajarea activa a utilizării soluțiilor open source fata de cele proprietare prin punctare favorabila în evaluarea ofertelor, limitarea duratei de valabilitate a contractelor de furnizare la maxim 5 ani, etc.

În Romania, recomandările strategiei pentru agenda digitala europeana, care includ aspecte de natura să limiteze efectul de captivitate (utilizarea standardelor deschise, utilizarea soluțiilor open source) sunt preluate în Strategia pentru Agenda Digitala a României, însă nu au trecut de nivelul de recomandare.

În 2016, ANIS în colaborare cu ANAP și Secretariatul General al Guvernului a elaborat o prima versiune a unui ghid special dedicat achizițiilor publice de software (Ghid de achiziții software pentru instituțiile publice, 1 decembrie 2016). Ghidul tratează în detaliu ciclul de viață al achiziției de software și poate fi un ajutor consistent pentru pregătirea achiziției (realizarea caietelor de sarcini, stabilirea criteriilor de calificare și de atribuire, elaborarea modelului de contract), evaluare, recepție și gestiunea relației cu furnizorul.

A doua versiune a ghidului, publicata în 2 martie 2018, conține o adăugire importanta pentru limitarea efectului de captivitate, recomandând includerea în cerințele caietului de sarcini a unui "Planul de transfer al cunoștințelor tehnice", subiect la care vom reveni mai jos.

În mai 2019, Consiliul Concurentei a publicat un “Studiu privind efectul de captivitate (lock-în) în sectoarele sensibile în domeniul achizițiilor publice, IT și echipamente/aparatura medicala”.

Este salutara atenția Consiliului Concurentei la acest subiect, atât prin sublinierea evidentei numărului mare de achiziții care induc sau perpetuează efectul de captivitate, cât și prin încercarea de a da recomandări privind evitarea acestei situații. Desi sunt citate recomandările europene pe acest subiect, este evident că studiul a fost făcut fară aportul eficient al specialiștilor în domeniul IT și conține recomandări care sunt în opinia noastră dubitabile sau cu risc de a produce efecte adverse, prin urmare recomandam că sursa principala a recomandărilor să fie Ghidul ANIS, alaturi de elementele pe care le vom prezenta în continuare.

Limitarea potențialității de captivitate trebuie avuta în vedere pe tot parcursul proceselor de achiziție, recepționare, punere în funcțiune și expoatare a sistemului software achiziționat.

În mod particular, prevederi explicite trebuie să fie conținut în Caietul de sarcini și în Contractul de furnizare.

Prevederile esențiale care trebuie avute în vedere sunt grupate în 3 capitole:

- prevederi privind licențierea

- prevederi privind documentarea

- prevederi privind transferul cunoștințelor tehnice

Licențierea este aspectul determinant, care reglementează drepturile pe care achizitorul le dobândește în urma achiziției.

Având în vedere că avem atât situații în care se realizează achiziția unui produs deja existent, cât și cazuri în care se achiziționează un serviciu de dezvoltare pentru realizarea unei aplicații noi specifice cerințelor achizitorului, dar și cazuri combinate, în care în livrabilul finit sunt include atât produse realizate anterior, uneori relicentiate, cât și aplicații noi, care extind sau complementeaza produsele, condițiile de licențiere trebuie adaptate situației.

Proprietate patrimoniala asupra tuturor datelor generate de către sistemele achiziționate, asupra bazei de date, a documentelor/fișierelor generate, sau alte structuri de date daca este cazul

În oricare dintre cazuri, indiferent daca achiziționam produs finit existent de tip COTS (Commercial off-the-shelf) sau servicii de dezvoltare, proprietatea asupra datelor trebuie să fie asigurata explicit.

Este preferabil să nu interpretam că implicit faptul că achizitorul dobândește acest drept ci să prevedem explicit acest lucru atât în caietul de sarcini cât și în contractul de furnizare.

Accesibilitatea și documentarea bazelor de date și a altor structuri de stocare a informației generate

Din nou aplicabila oricărei forme de achiziție, este esențial să fie prevăzută în caietul de sarcini și contract, dar și să facă parte explicit din procesul de recepție și să fie consemnat că atare în procesul verbal aferent.

Prin accesibilitate înțelegem accesul neîngrădit, direct și prin orice aplicație tertă compatibila, la baza de date și la datele generate, furnizorul oferind datele de autentificare necesare (daca e cazul). În cazul în care condițiile de securitate sau cele tehnologice fac dificil sau imposibil accesul direct la sursa primara a datelor, trebuie cel puțin asigurata, contractual și faptic, probata în cadrul recepției, posibilitatea de a realiza exporturi complete a tuturor datelor într-o forma procesabila, în orice moment și fară a necesita intervenția furnizorului. Aceasta varianta se poate utiliza de exemplu pentru cazurile în care se achiziționează sericii în regim SaaS, caz în care nu este posibila oferirea accesului direct la ţoață baza de date (aceasta fiind partajata și altor clienți).

Vom trata în continuare doua aspecte distincte care trebuie avute în vedere în tratarea licențierii:

- licențierea pentru exploatare

- licențierea pentru modificare și extindere

Achizitorul trebuie să își asigure dreptul neîngrădit de exploatare a bunului achizititionat, astfel încât să evite să fie pus în obligația de a relua achiziția în viitor doar pentru a putea în continuare să își desfășoare activitatea sau pentru a folosi datele pe care le-a generat prin procesele operaționale. Astfel, produsul achiziționat sau aplicația rezultata în urma unui serviciu achiziționat trebuie să aibă asigurata licențierea perpetua pentru exploatare. Trebuie de asemenea urmărit că licențierea să nu fie condiționată de rularea într-un anumit sistem impus pentru prevenirea replicării sau reutilizării aplicației, cum ar fi de exemplu limitarea de a rula pe un anumit server (restricție pe baza de hardware). În situațiile în care condițiile de licențiere ale furnizorului sunt de natura limitativa (aplicații care pot rula pe un singur computer la un moment

dat, OEM, etc) este esențial că aceste condiții să fie clare, prevăzute în contract și defavorizate prin criteriile de atribuire aplciate la achiziție în cazul în care exista pe piață alternative care permit o libertate mai mare. În cazul achizițiilor de produse în regim SaaS, când se cumpără un drept de eploatare explicit limitat în timp, trebuie asigurata posibilitatea de export a informațiilor generate astfel încât ele să poată fi ulterior utilizate în cazul în care contractul nu mai este continuat.

În cazul achiziției unor produse software, pe lângă asigurarea licențierii pentru exploatare perpetua, este esențială asigurarea serviciului de mentenanță, atât că garanție pentru remedierea eventualelor probleme (erori funcționale - "bugs") ale aplicației achiziționate, cât și pentru asigurarea unor actualizări specifice atunci când este necesar fară a genera un cost arbitrar impus de furnizor (de exemplu, o aplicație de contabilitate trebuie actualizata de către furnizor în cazul în care au loc modificări legislative). Acest tip de mentenanță, care prevede actualizări periodice sau când sunt îndeplinite anumite condiții, trebuie întotdeauna avuta în vedere în cazul achiziției de soluții bazate pe platforme Open Source. Chiar daca achiziția unei soluții Open Source nu crează efect de captivitate, tocmai natura publica a codului implica un risc de vulnerabilitate la atacuri din exterior (cu atât mai mare cu cât platforma respectiva este mai larg utilizata), risc care trebuie contracarat prin actualizări periodice (patches, updates) care de obicei sunt oferite de către dezvoltatorii acestor platforme.

Recomandam că în cazurile unde este prezenta necesitatea mentenanței de tip patch/update sau adaptări legislative aceasta cerință să se regăsească în caietele de sarcini și în contract, cu un termen recomandat de 36 de luni.

3 ani calendaristici reprezintă o perioada rezonabila de exploatare a unei aplicații în forma să inițială de implementare, atât funcțional cât și tehnologic, dar trebuie avut în vedere că în acest timp necesitățile sau oportunitățile funcționale este probabil să evolueze, iar tehnologiile să se perimeze, așadar după 3 ani este oportun să se evalueze oportunitatea unor modificări mai substanțiale.

Recomandam că pentru garanția împotrivă erorilor de implementare să se solicite 12 luni, timp suficient pentru a identifica problemele unei aplicații în exploatare.

Licențierea pentru modificare și extindere

În cazul achiziției unor servicii de dezvoltare software este esențial că achizitorul să își asigure dreptul de a putea modifica sau extinde aplicațiile livrate, fie prin forte proprii, fie achiziționând servicii de la alti furnizori, fără a fi necesar să apeleze la furnizorul inițial.

Pentru aceasta este necesar să fie asigurate două condiții:

Achizitorul să aibă acces efectiv la codul sursa a aplicației. Chiar dacă în producție aplicația poate fi un rezultat compilat al codului sursa, prin caietul de sarcini trebuie cerut, prin contract precizat și la recepție verificat, că achizitorul să obțină o copie a codului sursa a aplicației

Codul sursa trebuie să fie documentat, astfel încât să permită unui furnizor terț să îl înțeleagă și să îl extindă sau modifice fară a fi necesar să inducă un cost semnificativ suplimentar pentru înțelegerea codului

Planul de transfer al cunoștințelor tehnice

În cazul achiziției de servicii de dezvoltare, în urma cărora este livrat cod sursa, este recomandat că pe lângă asigurarea și probarea documentarii codului să aibă loc și un proces de transfer efectiv al cunoștințelor în cadrul unei sau unor întâlniri intre reprezentanții furnizorului și personalul tehnic al achizitorului, întâlniri în cadrul cărora furnizorul să prezinte în detaliu aplicația din perspectiva tehnica. Daca acest lucru nu este fezabil la recepție, de exemplu pentru că furnizorul nu deține personal specializat, este recomandat că procesul de transfer să poată fi realizat oricând la solicitarea achizitorului în cursul perioadei de mentenanță agreate, fară a necesita costuri suplimentare din partea achizitorului. Astfel, achizitorul poate în acest timp să contracteze furnizori terti, care să beneficieze direct la momentul oportun de procesul de transfer a cunoștințelor din partea furnizorului inițial

Considerații privind proprietatea patrimoniala asupra codului sursa

În aceasta privință susținem poziția exprimata în Ghidul realizat de ANIS (un link direct se regăsește la finalul documentului), prin care se subliniază importanta drepturilor efectiv utile achizitorului de tip instituție publica și recomandarea de a nu forță obținerea unor drepturi suplimentare care nu pot fi valorificate (în principiu, instituția publica nu urmărește exploatarea comerciala a unui produs achiziționat) dar pot fi de natura să limiteze sau descurajeze concurenta intre furnizori și să duca la oferte mai puține și mai slabe calitativ.

În mod particular este de evitat cerință de transfer în mod exclusiv a drepturilor de proprietate patrimoniala asura codului. Pe de o parte în multe cazuri acest lucru nu poate fi realizat datorita includerii în aplicații a unor componente sau secvențe de cod deja utilizate în cadrul altor implementări, pe de alta parte este puternic descurajant pentru potențiali furnizori care altfel ar putea da oferte foarte favorabile achizitorului considerand posibilitatea de a recomercializa anumite rezultate ale implementării.

Considerații privind Open Source

Tehnologiile Open Source prezinta avantajul important de a nu genera efect de captivitate. Totuși, trebuie avut în vedere că ele nu sunt în mod necesar mai performante sau mai sigure fata de alternative.

La achiziționarea de sisteme Open Source, sau de servicii de dezvoltare bazate pe platforme Open Source, în cazul în care achizitorul favorizează aceasta varianta, este recomandat să aibă în vedere de asemenea în grila de punctaj că:

- securitatea platformei Open Source să fie probata (de obicei prin banchmarks publice) și să fie evidențiat faptul că platforma este monitorizata din perspectiva securității și actualizata periodic (patched). Aceste aspecte sunt publice în cazul platformelor serioase

- dimensiunea comunității dezvoltatorilor și dinamica adopției platformei în piață - O companie poate declara că Open Source o platforma dezvoltata de aceasta, dar daca nu exista o comunitate de dezvoltatori în afara companiei respective, respectiv daca nu exista suficienți de mulți clienți care să fi implementat platforma fie prin forte proprii, fie prin intermediul altor furnizori decât producătorul inițial, atunci respectiva platforma, desi nominal poate fi Open Source, este în clar avantaj fata de platformele cu comunități active și piață dinamica

B. Recomandări privind Oportunitatea Educației Digitale a funcționarilor publici din cadrul Primăriei Municipiului Bistrița și a Instituțiilor Subordonate

În cursul procesului de audit și evaluare s-a evidențiat, atât prin analiza directa cât și prin discuțiile realizate cu conducătorii departamentelor, necesitatea și oportunitatea dezvoltării unui program de educație continua pentru funcționarii publici cu o componenta de bază reprezentată de abilitățile privind utilizarea eficienta a aplicațiilor informatice și capacitatea de adaptare la introducerea în activitatea curenta a suportului asigurat de sisteme informatice noi.

S-a evidențiat faptul că după încheierea Programului National de Certificare a Funcționarilor Publici (proiectul ECDL - ANFP) nu au mai avut loc acțiuni sistematice de educare digitală și actualizare a nivelului de educație digitală, nici în rândul angajaților existenți nici pentru cei care au fost angajați ulterior finalizării proiectului național amintit. S-a dovedit în practică a fi incorect și ineficient să folosim ipoteza că adaptarea și învățarea se poate realiza implicit, de la sine, prin simpla expunere generală a populației la unelte informatice uzuale, cum sunt browserele internet, dispozitivele smartphone, sistemele de teleconferință sau editoarele de text și de calcul tabelar, respectiv în cadrul instituției doar prin obligația instituita, formal prin proceduri interne sau informal, de a utiliza anumite aplicații informatice pentru a îndeplini anumite sarcini.

rmatice noi.

Astfel, se evidențiază practic faptul că exista discrepante semnificative în nivelul de pregătire și adaptare a personalului pentru utilizarea aplicațiilor informatice, că exista uneori dificultăți inclusiv în utilizarea unor aplicații uzuale necesare bunei funcționari a comunicării din cadrul instituției sau în relație cu alte organizații, respectiv în buna derulare a actului administrativ. Astfel de exemple uzuale în care unii funcționari au dificultăți sunt utilizarea certificatelor de semnătură electronica sau utilizarea sistemelor de video conferință.

Mai mult, un număr mic dar relevant de funcționari manifesta o lipsa de încredere în capacitatea proprie de a se adapta la sisteme informatice noi, aceasta atitudine fiind interiorizata că și principiu independent de natura efectiva a aplicației respective, ceea ce determina o reticenta directa inclusiv în procesul de pregătire a introducerii aplicațiilor și poate duce la riscuri majore de compromitere a efectului implementării noilor proiecte cu componenta digitala mai ales atunci când utilizarea acestora se impune că fiind necesara pentru întreg personalul unui compartiment.

Prin analiza și observația directa, realizata de către personalul instituției, se evidențiază că persoanele care au participat la proiectul ECDL-ANFP, chiar daca au parcurs cursurile respective cu peste 12 ani în urma și s-au bazat pe versiuni de aplicații care acum sunt învechite (pachetul Microsoft Office, etc), și-au păstrat abilitatea și avantajul competitiv prin eficienta mai buna în utilizarea aplicațiilor informatice în general fata de persoane din generații apropiate lor care nu au parcurs programul formal de educație digitala, desi atât unii cât și ceilalți au fost în mod direct expuși la utilizarea diverselor aplicații informatice.

Ca urmare a acestor analize și observații, se evidențiază necesitatea și oportunitatea abordării educației digitale generale a funcționarilor publici pe doua paliere:

- Educație digitala generala la care să participe tot personalul, pentru asigurarea și confirmarea unui nivel minim de capacitate individuala care este necesar pentru îndeplinirea eficienta a sarcinilor curente și adaptarea la introducerea de aplicații noi, inclusiv la eventuala înlocuire a celor existente
- Educație digitală continuă a personalului existent, pe baza unui plan de formare actualizat permanent, cu urmărirea efectiva a competentelor dobândite. Acest program poate fi extins pentru a include și alte componente educaționale, nu doar cele legate strict de abilitățile de utilizare a sistemelor informatice

Educatia digitala generala trebuie sa cuprinda cel putin urmatoarele componente:

- Utilizarea aplicatiilor de tip Office, in special editor de text si calcul tabelar, atat in forma de aplicatii desktop cat si in forma de aplicatii online
- Utilizarea sistemelor de video conferinta, cu exemplificarea mai multor sisteme uzuale (cel putin cele mai des utilizare cum sunt MS Teams, Zoom)
- Utilizarea certificatelor calificate de semnatura electronica, inclusiv instalarea acestora
- Utilizarea eficienta a browserelor web (folosirea taburilor multiple, curatare istoric si fisiere salvate, cautare, extensii etc)

Aceste elemente de baza trebuie suplimentate de instruirea specifica pentru fiecare dintre aplicatiile pe care respectivii functionari le utilizeaza in activitatea curenta. De asemenea trebuie avut in vedere ca pentru fiecare sistem informatic care va fi introdus in viitor in utilizare in cadrul institutiei sa fie prevazuta in mod explicit activitatea de educare formala prin sesiuni de training organizate de catre institutie impreuna cu furnizorul respectivului sistem.

Pentru a nu discrimina pe cei care au dobandit deja abilitati avansate de utilizare a sistemelor informatice, prin experienta proprie directa sau prin alte programe de formare, este oportun sa se realizeze o evaluare individuala efectiva a intregului personal, astfel incat cei care au deja capacitati avansate si sunt confortabili cu utilizarea sistemelor sa nu aiba obligatia de a parcurge acest program general.

Pe de alta parte, educația digitală continuă trebuie să includă toți funcționarii publici, fară excepție, implicând atât împrospătarea unor cunoștinte și abilitați legate de sistemele informatice uzuale mai ales că acestea evoluează și se actualizează continuu, cât și elemente avansate de educație digitala specifica activității administrative, cum ar fi de exemplu: principii de e-guvernare și optimizarea proceselor prin digitalizare, realizarea de analize statistice și prognoze pe baza datelor acumulate, managementul și urmărirea activității prin sisteme de gestiune a activităților și incidentelor, mecanisme digitale de consultare publica și colectare de feedback, și altele, cele enunțate fiind ilustrate cu caracter de exemplu.

C. Recomandări privind Oportunitatea derulării unui program special de educație tehnica avansata pentru personalul departamentului IT mai ales în contextul extinderii departamentului pentru asigurarea gestiunii centrului de date, a dispeceratului central informatic și a derulării proiectelor

În contextul creșterii continue a importantei și complexității proceselor de digitalizare din cadrul Primăriei Municipiului Bistrița și a instituțiilor subordonate, precum și pentru a putea asigura în bune condiții capacitatea tehnica și nivelul calitativ corespunzător pentru implementarea proiectelor incluse în planul de implementare prezentat în acest document, se evidențiază că fiind necesar și oportun să se dezvolte și să se implementeze un program de educație tehnica de nivel avansat pentru personalul specializat din

cadrul departamentului IT, care să cuprindă atât aspecte tehnologice cât și aspecte metodologice, care să permită în bune condiții cel puțin următoarele activități

- Identificarea, definirea, specificarea proiectelor cu componenta informatica, inclusiv dezvoltarea specificațiilor funcționale și tehnice, identificarea și definirea cerințelor de securitate, performanta, scalabilitate, accesibilitate, integrabilitate, replicabilitate, extensibilitate, definirea cerințelor de infrastructura, definirea cerințelor legate de backup și recuperare a sistemelor și a datelor, definirea necesarului de actualizare tehnologica în ciclul de viață al aplicațiilor, pentru toate sistemele informatice care vor fi implementate în cadrul instituției
- Realizarea componentelor tehnice ale documentației de atribuire pentru procedurile de achiziție publica de produse informatice sau servicii de dezvoltare, identificarea criteriilor specifici de calificare și selecție a furnizorilor, identificarea și definirea factorilor de evaluare inclusiv metodologia de evaluare și formulele de calcul, folosirea acolo unde este oportun a proceselor de interviu tehnic sau demonstrare tehnica, realizarea evaluării tehnice a ofertelor
- Coordonarea și supervizarea proceselor de implementare a noilor aplicații, asigurarea capacității de acordare sau solicitare de clarificări în relația cu furnizorii de produse sau servicii digitale, asigurarea proceselor de auditare a conformității, a calității, a scalabilitatii, a securității în vederea recepției sistemelor
- Asigurarea proceselor de transfer a cunoștințelor tehnice în relație cu orice sistem sau serviciu recepționat de la furnizori
- Dezvoltarea și gestiunea unui program de educație digitala pentru personalul instituției

În vederea dezvoltării și susținerii capacității corespunzătoare, este recomandat să fie avute în vedere atât componente de educație efectiva prin cursuri în persoana sau online cât și dobândirea de certificări recunoscute national sau international pentru anumite abilitați specifice.

Printre elementele educaționale relevante sunt

- Managementul proiectelor informatice, curs cu certificare recunoscuta international
- Managementul pregătirii și derulării proceselor de achiziție publica a aplicațiilor și serviciilor digitale, din perspectiva tehnica
- Dezvoltarea și analiza arhitecturilor informatice
- Principii de e-guvernare, analiza, optimizarea și modelarea proceselor, informatizarea proceselor de e-guvernare
- Principii de interoperabilitate semantica și tehnica, evaluarea nivelului de interoperabilitate, definirea planurilor de interoperabilizare

FISA DE PROIECT FANION

Titlu:

“Realizarea unei arhive electronice şi digitalizarea arhivei documentare actuale“

Coordonator din partea consultantului:

Paulina MITREA

Scop, context şi justificare. Obiective principale, beneficiari si rezultatele aşteptate

O mare provocare cu care sunt confruntate Primăriile la ora actuală, este aceea legată de gestionarea volumului uriaş de documente aflate în cele mai multe cazuri pe suport tradițional (hârtie), ori în paradigma digitalizării tuturor proceselor în vederea evoluției iterative în direcția dezvoltării oraşelor inteligente pe toate cele patru niveluri avute în vedere la ora actuală: Oraş Digital, Oraş „Smart”, Oraş Inteligent, Oraş Cognitiv – Brained City, este necesar, chiar crucial, ca şi sistemul de arhivare şi mamagement al documentelor administrației publice, să fie digitalizat în totalitate.

Obiectivele principale ale proiectului vizează:

- Digitizarea tuturor documentelor existente în arhiva clasică (deci pe suport hârtie)
- Definirea formatului digital pentru toate tipurile de documente ca formulare care să poată fi completate online
- Implementarea de funcționalități care să asigure managementul/circularea documentelor exclusiv în format electronic
- Accesibilizarea către toți funcționarii primăriei atât a documentelor din arhiva electronică, cât şi a celor aflate în circulație pe platforma de management documente anterior arhivării, în baza unor drepturi de acces ierarhizate conform diagramei organizaționale şi Fişei Postului

Beneficiarii sistemului vor fi în primul rând funcționarii publici ai Primăriei Bistrița, dar şi toți cetățenii urbei, prin faptul că vor putea beneficia de servicii online care vor permite interacțiunea de la distanță cu Primăria privitor la toate tipurile de acte/documente necesare în comunicarea cu orice tip de compartiment/serviciu/direcție/birou al Primăriei.

Acest principiu este de fapt cel de „paperless”, adică fără hârtii, care este menit a preveni:

- pierderea accidentală a documentelor (ceea ce se întâmplă de foarte multe ori cu cele aflate pe suporturi tradiționale)
- căutările greoaie în arhivele tradiționale (manuale) şi care consumă foarte mult mult timp
- cozile de la ghişee şi nervozitatea aferentă, manifestată de ambele părți (deci atât pe partea funcționarilor de la ghişee cât şi pe partea cetățenilor care au de interacționat cu aceştia)
- posibilitatea automatizării întregului proces de management şi arhivare a documentelor
- posibilitatea implementării de funcționalități bazate pe tehnologii ale Inteligenței Artificiale, inclusiv a asistenților virtuali (Chatbot)

Rezultatele aşteptate se regăsesc tocmai prin realizarea avantajelor mai sus enumerate, care vor fi în beneficiul major atât al funcționarilor publici ai Primăriei Municipiului Bistrița, cât şi, în mod extins, al tuturor cetățenilor urbei.

Obiective detaliate

Sistemul de arhivare electronică va permite gestionarea documentelor arhivate cu ajutorul aplicației de arhivare electronică, așa cum este cerut de Legea Arhivelor Naționale nr. 16/1996, precum și retro-digitizarea documentelor, inclusiv a documentațiilor de urbanism.

Sistemul va pune la dispoziție două variante de arhivare conform legii, care permit arhivarea electronică simplă a documentelor și respectiv arhivarea electronică însoțită de semnătură electronică și certificate digitale ale persoanelor autorizate, în baza Legii 135/2007.

Sistemul de arhivare electronică şi digitalizare a arhivei documentare actuale are următoarele obiective detaliate:

- Dezvoltarea și implementarea platformei informatice menită să digitalizeze procesele de administrare a documentelor primite sau întocmite pentru uz intern în cadrul instituției, așa cum este cerut de Legea Arhivelor Naționale nr.16 din 1996, republicată, trebuind să includă:
  - procesul de administrare arhivistică a documentelor: luare în evidență, asociere, mecanisme de acces şi de identificare
  - export securizat de date pentru utilizatorii cu drepturi
  - capacitate de integrare cu alte sisteme.

- Arhivarea datelor/documentelor în conformitatea cu prevederile legale privind arhivarea electronică.

- Retro-digitalizarea arhivei, adică crearea unei arhive de copii digitale ale documentelor tradiționale existente deja în arhiva Primăriei Bistrița, incluzând mecanismele de indexare a acestora

- Metadatele rezultate din indexare și cele referitoare la copiile digitale vor fi acesibile în contextul platformei integrate de digitalizare a tuturor proceselor administrative din Primăria Bistrița, conform unor drepturi de acces ierarhizate, bazate pe nume utilizator şi parolă, conferite conform organigramei instituționale şi conform cu Fişele de Post ale funcționarilor publici.

  Sistemul de arhivare electronică va presupune stocarea documentelor pe două zone, după cum urmează:
  - o zonă dedicată stocării documentelor electronice care nu vor fi semnate electronic
  - o zonă dedicată arhivei electronice în sensul Legii nr. 135/2007

Arhiva electronică astfel constituită va fi structurată pe următoarele categorii de documente:

- Documentații urbanistice (Plan de Amenajare a Teritoriului Județean, Planuri Urbanistice Generale, Planuri Urbanistice de Detaliu, Planuri Urbanistice de Zonă, Planuri Urbanistice de Zonă Protejată, studii diverse, etc)
- Documente existente deja în arhiva Primăriei în formă scanată
- Documente create în format electronic cu ajutorul subsistemelor platformei informatice de digitalizare integrată a proceselor din cadrul Primăriei Bistrița
- Documentații/proiecte/date vectoriale – dxf., dwg., cdr., shp, etc. - primite/preluate
- Documente semnate digital

În privința tuturor acestor categorii, se va asigura posibilitatea exportului documentelor semnate electronic în format .word sau .pdf pentru cazul în care este necesară semnarea acestora inclusiv în format fizic.

Planul de implementare

Din punct de vedere tehnologic, planul de implementare recomandă ca sistemul de arhivare electronică să fie dezvoltat în tehnologie Java Web și toate modulele în care urmează a fi structurată să fie concepute pe baza de servicii de tip REST care permit interoperabilitatea cu celelalte sisteme ale platformei integrate de digitalizare a proceselor administrative din Primăria Bistrița.

In plus, sistemul va trebui să fie interfațabil pentru utilizare externă, inclusiv pentru aplicații mobile.

Din punct de vedere structural, planul de implementare prevede următoarele componente ca module ale sistemului de arhivare electronică:

- **Modul de căutare avansată multicriterială** - care permite identificarea documentelor pe baza de metadate sau conținut al fișierelor de tip pdf, doc, text sau tabelar.

- **Modul de arhivare manuală sau automatizată** care permite utilizatorului să parcurgă întregul flux de arhivare, care constă în:
    - preluare documente scanate
    - introducere metadate
    - introducere atașamente
    - semnare electronică
    - arhivare
    - gestionare documente expirate
    - înregistrare in registrul de arhivare.

- Modul de administrare și configurare, care cuprinde:
  - gestionarea de roluri și utilizatori
  - profil de înlocuire
  - editor al tipologiilor de documente cu metadatele aferente
  - gestionare acces la documente si la zone ale aplicației
  - jurnalul privind activitățile din arhiva, nomenclatoare și parametrizarea aplicației.

- Modul de automatizare a proceselor și integrarea cu servicii externe, care permite definirea de agenți/servicii care efectuează operații automatizate de preluare documente, arhivare, notificări, aceşti agenți fiind programați să ruleze în condiții specificate.

Din punct de vedere funcțional, planul de implementare prevede următoarele funcționalități:

- Gestionarea automată a fluxurilor de documente - pe bază de fluxuri de lucru personalizate
- Colectare/introducere documente în sistem – conținând totalitatea operațiunilor de scanare/recunoaștere/indexare/arhivare
- Implementarea fluxurilor de integrare cu componente informatice ale platformei de digitalizare a proceselor administrative ale Primăriei Bistrița.
- Implementarea unui planificator de fluxuri de lucru
- Implementarea unei funcționalități de definire de fluxuri de lucru noi
- Asigurarea securității accesului utilizatorilor în lucrul cu fluxurile informatice precum administrare acces utilizatori și administrare profil/identitate utilizator
- Asigurarea tuturor funcționalităților caracteristice unui sistem relațional de baze de date pentru stocarea metadatelor și a altor informații/date necesare
- Stocarea de fișiere imagine rezultate în urma digitizării documentelor fizice

Capabilitatea de gestiune a proceselor bazate pe documente va trebui să permită circulaţia documentelor pe trasee ierarhice sau alte trasee definite de autorul documentului, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea şi circulaţia informaţiilor şi a documentelor interne în cadrul structurii, precum şi a celor generate în relația cu autorităţile externe.

Astfel, se vor implementa componente dedicate pentru:

- modelarea şi implementarea proceselor într-un mod colaborativ,

- documentare, analiză, optimizări

- automatizarea şi monitorizarea proceselor de lucru şi a fluxurilor de documente.

La nivel macro, sistemul va trebui să cuprindă:

- Fluxuri de integrare
- Optimizarea încărcării şi Gestionarea Modificărilor
- Orchestrarea serviciilor şi activităţilor
- Gestionarea Evenimentelor
- Monitorizarea Evenimentelor
- Raportarea Evenimentelor.

Una dintre funcționalitățile cele mai importante trebuie să fie **administrarea utilizatorilor și controlul accesului**, care se detaliază după cum urmează:

- Administrarea utilizatorilor inclusiv în sensul de corelare cu celelalte componente ale platformei integrate de digitalizare a proceselor Primăriei Bistrița, astfel fiind necesară o singură logare
- Administrarea conturilor de utilizator
- Crearea de reguli bazate pe rol
- Delegarea administrării
- Administrarea parolelor
- Interfaţa cu utilizatorul
- Arhitectură de conectare cu caracteristici riguroase de securitate cibernetică.

Specificaţii funcţionale

• Abstractizarea/Translatarea Adresei de Reţea - Toate adresele interne trebuie să fie abstractizate, translatate sau ascunse utilizatorilor finali care accesează aplicaţii interne.

• Abstractizarea/Translatarea Namespace/URL - Serverul Reverse Proxy trebuie să abstractizeze, translateze și să ascundă numele de sistem şi URL-urile interne.

• Suport pentru autentificare globală (SSO) - Mecanismul Reverse Proxy trebuie să ofere mecanisme pentru autentificare globală, cu posibilitatea de efectuare a mai multor operaţii de autorizare pentru resurse sau aplicaţii diferite fără să fie necesară reautentificarea utilizatorului dacă noua resursă sau aplicaţie necesită un nivel mai ridicat de autentificare.

• Accelerarea Criptării/Decriptării SSL - Mecanismul Reverse Proxy trebuie să suporte mecanisme de criptare/decriptare hardware pentru a îmbunătăţi performanţa SSL

• Suport pentru Split SSL Certificate - Mecanismul Reverse Proxy trebuie să ofere serverului suport pentru certificate SSL pentru sisteme client externe

• Asigurare suport pentru următoarele mecanisme de criptare, fără a se limita la: 128-bit RC2, 128-bit RC4, 256-bit AES, 56-bit DES, 168-bit triple DES Scalabilitate

- Din punct de vedere al scalabilităţii, Mecanismul Reverse Proxy trebuie să fie scalabil pentru a suporta minim 10 mii de sesiuni simultane
- Integrare cu mecanismele de balansare a sarcinii - Serverul Reverse Proxy trebuie să coexiste şi să opereze în spatele oricărei soluţii de balansare a încărcării pentru a echilibra traficul şi a oferi disponibilitate ridicată a sistemului.
- Suport pentru centre de date multiple - Serverul Reverse Proxy trebuie să suporte capabilitatea de a migra suportul pentru aplicaţie către alte servere proxy dintr-un centru de date alternativ sau dintr-un alt punct de conectivitate în eventualitatea unei probleme majore sau al unui eveniment de întreţinere.

Caracteristici pentru Monitorizare/Raportare

- **Evenimente/Alarme** - sistemul de arhivare trebuie să fie prevăzut cu funcționalități de monitorizare şi corelare de evenimente pentru a afişa evenimente şi alerte personalului administrativ.
- **Auditare şi Raportare** - sistemul de arhivare trebuie să includă mecanisme de auditare pentru toate evenimentele de autentificare, autorizare şi administrare, precum şi avertizări legate de componentele soluţiei, incluzând cel puţin: logări reuşite, logări nereuşite, conturile blocate, mesaje de acces neautorizat, toate încercările de acces, erorile de autorizare, utilizatorii anonimi, identificarea creării, modificării sau ștergerii, evenimente suspicioase, urmărirea utilizatorilor anonimi
- **Istoricul schimbării/reconfigurării** - sistemul de arhivare trebuie să păstreze istoricul modificărilor configurației pentru administrarea configurării şi pentru scopuri de investigare a eventualelor de securitate.
- **Administrarea logurilor** - sistemul de arhivare trebuie să suporte arhivarea log-urilor de evenimente/alerte precum şi funcţionalităţi de export a acestora; aceste log-uri trebuie reţinute pe termen lung şi informaţia din log-uri trebuie să fie exportabilă în formate pentru postprocesare şi analiză.

Alte funcționalități suplimentare

- Integrarea cu editor de fluxuri, care permite definirea oricăror tipuri de fluxuri în cadrul cărora documentele rezultate si metadatele vor fi arhivate
- Acces securizat la documente pentru utilizatori externi ai arhivei prin link sau e-mail
- Nomenclatoare dinamice care permit definirea de tipologii și categorii de date ce pot fi preluate in mod automat după ce sistemul este populat cu date concrete, precum: denumiri instituții, tip avize, localități, străzi, categorii, etc.

- Integrarea cu roboți de tip RPA pentru automatizarea proceselor repetitive.

- Structurare dinamică, arborescentă a arhivei electronice, bazată pe: **Mod Arhivare** (care poate fi „simpla” sau „semnat electronic”), **Foldere** (department, an, luna, etc.), **Dosare** și **Tipologii de documente**, care permite mutarea datelor între locații.

Sustenabilitate şi impact

Sustenabilitatea sistemului se bazează pe caracteristicile smart ale acestuia, acestea fiind următoarele:

- **Extensibilitate** asigurată prin definirea în mod dinamic a oricăror tipologii de documente și metadate aferente, prin definirea structurii virtuale a arhivei electronice pe spații de arhivare, foldere și subfoldere, acces la documente pe baza de roluri și zone de acces delimitate.

- **Eficiență** dată de reducerea timpilor de căutare a documentelor, diminuarea perioadelor de emitere a autorizațiilor, controlul riguros și organizat asupra documentelor.

- **Uşurarea semnificativă a activității umane** prin activități de arhivare automatizată a tuturor tipurilor de documente

- **Scalabilitate** asigurată prin faptul că se recomandă ca arhivarea datelor să se realizeze la nivelul bazei de date relaționale integrate cu CMS Repository, care permit scalarea în funcție de volumul de date

- **Interconectivitate** asigurată prin însăşi structura arhitecturii sistemului, care poate fi interconectata la orice sursa interna sau externa de informații

Impactul este dat de către caracteristica de utilizabilitate, care va fi asigurată prin Interfața Grafică Utilizator care trebuie să fie ***responsive*** - în sensul că poate fi redată bine pe o varietate de dispozitive și dimensiuni de ecran, de la dimensiunea minimă posibilă la cea maximă a afișajului - și trebuie să aibă un UX (user experience) care să faciliteze o utilizare ușoară și o adopție rapidă atât de către cetățean cât și de către funcționarii publici ai Primăriei Municipiului Bistrița.

FISA DE PROIECT FANION

Titlu:

“Sistem de monitorizare a calității aerului din sălile de clasă din gradinițe, şcoli şi licee”

Coordonator din partea consultantului:

Paulina MITREA

I. Scop, context şi justificare. Obiective principale, beneficiari si rezultate generice asteptate

In baza principiului conform căruia cheia dezvoltării oricărei comunități urbane constă în creşterea continuă a nivelului educațional al membrilor comunității, gradul de confort şi igienă al locațiilor în care se desfăşoară procesul educațional este la fel de important ca şi procesul principal de transmitere şi evaluare a cunoştințelor.

Proiectul se înscrie în gama proiectelor de digitalizare situate pe nivelul cel mai înalt al Casei IT reprezentată în Fisa Proiectului Fanion de Management al Digitalizării/Transformii digitale a Municipiului Bistrița, anume pe cel de Organizare şi Cultură pentru digitalizare/Arhitectură IT, Infrastructură şi portofoliu de aplicații.

In contextul ecosistemului urban al Oraşului Inteligent Bistrița, proiectul adresează atât pilonul educațional, cât şi pilonul de mediu – care devine din ce în ce mai important, fiind considerat vital pentru toate celelalte sectoare/piloni care stau la baza arhitecturii conceptuale şi efective a oricărui Oraş Inteligent.

Pornindu-se de la aspectul extrem de important al faptului că, pentru a funcționa în mod performant, creierul uman are nevoie de oxigenare optimă – ceea ce este crucial pentru procesul educațional, trebuie luate în considerare pe acelaşi palier al importanței toate celelalte condiții care sunt „sine qua non" pentru sănătatea generală a copiilor/elevilor ca subiecți principali ai procesului educațional, rolul calității aerului din sălile de clasă - privit sub toate aspectele componenței şi proprietăților acestuia - fiind de fapt de importanță primordială.

Argumentele în această privință sunt şi mai serioase decât cele referitoare la nevoile adulților, deoarece este în general bine ştiut faptul că riscurile asociate poluării aerului de interior sunt cel puțin duble pentru copii, din următoarele motive:

- În primul rând, plămânii copiilor sunt expuși la mai mult aer într-o anumită perioadă de timp, deoarece respiră mai rapid decât adulții
- În al doilea rând, plămânii copiilor sunt mai mici și mai puțin dezvoltați decât în cazul adulților, astfel încât sunt mai predispuși să întâmpine complicații din cauza expunerii la poluanții aerului interior.

Practic, calitatea precară a aerului din interiorul sălilor de clasă poate afecta sănătatea şi gradul de concentrare al copiilor/elevilor, putându-se declanşa în unele cazuri afecțiuni precum astmul sau alte boli ca urmare a iritației sistemului respirator.

Studiile de specialitate arată cu multă claritate faptul că, pe **termen scurt** aerul poluat din interiorul sălilor de clasă poate cauza iritații la nivelul ochilor, nasului sau căilor respiratorii, chiar

şi oboseală sau dureri de cap în cazul persoanelor sensibile, mergându-se deci până la posibila instalare a astmului – care este o maladie extrem de gravă.

Pe **termen lung** s-a descoperit că expunerea periodică la anumite substanțe poate să se constituie în cauze majore pentru boli şi mai serioase, precum: cancer, boli ale ficatului , rinichi, astm în forme agravate, sau chiar inflamații ale sistemului nervos.

In ceea ce priveşte astmul, mulți factori declanșatori ai astmului includ poluanții din aer, la care copiii sunt expuși în fiecare zi în școală, cum ar fi mucegaiul, praful și alți contaminanți ai aerului din interior.

Tot în conformitate cu studiile de specialitate, principalele pericole asociate cu poluarea aerului in interiorul sălilor de clasă sunt reprezentate de următorii poluanți/noxe:

- **Mucegaiul si Umiditatea:** sporii de mucegai se găsesc aproape peste tot în mediul nostru și, în prezența umezelii, au nevoie doar de una sau două zile pentru a se extinde, ca atare rezultă faptul că cheia pentru evitarea creșterii mucegaiului în școli este prevenirea umezelii în primul rând; efectele asupra sănătății și simptomele asociate creșterii mucegaiului în școli includ reacții alergice, astm, iritații respiratorii, oboseală, diaree și greață; în astfel de condiții, copiii/elevii cu alergii preexistente și astm sunt adesea primii care sunt afectați.

  Pentru a se putea preveni problemele generate de nivelul inadecvat de umiditate din componența aerului interior, este nevoie în primul rând de ***monitorizarea calității acestuia inclusiv sub aspectul gradului de umiditate***, pentru ca în cazul semnalării depăşirii nivelului maxim admis conform standardului, să se poată interveni asupra potențialelor surse de disconfort, precum: drenajul slab, aspersoare direcționate greșit, inundare din acoperișuri, țevi, ferestre, fundații și alte deschideri structurale; probleme legate de umiditate pot apărea, de asemenea, din cauza unei ventilații slabe în timpul întreținerii regulate, sau când aerul condiționat și încălzirea sunt reduse în timpul pauzelor școlare. De aici decurge inclusiv importanța monitorizării aerului sub aspectul temperaturii acestuia.

- **Radonul –** acesta este un gaz radioactiv natural, fiind în prezent a doua cauză principală de cancer pulmonar (după fumat); este emanat în timpul descompunerii uraniului din sol și pătrunde în clădiri prin fisuri și găuri în pereții subsolului, podelele și fundațiile clădirilor. Potrivit Agenției pentru Protecția Mediului (EPA), peste 70.000 de școli la nivel național au niveluri ridicate de radon cel puțin o parte din timp; deoarece este incolor și inodor, gazul radon este nedetectabil dacă nu se efectuează un test de radon, de aceea toate școlile sunt încurajate să testeze radonul, deoarece acesta se numără printre cele mai grave pericole pentru mediu identificate în școli.

- **Compușii organici volatili (COV) –** aceştia provin dintr-o multitudine de produse utilizate în școli, care conțin vapori organici nocivi sau compuși organici volatili, precum: vopsele și decapanți de vopsea, conservanți pentru lemn, produse de curățat, spray-uri cu aerosoli,

odorizante de aer etc; nivelul de risc al COV variază de la produs la produs, dar, în general, expunerea la COV este asociată cu iritarea ochilor, nasului și gâtului, iar efectele mai grave pe termen lung asupra sănătății asociate cu COV includ cancerul și afectarea ficatului, a rinichilor și a sistemului nervos central; unitățile şcolare pot reduce prezența COV în campusurile lor utilizând produse ecologice și alternative cu niveluri mai scăzute de COV, iar atunci când sunt nevoite să utilizeze produse care conțin COV, este important ca acestea să depoziteze și să elimine în siguranță produsele și să ventileze zonele de lucru atunci când este cazul.

- **PM2.5/PM10** – această categorie se referă la particulele în suspensie mai mici de 10 micrometri, care trec prin nas și gât şi pătrund în alveolele pulmonare provocând inflamații și intoxicări; sunt afectate în special persoanele cu boli cardiovasculare și respiratorii, dar in special copiii, vârstnicii şi astmaticii; poluarea cu pulberi înrăutăţeşte simptomele astmului, respectiv tuse, dureri în piept și dificultăți respiratorii; expunerea pe termen lung chiar şi la o concentrație scăzută de pulberi poate cauza cancer și moartea prematură, principala sursă dintr-o unitate educațională putând fi chiar aerul provenit de la cea mai apropiată stradă circulată; prevenția în raport cu această problemă necesită în primul rând monitorizarea nivelului de poluare a aerului cu PM2.5/PM10, cât şi prezența filtrelor pentru astfel de particule.

- **CO2 (bioxidul de carbon) –** acesta trebuie să fie ținta unei preocupări de importanță majoră, deoarece fiecare copil produce o cantitate mica de CO2 prin respiratie, astfel încât într-o sală de clasă supra-populată, cu multe ore de curs fără pauză, sau fără ventilație, se poate ajunge la o creştere a CO2 care poate avea ca efecte durerile de cap sau pierderea concentrării; prevenția în raport cu această problemă necesită în primul rând monitorizarea nivelului de poluare a aerului cu CO2, pentru ca în cazul semnalării depăşirii nivelului maxim admis conform standardului, să se poată lua măsurile imediate cele mai adecvate, precum intensificarea aerisirii pe cale naturală sau prin sistemul de ventilație/aer condiționat.

De altfel, sistemele de încălzire, ventilație și aer condiționat - denumite ***HVAC*** în literatura de specialitate, pot ajuta sau pot afecta foarte mult situația calității aerului unei școli. Sistemele ***HVAC*** (**H**eating, **V**entilation, **A**ir **C**onditioning) eficiente, sunt proiectate pentru a menține temperatura, umiditatea și poluanții atmosferici dintr-un spațiu la niveluri sigure și confortabile.

Dacă sistemul ***HVA***C este depășit sau nu funcționează corect, calitatea aerului din interior se poate deteriora rapid. Temperaturile incomode din clasă pot face dificilă concentrarea și performanța elevilor. În plus, acumularea de iritanți și poluanți în aer poate declanșa alergiile și astmul copiilor/elevilor sau poate provoca alte simptome respiratorii.

Se identifică deci, ca obiective principale ale proiectului, următoarele:

- Nevoia instalării de sisteme de monitorizare a calității aerului din toate unitățile de învățământ ale Mun. Bistrița

- Nevoia instalării şi întreținerii adecvate a sistemelor HVAC menite a genera şi a menține condițiile atmosferice optime în interiorul sălilor de clasă ale tuturor unităților de învățământ

II. Obiective si rezultate detaliate

Realizarea obiectivelor principale menționate în cadrul secțiunii **I**, presupune focalizarea următoarelor obiective de detaliu de primă importanță :

1. Instalarea în fiecare sală de clasă a dispozitivelor ce monitorizează parametrii prezentați în secțiunea I în fiecare sală de clasă.
2. Implementarea unui sistem de avertizare sau informare a directorilor de școală şi legarea tuturor dispozitivelor de monitorizare la acest sistem.
3. Legarea întregului sistem pus la punct în acest mod, la cloud-ul urban, atât la Centrele de Date şi de Procesare aferente pilonului educațional, cât şi la cele aferente pilonului de mediu.

Ca măsuri suplimentare menite a preveni/minimiza încărcarea cu noxe a aerului din sălile de clasă, constituite în tot atâtea obiective de detaliu, este necesar să se acorde importanța cuvenită inclusiv pentru următoarele:

4. Izolarea mediilor cu potențial umed, ce pot provoca mucegai.
5. Izolarea locațiilor aflate la demisol sau parter ce reprezintă o expunere mai mare la Radon3.
6. Utilizarea unor dispozitive adecvate de tip ventilare/curățare/purificare aer pe timpul pauzelor școlare.

In cele ce urmează, vom focaliza în mod deosebit **detaliile sistemului de monitorizare a calității aerului din sălile de clasă din gradinițe, şcoli şi licee**, conceput ca o soluție bazată pe tehnologii avansate ale domeniului senzoristicii şi digitalizării proceselor prin sisteme IT avansate, integrate în cloud-ul urban în vederea asigurării interoperabilității tuturor componentelor arhitecturii IT integrate la nivelul tuturor pilonilor Oraşului Inteligent Bistrița.

Din punct de vedere structural, un asemenea sistem este format din următoarele componente:

- Sisteme de senzori inteligenți instalate în fiecare sală de clasa având în componența lor următoarele tipuri de senzori:
    - senzor pentru temperatură
    - senzor pentru umiditate

- senzori pentru calitatea aerului
- senzor pentru miros.

- Platformă middleware care interfațează transmiterea datelor colectate de la senzori, direct în cloud-ul urban, unde pot fi accesate/vizualizate/procesate conform necesităților de informare şi drepturilor de acces ierarhizate ale tuturor actorilor (utilizatorilor) care au responsabilitati privitor la asigurarea condițiilor din sălile de clasă ale şcolilor din Municipiului Bistrița, cât şi ale tuturor celor interesați de condițiile asigurate copiilor de vârstă preşcolară şi şcolară în egală măsură, anume:

    - Top managementul şi managementul administrativ al unităților educaționale
    - Responsabilii din Primărie asignați pe domeniul educațional
    - Responsabilii din cadrul Inspectoratului Scolar
    - Parinții şi elevii
    - Cadrele didactice
    - Responsabilii din Agenția de Mediu Bistrița
    - Cetățenii urbei interesați de aspectul condițiilor optime de care trebuie să se bucure copiii/elevii din Municipiul Bistrița.

- In paralel cu transmiterea datelor direct în Centrele de Date şi de Procesare ale cloud-ului urban, în mod opțional acestea se pot colecta în paralel şi pe un server local, dacă managementul şcolii este interesat să aibă şi o interfață de acces la datele culese din sălile de clasă într-o manieră personalizată conform unor opțiuni locale.

In acest sens, următorul tabel conține un set de specificații tehnice orientative, care urmează a fi adaptate la condițiile din teren si la modalitatea de implementare.

Hardware	**Caracteristici**
Stație de sortare	
Unitate de control principala	Alimentare: 20.4 – 28.8 VDC Memorie program >= 100 kB Card memorie >= 128 MB Intrări Digitale 24 VDC >= 10 Ieşiri Digitale Releu >= 10 Intrări Analogice >= 8 Interfața de comunicație: Profinet, Modbus TCP. Temperatura de operare: -20 – 60 °C Limbaje de programare: Ladder, Functional Block Diagram
Extensii unitate de control	Alimentare: 20.4 – 28.8 VDC Memorie program >= 100 kB Card memorie >= 128 MB Intrări Digitale 24 VDC >= 10

	Ieșiri Digitale Releu >= 10 Intrări Analogice >= 8 Interfața de comunicație: Profinet, Modbus TCP. Temperatura de operare: -20 – 60 °C Limbaje de programare: Ladder, Functional Block Diagram
Senzor Temperatură	Domeniu de măsura recalibrabil: da Alimentare: 20 – 30 VDC Semnal de ieșire: 4 – 20 mA Condiții de operare: -25 – 55 °C Rezistent la medii corozive Protocoale de comunicație: Profinet, Profibus/Modbus TCP
Senzor Umiditate	Domeniu de măsura recalibrabil: da Alimentare: 20 – 30 VDC Semnal de ieșire: 4 – 20 mA Condiții de operare: -25 – 55 °C Rezistent la medii corozive Protocoale de comunicație: Profinet, Profibus/Modbus TCP
Senzor Calitate Aer	Domeniu de măsura recalibrabil: da Alimentare: 20 – 30 VDC Semnal de ieșire: 4 – 20 mA Condiții de operare: -25 – 55 °C Rezistent la medii corozive Protocoale de comunicație: Profinet, Profibus/Modbus TCP
Senzor Miros	Domeniu de măsura recalibrabil: da Alimentare: 20 – 30 VDC Semnal de ieșire: 4 – 20 mA Condiții de operare: -25 – 55 °C Rezistent la medii corozive Protocoale de comunicație: Profinet, Profibus/Modbus TCP

Analiza riscului și acțiuni de natură preventivă pentru creșterea robusteții sistemului la acțiuni intenționate sau neintenționate de vulnerabilizare a monitorizării

Aceste tipuri de riscuri sunt analizate în contextul tabelului următor:

Risc potențial	**Severitatea în caz de producere**	**Probabilitatea de apariție în teren**	**Nivelul costurilor de remediere (Euro)**	**Propuneri de prevenire**
Lipsă comunicație Intranet	Scăzută	Ridicată	50	Topologie inel rețea Intranet
Lipsă semnal Internet	Scăzută	Ridicată	30	Linie dublă acces Internet
Lipsă comunicație senzori	Scăzută	Ridicată	30	Topologie inel rețea Intranet

Lipsă comunicație unitate de control	Ridicată	Scăzută	30	Topologie inel rețea Intranet
Blocare unitate de control	Ridicată	Scăzută	30	Instalare releu reset de la distanță

In ceea ce privește tipurile de senzori care sunt cele mai adecvate, următorul tabel conține propuneri de soluții și echipamente orientative, acestea urmând a fi adaptate la condițiile din teren si la modalitatea de implementare.

Senzor Temperatura	https://www.process-heating.com/articles/90148-temperature-measurement-system-with-profinet-interface
Senzor Umiditate	https://www.testo.com/en-ID/testo-6681/p/0555-6681
Senzor Calitate aer	https://www.led-grower.eu/ram-co2-monitor-and-controller/?gclid=Cj0KCQjwpdqDBhCSARIsAEUJ0hPc7hp6-rcPkpW-HgcwMWNUAYKGFgd7TcKy04XJo7bxif4Pz1Ug1kcaAtZrEALw_wcB
Senzor Miros	https://www.newcosmos-global.com/product/2365/

Estimarea bugetului

Următorul tabel conține preturi estimative pentru echipamentelor propuse, care se vor adapta desigur la condițiile din teren si la modalitatea de implementare. Costurile nu includ manopera de montare, execuție, etc.

Echipamente Hardware	**Buc**	**Cost estimativ[Euro] / bucată**
Tablou electric principal	1	5000
Tablouri electrice secundare	1	1500
Unitate de control principala	1	4500
Extensii unitate de control	1	2000
Senzor Temperatura	1	1500
Senzor Umiditate	1	1500
Senzor Calitate aer	1	2500
Senzor Miros	1	2500
Total estimativ		**21000 Euro**

Estimarea bugetului pe sistemele software:

Costurile dezvoltării sistemelor software au fost evaluate ca fiind un procent de 30% din totalul estimativ: **6300 Euro**

Estimarea costurilor operaționale anuale și pe 10 ani:

Costurile operaționale au fost evaluate ca fiind un procent de 15% din totalul estimativ: **4095 Euro**

Estimarea bugetară pe serviciile necesare întreținerii, actualizării, intervențiilor în caz de urgență, retragerii din utilizare:

Serviciile necesare întreținerii, actualizării, intervențiilor în caz de urgență au fost evaluate ca fiind un procent de 5% din totalul estimativ per an: **1365 Euro**

Bugetul cumulat pe obiectiv de investiție:

Bugetul cumulat pe obiectiv de investiție este de **26460 Euro**

Preturile sunt exprimate în Euro fără TVA.

Sistemul propus este descentralizat, reconfigurabil, reprogramabil, neredundant şi foarte fiabli.

Tot sistemul necesită alimentarea din sursă neintreruptibilă şi cu protecție (UPS online).

De asemenea, unul dintre senzorii propuşi include măsurarea temperaturii si umidității din încapere, cât şi alte valori importante precum concentrația de CO2.

Pe viitor, senzorul de temperatură poate fi utilizat şi pentru implementarea controlului termic din încăpere.

Pentru automatizare trebuie sa fie montate următoarele doze şi trebuie tras din tablou câte un cablu KNX sau JYSTY 2x2x0.8, sau înseriate dozele cu acelaşi tip de cablu, cu o pornire de la tablou la prima doză şi întoarcere la tablou de la ultima.

Doze OBO recomandate sunt UG 60 VD, care sunt mult mai adânci şi au loc suficient pentru legături. In catalog este si echivalent rigips.

Pentru BUS se recomandă cablu KNX sau JYSTY 2x2x0.8.

Pentru montat aparatajele şi prizele în doze, este nevoie de şuruburi de prindere U 15 GS de la OBO BETTERMANN sau echivalent de la altă firmă.

Ideal este ca sistemul de monitorizare a calității aerului să fie integrat în sistemul BMS (Building Management System) al clădirii/campusului şcolii, topologia de BUS a acestuiatrebuind să fie următoarea:

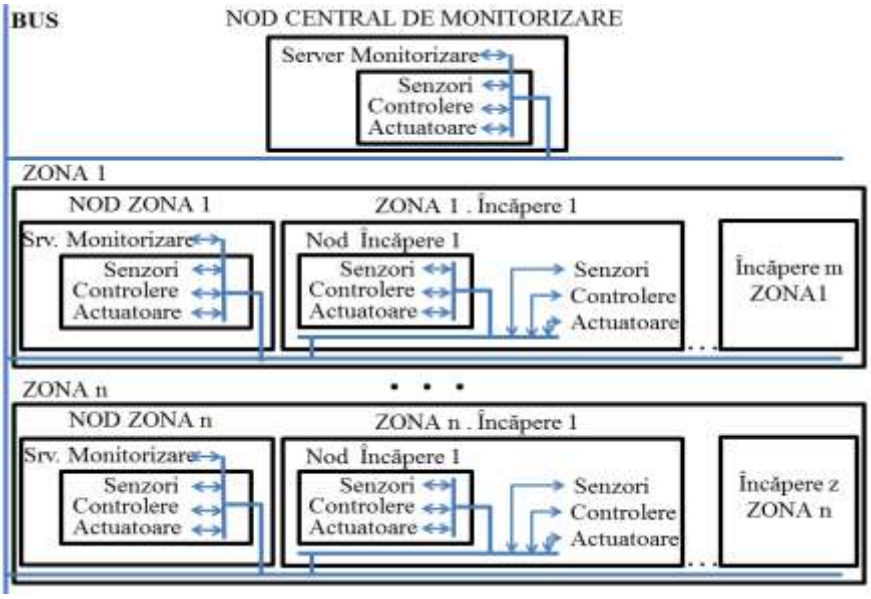


Fig.1 Topologia de BUS a sistemului BMS

Poziționarea Sistemul de Monitorizare a Calității Aerului în cadrul sistemul BMS (Building Management System) al clădirii/campusului şcolii este ilustrată în figura următoare:

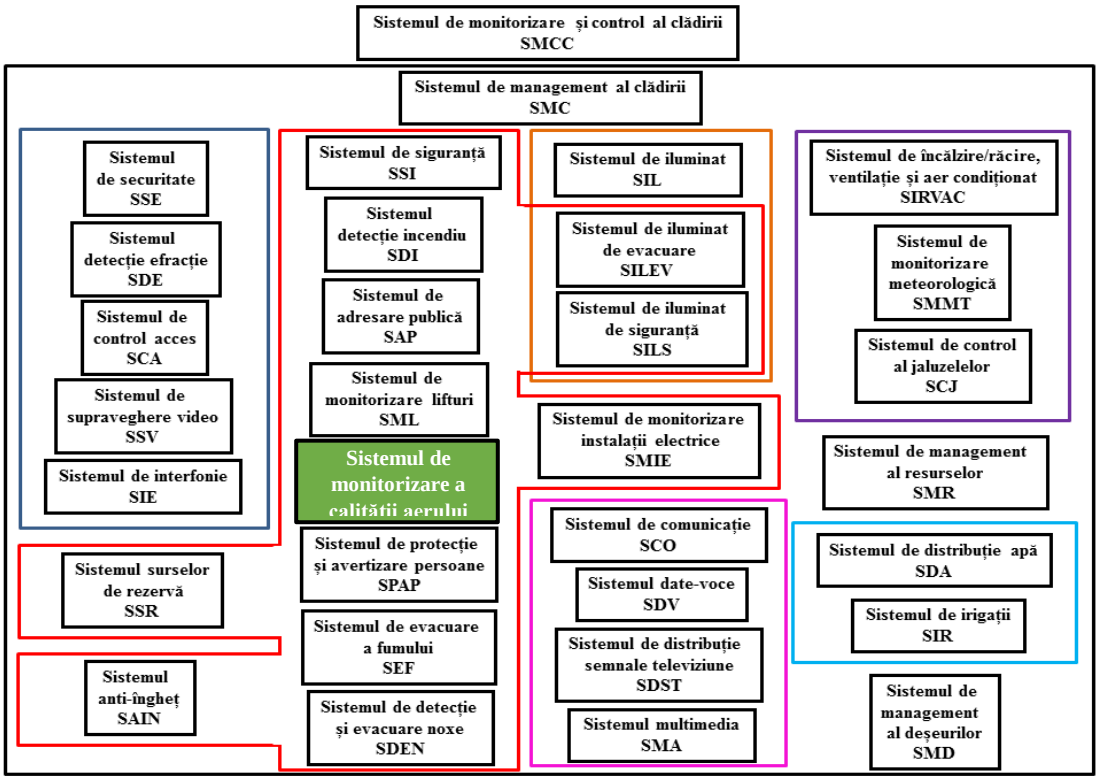


Fig.2 Poziționarea Sistemului de Monitorizare a Calității Aerului în context BMS

III. Sustenabilitate şi impact

Elementele pe care se bazează sustenabilitatea sistemului de monitorizare a calității aerului, sunt următoarele:

- Gradul în care sistemul este capabil a furniza cunoştințe/cunoaştere în domeniul calității aerului
- Gradul în care acest sistem este adaptabil
- Gradul de „offloading", adică capabilitatea sistemului de monitorizare a calității aerului, fie de a-şi autoregla erorile sau neconcordanțele care pot să apară pe parcursul versionărilor succesiv evolutive, fie capabilitatea de a permite efectuarea acestor corecții din mers, prin intervenția directă a specialiştilor IT&C/ automatişti/ electronişti, fără a fi nevoie de reimplementarea totală a sistemului.

In toate aceste trei sensuri, sustenabilitatea sistemului digitalizat de monitorizare a calității aerului din sălile de clasă ale grădinițelor şi şcolilor din oraşul Bistrița, este conferită atât prin arhitectura software a acestuia, cât şi prin natura arhitecturii cloud a infrastructurii hardware pe care urmează a fi găzduit, dar şi prin intermediul componentelor structurale ale sistemului.

In mod mai concret, migrarea datelor de mediu interior eventual existente şi la ora actuală din situații deja existente în contextul IT actual al şcolilor din Municipiul Bistrița, poate asigura, într-o primă etapă, o populare rapidă cu datele actuale a Centrului de Date al Cloud-ului Urban. In urma finalizării operațiunilor de migrare a datelor deja existente, devine obligatorie renunțarea la bazele/sursele de date vechi, în vederea evitării paralelismelor şi redundanțelor.

In urma acestei prime etape de populare a Bazelor de Date din Centrul de Date al Cloud-ului Urban, alimentarea cu date se continuă dinamic, atât în mod direct prin migrarea datelor furnizate de sistemele de monitorizare din fiecare unitate de învățământ - bazat pe mecanismele de interoperabilitate ale arhitecturii de integrare pe cloud-ul urban, cât şi prin activitățile de interacțiune cu sistemul ale tuturor tipurilor de utilizatori (actori) cărora le este destinat.

Tot acest mecanism asigură o sustenabilitate a la long a alimentării cu date a resurselor de date privitoare la calitatea aerului din sălile declasă ale grădinițelor şi şcolilor, găzduite în cloud.

In ceea ce priveşte sustenabilitatea componentelor de procesare, actualizarea acestora se realizează de asemenea în mod direct şi cu eficiență maximă în cadrul contextului integrat, acesta permițând cuplarea şi decuplarea fluxurilor de procesare în mod dinamic.

Impactul asupra dezvoltării comunității urbane Bistrița al sistemului digitalizat de monitorizare a aerului din sălile de clasă ale grădinițelor şi şcolilor, este acela de a se putea monitoriza în permanență, în mod continuu, calitatea aerului, astfel încât să se poată interveni operativ cu acțiuni menite a regla şi chiar optimiza calitatea acestuia, în primul rând în folosul menținerii stării de sănătate a copiilor/elevilor ca premiză esențială a stării de sănătate a viitorilor adulți, iar în al

doilea rând în folosul asigurării unui context ambiental optim pentru desfăşurarea procesului educațional, în toate unitățile de învățământ ale Municipiului Bistrița.

ANEXE

Mostre senzori de monitorizare a calității aerului:

1. **Senzori de temperatură:**

Senzor temperatură; Pt100; cl.A; Term: 3 cabluri,bandă cu cleme
Denumire producător:**64-23301001-0050.TM**
Simbol TME:**64-23301001-0050**

Termometru de panou -50°C ~ +110°C
Referinta **XSXDRO**

2. **Senzori umiditate**:

Senzor umiditate 40-90% Stego

Modul Controller de Umiditate W3005

3. Senzori 2 in 1 - temperatură & umiditate:

Senzor temperatura si umiditate smart Zigbee Tosyco compatibil cu Tuya, Google Home, Amazon Alexa, IFTTT

FISA DE PROIECT FANION

Titlu:

“ Sistem de evidență a copiilor şcolarizați în oraşul Bistrița şi distribuția acestora pe unități de învățământ”

Coordonator din partea consultantului:

Paulina MITREA

I. Scop, obiective principale, beneficiari si rezultate generice asteptate

Cheia dezvoltării oricărei comunități urbane constă în creşterea continuă a nivelului educațional al membrilor comunității. Din acest motiv, focalizarea situației şcolarizării copiilor şi tinerilor Municipiului Bistrița este crucială atât sub aspectul tuturor componentelor procesului de şcolarizare, cât şi privitor la toate nivelurile procesului educațional.

Astfel, un sistem digitalizat de evidență a copiilor şcolarizați în oraşul Bistrița, cât şi a distribuției acestora pe unități de învățământ, constituie punctul de pornire al demersului de supervizare a întregului proces educațional, cu scopul final de a se putea realiza evoluția incrementală a acestuia, în sensul creşterii ponderii şcolarizării copiilor/tinerilor urbei pe nivelurile educaționale superioare, această creştere fiind desigur calibrată/echilibrată pe baza atât a capabilităților cât şi a aspirațiilor individuale ale acestora.

Proiectul se înscrie în gama proiectelor de digitalizare situate pe nivelul cel mai important al CaseiIT reprezentată în Fisa Proiectului Fanion de Management al Digitalizării/Transformii digitale a Municipiului Bistrița, anume pe cel de Organizare şi Cultură pentru digitalizare/Arhitectură IT, Infrastructură şi portofoliu de aplicații.

Obiectivele principale ale proiectului vizează:

- **OP1:** Realizarea evidenței în timp real a situațiilor privind copiii şcolarizați din oraşul Bistrița, atât sub aspect numeric - cu defalcarea acestora pe categorii de vârstă, cât şi sub aspectul performanței şcolare prin defalcare pe şase categorii de performanță: foarte slabă, slabă, satisfăcătoare, bună, foarte bună şi de excelență.
- **OP2:** Urmărirea în timp real a dinamicii categoriilor mai sus menționate – inclusiv ca o ilustrare a calității procesului de învățământ derulat în contextul Mun. Bistrița, cu defalcarea acestei dinamici la nivelul fiecărei instituții de învățământ în parte.
- **OP3:** Evidența în timp real a situațiilor privind copiii neşcolarizați din oraşul Bistrița, atât sub aspect numeric - cu defalcarea acestora pe categorii de vârstă, cât şi sub aspectul categoriilor sociale de proveniență, după cum urmează: (1) categorii sociale defavorizate; (2) categorii sociale aparținând clasei de mijloc; (3) categorii sociale cu disponibilitate financiară/materială superioară. In toate aceste situații, se consemnează cauza posibilă (presupusă sau declarată) a nefrecventării contextului educațional organizat.

  Toate aceste evidențe sunt în mod obligatoriu supuse reglementărilor GDPR, prin anonimizarea obligatorie a subiecților acestor evidențe.

  Beneficiarii proiectului sunt, în primul rând, factorii de decizie din domeniul educațional (ex. Inspectoratul Scolar Județean), cât şi factorii de decizie de la nivelul Mun. Bistrița care au responsabilități la nivelul dezvoltării evolutive/incrementale a resursei umane a municipiului, sub aspectul calității pregătirii profesionale/intelectuale a acesteia.

Rezultatele aşteptate în urma implementării proiectului, constau în **furnizarea unui instrument digitalizat complex, constând într-o platformă – suport pentru decizii bazate pe urmărirea, analiza şi verificarea în timp a eficienței măsurilor aplicate de către factorii de decizie şi execuție din domeniul educațional al Mun. Bistrița.** De aici decurg încă două obiective principale, anume:

- **OP4**: Acumularea de **date masive**, în mod continuu în timp, privitoare la situația şcolarizării copiilor din Mun. Bistrița şi a performanței şcolare defalcată pe unități de învățământ;
- **OP5:** Realizarea unei **platforme suport pentru decizii** – ca o componentă importantă a sistemului digitalizat de evidență a copiilor şcolarizați în oraşul Bistrița, cât şi a distribuției acestora pe unități de învățământ.

II. Context si justificare

Din datele culese si analizate aferent stadiului actual al domeniului resurselor umane şi al potențialului uman al Mun. Bistrița, cât şi privitor la tendințele de evoluție în timp a acestor resurse şi capabilități, rezultă cu claritate faptul ca există, se menține şi chiar se amplifică migrația resursei umane a Mun. Bistrița mai ales către marile centre urbane din proximitate (ex. către Cluj-Napoca, Tg. Mureş, Oradea, Timişoara, Iaşi), dar şi către cele mai îndepărtate din sudul țării, precum şi spre destinații din afara României – acest fenomen fiind unul chiar mai amplu decât ceea ce înseamnă migrația internă.

Ca atare, este imperios necesar ca, prin dezvoltare urbană echilibrată, focalizată mai ales pe dezvoltarea mediului economic / de afaceri, să se poată inversa sensul migrației, iar acest lucru devine posibil în primul rând prin asigurarea **unui nivel de instruire şcolară adecvat formării de specialişti autoftoni capabili a dezvolta mediul economic local**, ceea ce să ducă finalmente la creşterea semnificativă a numărului de locuri de muncă, urmându-se, desigur, strategii adecvate de specializare inteligentă a zonei.

Asigurarea unui astfel de nivel de instruire, necesită în primul rând monitorizarea continuă şi atentă a procesului de instruire şcolară pe toate palierele sale, generarea de statistici relevante pentru evoluția procesului, astfel încât funcție de aceste evoluții să se poată lua măsurile de optimizare necesare.

Din acest motiv, realizarea sistemului digitalizat de evidență a copiilor şcolarizați din oraşul Bistrița şi distribuția acestora pe unități de învățământ, este o necesitate primordială, iar integrarea acestuia cu celelalte sisteme digitalizate ale municipalității care sunt recomandate prin Strategia de Smart City a Mun. Bistrița, va putea conferi interoperabilitatea acestei platforme software cu toate celelalte sisteme menite a constitui o bază decizională robustă ca instrument de asistare a politicilor/acțiunilor/măsurilor de dezvoltare urbană inteligentă şi durabilă.

Oportunitatea abordării în această manieră a segmentului educațional este dată de existența unui material uman local şi zonal cu capabilități certe de dezvoltare continuă prin instruire adecvată, nivelul constant evolutiv de instruire putând fi asigurat doar prin urmărirea atentă a cifrelor de şcolarizare şi a performanțelor şcolare din toate entitățile educaționale ale Mun. Bistrița, pentru a se putea acționa în timp real asupra situațiilor în care se constată scăderi ale performanțelor şcolare, cât şi în vederea implementării de măsuri menite a asigura creşterea continuă a acestora.

Referindu-ne la potențialul/capabilitățile de asimilare de cunoştințe şi abilități existente inclusiv în zonele rurale din proximitatea Mun. Bistrița, este de interes în egală măsură asigurarea de condiții menite a atrage în entitățile şcolare ale municipiului, alături de elevii/tinerii locali, a cât mai mulți elevi/tineri din zonele acestea de proximitate, în vederea înlesnirii şi către aceştia a unor niveluri de instruire evolutive/incrementale.

III. Obiective si rezultate detaliate

Realizarea obiectivelor principale menționate în cadrul secțiunii **I**, presupune în primul rând - ca obiectiv de detaliu de primă importanță - dezvoltarea, mai întâi la nivel structural, a unei **resurse de date specifice domeniului educațional**, această resursă de date - structurată ca o bază de date de înaltă performanță - urmând a fi stocată într-un centru de date specializat, găzduit în contextul arhitecturii cloud menită a integra toate platformele/sistemele care digitalizează procesele specifice ale administrației locale a Mun. Bistrița.

In vederea populării resursei de date, care este nevoie să fie exhaustivă privitor la absolut tot ceea ce caracterizează afluxul de material uman şi prezența acestuia în contextul procesului educațional, un al doilea obiectiv de detaliu este acela de **încărcare/populare a acestei resurse cu datele existente**, pentru ca mai apoi să fie **alimentată în mod continuu, în timp real, cu date noi, actualizate în permanență.**

In acest scop, este nevoie atât de **interfete de migrare date** - pentru cazul datelor care există deja, de pe urma unor activități de colectare a acestora deulate anterior, cât şi de **interfețe de culegere date si alimentare continuă cu date în timp real,** bazate pe capabilitățile de interoperabilitate asigurate prin mecanismele intrinseci ale **arhitecturii cloud** descrisă în secțiunile referitoare la infrastructura hardware .

Un alt obiectiv de detaliu important constă în aceea că platforma digitalizată de evidență a copiilor şcolarizați din Mun. Bistrița cu distribuția acestora pe unități de învățământ, va trebui să fie **accesibilă online,** prin intermediul unor **interfețe utilizator prietenoase şi eficiente**, operabile pe baza unor **ierarhii riguroase de drepturi de acces specifice fiecărui tip de utilizator** din categoriile de urtilizatori cărora le este destinată platforma, după cum urmează:

- **Funcționari ai Primăriei Mun. Bistrița** cu responsabilități în domeniul resurselor educaționale ale Municipiului (**UT1**)
- **Membrii Consiliului Local (UT2)**

- **Cetățeni ai Mun. Bistrița** interesați de resursele educaționale ale Municipiului (**UT3**)
- **Specialiştii de la Inspectoratul Scolar local (UT4)**
- **Funcționarii/Specialiştii de la nivel guvernamental** cu responsabilități în domeniul resurselor educaționale - in primul rând cei de la nivelul Ministerului Educației Naționale **(UT5)**
- **Părinții copiilor/tinerilor înrolați în procesul educațional sau care urmează a fi înrolați în procesul educațional (UT6)**
- **Elevi ai ciclului primar, gimnazial şi liceal (UT7)**
- **Educatori, cadrele didactice ale ciclului primar, cadrele didactice ale ciclului gimnazial si cadrele didactice de la nivelul liceelor (UT8)**
- **Asistenți sociali (UT9)**
- **Asistenți maternali (UT10)**
- **Funcționarii secretariatelor instituțiilor/entităților de învățământ** ale Mun. Bistrița (**UT11**)
- **Managerii/directorii instituțiilor/entităților de învățământ** ale Mun. Bistrița (**UT12**).

Cele cinci obiective principale prezentate în **Secțiunea I** (OP1, OP2, OP3, OP4 şi OP5) se detaliază pe tipurile de utilizatori mai sus menționate, după cum urmează:

Categoria de utilizatori **UT1** - **Funcționarii Primăriei Mun. Bistrița –** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1, OP2, OP3, OP4 şi OP5.

Categoria de utilizatori **UT2** - **Membrii Consiliului Local -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP2 şi OP5.

Categoria de utilizatori **UT3** - **Cetățeni ai Mun. Bistrița** interesați de procesul educațional din Municipiul Bistrița - vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1, OP2 şi OP3.

Categoria de utilizatori **UT4** - **Specialiştii de la Inspectoratul Scolar -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1, OP2, OP3, OP4 şi OP5.

Categoria de utilizatori **UT5** - **Funcționarii/Specialiştii de la nivel guvernamental -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1, OP2, OP3, OP4 şi OP5.

Categoria de utilizatori **UT6** - **Părinții copiilor/tinerilor înrolați în procesul educațional -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1 şi OP2.

Categoria de utilizatori **UT7** - **Elevi ai ciclului primar, gimnazial şi liceal** - vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1 şi OP2.

Categoria de utilizatori **UT8** - **Educatori, cadrele didactice ale ciclului primar, cadrele didactice ale ciclului gimnazial si cadrele didactice de la nivelul liceelor -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1 şi OP2, OP4 şi OP5.

Categoria de utilizatori **UT9** - **Asistenți sociali -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1 şi OP2.

Categoria de utilizatori **UT10** - **Asistenți maternali -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1 şi OP2.

Categoria de utilizatori **UT11** - **Funcționarii secretariatelor instituțiilor/entităților de învățământ -** vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1, OP2, OP3, OP4, OP5

Categoria de utilizatori **UT12** - **Managerii/directorii instituțiilor/entităților de învățământ** - vor fi interesați şi implicați în interacțiuni cu componentele sistemului care implementează obiectivele OP1, OP2, OP3, OP4 şi OP5.

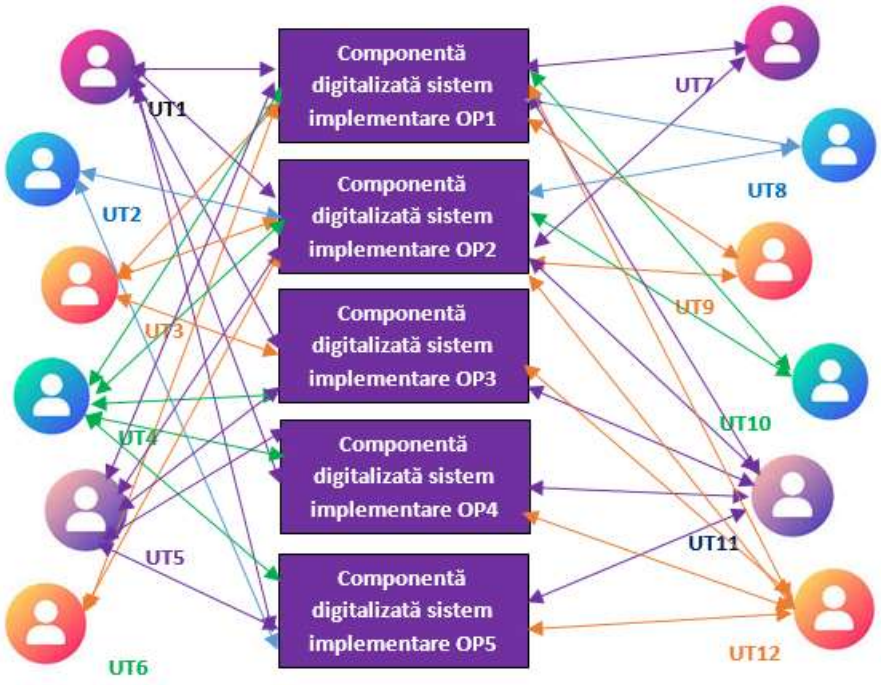


Fig. 1 Diagrama interacțiunilor utilizatorilor cu platforma

Diagrama din Fig. 1 de mai sus ilustrează intensitatea interacțiunilor utilizatorilor cu platforma digitalizată de evidență a copiilor şcolarizați din Mun. Bistrița, cu distribuția acestora pe unități de învățământ.

Rezultate pe termen scurt, mediu si lung:

Rezultatele pe termen scurt şi mediu care vor fi obtinute prin punerea în functiune a platformei vor consta în următoarele:

R1: Asigurarea contextului pentru **transpunerea în format digital a tuturor datelor aferente domeniului învățământului de pe toate nivelurile**, acesta reprezentând primul pas în demararea digitalizării întregului proces educațional al Mun. Bistrița

R2: Facilitarea interacțiunilor cu toți actorii implicați în procesul educațional (anume utilizatorii de tip UT1 – UT12), prin digitalizarea întregului proces putându-se maximiza eficiența derulării acestor interacțiuni într-o manieră prietenoasă, directă şi rapidă.

R3: Optimizarea activităților aferente procesului educațional de care răspund funcționarii publici ai Primăriei, angajații Inspectoratului Scolar cât şi staff-ul administrativ-birocratic din toate unitățile de învățământ ale Mun. Bistrița.

R4: Optimizarea interacțiunilor cu nivelurile guvernamentale, cât şi cu toți factorii locali de decizie implicați în strategia şi managementul procesului educațional al Mun. Bistrița.

Rezultatele pe termen lung sunt de asemenea de o importanță deosebită, ele înscriindu-se de fapt în setul de rezultate ce vor conferi Municipiului Bistrița statutul de Brained City – adică oraş cognitiv, aceasta fiind treapta cea mai înaltă de evoluție a Oraşului Inteligent. Setul acestor rezultate vizate în mod special prin evoluția pe termen lung a ecosistemului IT a Oraşului Inteligent Bistrița, cuprinde următoarele:

RL1: Acumularea unor seturi consistente de date masive, pe baza cărora vor putea fi realizate simulări şi prognoze privitoare la tendințele implicării numerice şi ca grad de capabilitate intelectuală, a copiilor şi tinerilor Mun. Bistrița în procesul educațional.

RL2: Această perspectivă a acumulării de date masive în timp permite **implementarea algoritmilor de Inteligență Artificială care stau la baza funcționalităților platformei suport pentru decizii**, ca o componentă importantă a sistemului de evidență a copiilor şcolarizați din Mun. Bistrița, cu distribuția acestora pe unități de învățământ.

Planul de implementare

Planul de implementare cuprinde:

- Modelarea, proiectarea şi implementarea componentelor resursei de date, după cum urmează:
- Baze de date pentru: Cadre Didactice, Scoli, Resurse Educaționale – amplasate în Componenta Educațională a Centrului de Date, plus Baza de Date pentru Evidența Populației – amplasată în Componenta Administrației Publice a Centrului de Date;

- Depozite de Date (DataWarehouse) şi componentele DataMart aferente – pentru stocarea datelor pe lunga durata în vederea aplicării mecanismelor de Inteligența Artificială pentru generarea rezultatelor pe termen lung.

- Identificarea setului exhaustiv de cazuri de utilizare ale platformei, care vor sta la baza proiectării şi implementării funcționalităților sistemului

- Definirea, proiectarea şi implementarea Interfețelor Utilizator cu capabilități avansate de interacțiune implementate cu tehnologii GUI bazată pe biblioteci de shape-uri grafice)

- Definirea, proiectarea şi implementarea componentelor de interfațare şi interoperabilitate cu celelalte sisteme/subsisteme ale contextului integrat de digitalizare a proceselor

specifice ecosistemului IT al Mun. Bistrița, cu găzduire pe infrastructura de cloud urban prezentată/recomandată în cadrul secțiunii referitoare la infrastructura hardware.

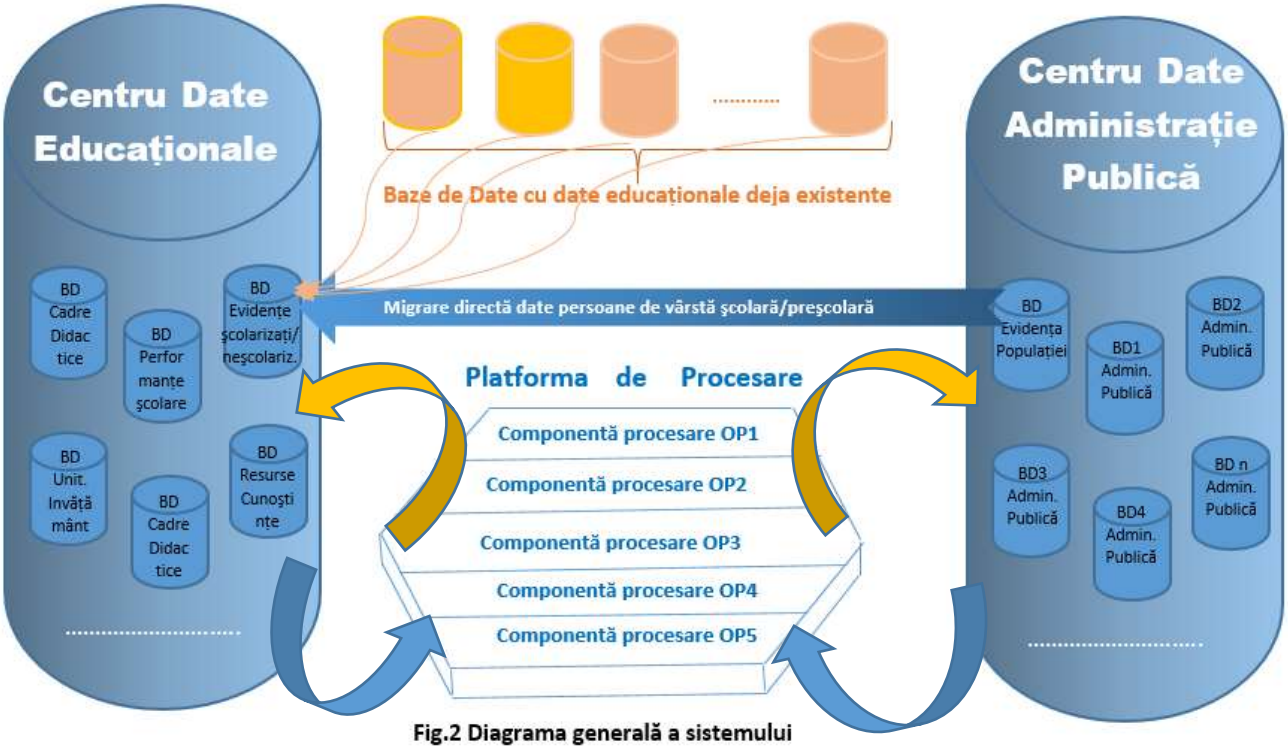


Fig.2 Diagrama generală a sistemului

Sustenabilitate şi impact

Sustenabilitate Sistemelor Informaționale/Informatice (SI) este abordată, în general, prin modele și instrumente dezvoltate pentru a evalua inclusiv sustenabilitatea organizațională bazată pe existența sistemelor informatice.

Practic, elementele pe care se bazează sustenabilitatea sistemelor informatice (deci a sistemelor digitalizate), sunt următoarele:

- Gradul în care sunt capabile a furniza cunoştințe/cunoaştere
- Gradul în care aceste sisteme sunt adaptabile
- Gradul de „offloading”, adică capabilitatea sistemului fie de a-si autocorecta erorile sau neconcordanțele care pot să apară pe parcursul versionărilor succesiv evolutive,

fie aceea de a permite efectuarea acestor corecții din mers, prin intervenția directă a specialiştilor IT, fără a fi nevoie de reimplementarea totală a sistemului.

In toate aceste trei sensuri, sustenabilitatea sistemului digitalizat de evidență a copiilor şcolarizați în oraşul Bistrița cât şi a distribuției acestora pe unități de învățământ, este conferită atât prin arhitectura software a acestuia, cât şi prin natura arhitecturii cloud a infrastructurii hardware pe care urmează a fi găzduit, dar şi prin intermediul componentelor structurale ale sistemului.

In mod mai concret, migrarea datelor educaționale din bazele de date şi situațiile deja existente în contextul IT actual al Municipalității Bistrița, asigură într-o primă etapă o populare rapidă cu datele actuale a bazelor de date ale Componentei Educaționale a Centrului de Date al Cloud-ului Urban. In urma finalizării operațiunilor de migrare a datelor deja existente, devine obligatorie renunțarea la bazele/sursele de date vechi, în vederea evitării paralelismelor şi redundanțelor.

In urma acestei prime etape de populare a Bazelor de Date din Centrul de Date al Cloud-ului Urban, alimentarea cu date se continuă dinamic, atât în mod direct prin migrarea de date bazată pe mecanismele de interoperabilitate ale arhitecturii de integrare pe cloud-ul urban, cât şi prin activitățile de interacțiune cu sistemul ale tuturor tipurilor de utilizatori (actori) cărora le este destinat, anume categoriile UT1-UT12 prezentate în secțiunile anterioare. Tot acest mecanism asigură o sustenabilitate a la long a alimentării cu date a resurselor de date educaționale gazduite în cloud.

In ceea ce priveşte sustenabilitatea componentelor de procesare, actualizarea acestora se realizează de asemenea în mod direct şi cu eficiență maximă în cadrul contextului integrat, acesta permițând cuplarea şi decuplarea fluxurilor de procesare în mod dinamic.

Impactul asupra dezvoltării comunității urbane Bistrița al sistemului digitalizat de evidență a copiilor şcolarizați în oraşul Bistrița şi a distribuției acestora pe unități de învățământ, este acela de a se putea monitoriza în permanență nivelul de educație şi instruire şi, ca atare, a se putea interveni cu acțiuni menite a regla şi chiar augmenta acest nivel, în folosul dezvoltării continue a mediului economic şi de afaceri al municipiului, aceasta fiind de fapt cheia evoluției într-o spirală continuu ascendentă a Oraşului Inteligent.

FISA DE PROIECT FANION

Titlu:

“GIS pentru gestiunea informațiilor de urbanism, colectarea şi accesibilitatea acestora”

Coordonator din partea consultantului:

Paulina MITREA

I. Scop, context şi justificare. Obiective principale, beneficiari si rezultate generice asteptate

In contextul ecosistemului de Oraş Inteligent, pilonul de Urbanism are o importanță deosebită prin faptul că acest pilon conferă şi gestionează cadrul fizic general, atât din punct de vedere estetic cât şi funcțional, al Oraşului Inteligent.

Proiectul se înscrie în gama proiectelor de digitalizare situate pe nivelul cel mai important al CaseiIT reprezentată în Fisa Proiectului Fanion de Management al Digitalizării/Transformării Digitale a Municipiului Bistrița, anume acela de organizare şi cultură pentru digitalizare/Arhitectură IT, Infrastructură şi Portofoliu de Aplicații.

Obiectivele principale ale proiectului vizează **realizarea unui sistem GIS pentru urbanism**, integrat pe arhitectura Cloud – ului urban al Municipiului Bistrița, care **să permită analiza și modelarea spațială**, elemente care pot contribui la o varietate de sarcini importante de planificare urbană.

Planificarea urbană fiind atât un proces de proiectare, cât și de dezvoltare arhitecturală a terenurilor deschise, a zonelor urbane și a mediului construit, este de fapt un proces cu mai multe fațete care implică:

- Infrastructură urbană
- Sisteme de utilități
- Rețele de comunicați
- Lanțuri de distribuție și multe altele.

Gestionarea atâtor variabile poate fi o provocare substanțială, dar **tehnologia GIS modernă** este cea care oferă soluția adecvată nivelului tehnologic al zilelor noastre, sub următoarele aspecte:

- hărțile GIS permit afișarea datelor aferente locației geografice în straturi
- datele GIS sunt organizate/stocate tot pe straturi în cadrul Bazei de Date Geografice la care este conectat sistemul GIS.

Beneficiarii proiectului sunt, în primul rând, factorii de decizie din domeniul urbanismului şi planificării urbane ai Municipiului Bistrița, funcționarii publici din departamentul de urbanism, arhitecții şi constructorii/dezvoltatorii implicați în dezvoltarea urbană a Municipiului Bistrița precum şi toți cetățenii interesați în dezvoltarea urbană..

Rezultatele aşteptate în urma implementării proiectului, constau în **furnizarea unui instrument digitalizat complex, constând într-o platformă GIS integrată pe cloud-ul urban al Municipiului Bistrița,** care va permite abordarea şi efectuarea activităților de urbanism şi planificare urbană într-o manieră eficientă şi armonioasă, datorită posibilității de abordarea problemelor de

urbanism într-un context extins, ce permite controlul tuturor interdependențelor existente la nivelul urbei.

II. Obiective si rezultate detaliate

Obiectivele detaliate ale proiectului sunt mulate practic pe varietatea de sarcini importante de planificare urbană care urmează a fi automatizate, aceste sarcini incluzând:

- Selectarea amplasamentului diverselor obiective de urbanism
- Analiza adecvării terenului
- Modelarea utilizării terenului și a căilor de acces (transport)
- Identificarea zonelor de acțiune de tip planificare
- Evaluări de impact.

Abordarea acestor obiective se referă, evident, la principalele straturi aferente oricărei locații geografice din contextul urban, după cum urmează:

- Stratul (layer-ul) clădirilor
- Stratul (layer-ul) utilităților subterane
- Stratul (layer-ul) suprateran sau subteran al liniilor electrice
- Stratul (layer-ul) liniilor de comunicații
- Stratul (layer-ul) vegetației

Tot ca straturi – de această dată adiacente - pot fi considerate următoarele:

- Stratul (layer-ul) rețelei de străzi dintr-o localitate
- Stratul (layer-ul) parcărilor şi locurilor de parcare din zonele centrale şi rezidențiale
- Stratul (layer-ul) rutelor de transport public.

Ca atare, sistemul GIS integrat pe cloud care urmează a fi realizat, are menirea de a crea astfel de hărți care să poată gestiona mai eficient cantități mari de date urbane complexe.

Rezultate pe termen scurt, mediu si lung:

Rezultatele pe termen scurt mediu şi lung care vor fi obtinute prin punerea în functiune a platformei vor consta în furnizarea într-o manieră elegantă şi eficientă a următoarelor funcționalități:

Funcționalitățile de bază ale oricărui sistem GIS:

- Cartografiere ca funcționalitate de bază, înțelegand prin aceasta generarea de hărți ale tuturor straturilor mai sus menționate, afişabile separat sau suprapuse în diverse combinații ale lor
- Managementul (gestionarea) de date geografice într-un context integrat la nivel urban
- Managementul (gestionarea) tuturor activelor urbane
- Detectarea modificărilor (Detecția schimbărilor)
- Planificare urbană integrată la nivelul întregului municipiu
- Managementul situațiilor de urgență și dezastre.

Vizualizarea datelor cu cartografierea GIS va permite:

- Urmărirea progresului pe măsura dezvoltării în timp a zonelor urbane
- Analiza relațiile spațiale dintre straturi
- Gestionare de sarcini ale unor echipe de proiectare/dezvoltare
- Identificarea de zone cu diverse grade de risc
- Urmărirea graficului rutelor de transport
- Compararea caracteristicile naturale cu cele generate prin activitate umană.

Deși cartografierea este cea mai obișnuită funcționalitate pentru GIS, aceste hărți sunt, de asemenea, baza pentru toate celelalte funcționalități: managementul datelor, managementul activelor, detectarea schimbărilor etc.

Planul de implementare

Planificarea urbană fiind procesul de proiectare și decizie de utilizare a terenurilor în orașe și municipii, ceea ce se referă inclusiv la alocarea resurselor necesare pentru activitățile de transport, comunicații, construcții, ca atare planificarea urbană are mai multe fațete și poate fi destul de complexă. De aceea, un GIS modern este util în special pentru orașele care se confruntă cu o creștere rapidă, aşa cum îşi propune şi Municipiul Bistrița prin toate strategiile sale de dezvoltare urbană.

Pe măsură ce orașul crește, la fel și cerințele de infrastructură. Rețelele energetice, sistemele de canalizare, conductele și drumurile trebuie să fie toate planificate și construite într-un mod durabil și scalabil.

Ca atare, planificatorii urbani ai Municipiului Bistrița vor putea folosi sistemul GIS integrat pe Cloud pentru a compila toate datele de infrastructură pe o aceeaşi hartă. Cu această hartă, ei vor putea urmări creșterea actuală şi viitoare, vor putea monitoriza starea de sănătate a infrastructurii existente și vor putea crea un plan scalabil pentru viitor.

Pentru că datele geospațiale sunt de fapt baza oricărui sistem GIS, planul de implementare trebuie să înceapă de la nivelul acestora, continuând cu toate celelalte elemente de procesare aferente lor, menite a genera funcționalități specifice, după cum urmează:

Planul de implementare a funcționalităților de management al datelor:

De la foi de calcul la fotografii, imagini din satelit, până la sarcini de proiect – platforma GIS integrată pe cloud-ul urban urmează a fi un instrument excelent pentru organizarea, analizarea și partajarea datelor bazate pe locație, pentru că sistemele GIS în general sunt folosite pentru a gestiona aproape orice tip de date, precum:

- Foi de calcul
- Fotografii
- Videoclipuri
- Hărți topografice
- Imagini din satelit și aeriene în general
- Scheme și planuri diverse

Pe baza managementului acestor categorii de date, pot fi dezvoltate în mod prioritar **funcționalitățile de management al activelor,** ale căror caracteristici sunt detaliate în cele ce urmează.

Activele fizice ale oricărei localități sunt dispersate geografic. În plus, fiecare are propriul său istoric, specificații și program de întreținere. Această combinație de date și locația acestora face ca sistemul GIS integrat să fie instrumentul perfect pentru gestionarea eficientă a activelor, asociat cu localizarea geografică a acestora, după cum urmează:

- Urmărirea pe hartă a localizării activelor
- Inregistrarea activelor şi a localizării precise a acestora în contextul sistemului GIS
- Menținerea unui inventar actualizat de active
- Estimarea şi urmărirea ciclului de viață al activelor
- Prezicerea riscului defectării/deteriorării activelor
- Generarea calendarului activităților de întreținere preventivă, calendar bazat pe date referitoare la tipul şi caracteristicile activelor în cauză.

In următoarea ordine de prioritate, sunt dezvoltate funcționalitățile de detecție a schimbărilor din contextul urban, după cum urmează:

Detectarea modificărilor urmărește modul în care un activ sau o zonă se schimbă în timp. Deși se pot urmări schimbările printr-o foaie de calcul sau alt flux de lucru liniar manual, aceste metode nu sunt eficiente.

Sistemul GIS integrat pe cloud va reprezenta de departe cea mai eficientă modalitate de a urmări vizual schimbările pe suprafețe extinse şi pe perioade lungi de timp.

Metodele de urmărire a modificărilor includ:

- Stratificarea evoluțiilor semnalate prin preluarea de imagini de la înălțime
- Stratificarea hărților topografice
- Planuri suprapuse pe preluările anterioare de imagini de la înălțime (fotograme)
- Documentație foto cu etichetare geografică.

Abilitatea de a urmări schimbările în timp, deși destul de simplă, este incredibil de utilă pentru o multitudine de industrii/domenii de activitate urbană, după cum urmează:

- În construcții - se poate monitoriza evoluția construcției.
- În silvicultură - se poate urmări interacțiunea dintre activitatea umană și lumea naturală.
- În planificarea urbană - se poate urmări dacă identitatea unui bun fizic s-a schimbat, adică dacă o clădire care a fost un restaurant (spre exemplu) este acum un magazin pentru animale de companie.

De o importanță deosebită sunt, de asemenea, funcționalitățile destinate managementului situațiilor de urgență și dezastre.

In acest sens, cele mai relevante cazuri de utilizare pentru o abordare eficientă sunt următoarele:

- Definirea limitelor zonei afectate
- Crearea unui inventar al proprietăților distruse, al infrastructurii deteriorate și al persoanelor dispărute
- Prioritizarea pașilor de acțiune în funcție de zonele cele mai afectate
- Crearea de planuri cuprinzătoare de răspuns și recuperare.

Sistemul GIS integrat va fi instrumentul perfect pentru a se putea implementa în contextul său toate aceste funcționalități, oferind astfel responsabililor cu managementul situațiilor de urgență o modalitate de a accesa și partaja rapid datele bazate pe locație.

Din punctul de vedere al componentelor structurale ale sistemului GIS integrat pe cloud, abordarea în cea ce priveşte implementarea focalizează următoarele:

Componenta Hardware

In general, în cazul sistemelor GIS clasice, hardware-ul poate fi un dispozitiv fizic local: computer, laptop, tabletă, telefon mobil etc. Majoritatea programelor GIS vechi pot rula doar pe un desktop, necesitând servere locale. În general, acestea nu pot fi utilizate pe dispozitive mobile.

Sistemul GIS integrat pe cloud-ul urban, va avea însă ca infrastructură hardware arhitectura prezentată în fişa de proiect care detaliază componentele hardware ale cloud-ului urban propus pentru Municipiul Bistrița, această arhitectură fiind interfațabilă inclusiv cu orice tip de dispozitive mobile.

Componenta Software

Software-ul GIS integrat pe Cloud este instrumentul digital care va permite capturarea, organizarea, stocarea și procesarea datelor geospațiale. Funcționalitățile principale implementate la nivel software, sunt următoarele:

- Gestionarea datelor bazată pe locație
- Instrumente pentru captarea datelor
- Opțiuni pentru vizualizare
- Accesarea acestor funcționalități atât online cât şi offline.

Componenta de Date

Datele sunt probabil cea mai semnificativă componentă a oricărui sistem GIS. Acestea pot proveni sub următoarele formate, corespunzătoare tipurilor de date enumerate şi în secțiunile anterioare:

- Foi de calcul
- Imagini prin satelit
- Schițe și planuri
- Hărți topografice
- Shapefiles.

Recomandările pentru standardizarea datelor pentru sistemul GIS integrat pe cloud-ul urban:

OGC (Open Geospatial Consortium) este o comunitate profesională care creează standarde geospațiale deschise, care pot fi utilizate atât de sistemele deschise, cât și de cele proprietare.

Câteva dintre aceste standarde sunt:

- SRID - o identificare pentru sistemele de coordonate spațiale
- WFS (Web Feature Service) - pentru preluarea sau modificarea descrierilor caracteristicilor
- WMS (Serviciu de Hărți Web) - oferă imagini de tip hartă
- WMTS (Web Map Tile Service) - furnizează imagini ale unor zone rectangulare ale hărții felii de hartă)

- KML (Keyhole Markup Language) - schemă de limbaj bazată pe XML pentru exprimarea adnotărilor geografice și a vizualizării pe hărți existente (sau viitoare) bidimensionale, bazate pe web și browsere Earth tridimensionale.

Componentele funcționale ale sistemului GIS integrat pe cloud-ul urban vor fi următoarele:

1. **Interfața cu utilizatorul** în care utilizatorii interacționează cu sistemul. Această componentă constă din hardware precum laptopuri, computere desktop și dispozitive mobile, precum și software de tip browser și aplicații pe care utilizatorul le accesează direct.

2. **Aplicațiile** sunt componentele software pe care utilizatorul le poate folosi pentru a manipula sau analiza datele.

3. **Sistemul de management al bazelor de date** (DBMS) este software-ul care controlează accesul la date și le convertește în formate care pot fi utilizate prin intermediul unor instrumente și interfețe cu utilizatorul.

4. **Baza de date** este resursa care stochează datele geospațiale şi le pune la dispoziția utilizatorilor.

În contextul arhitecturii cloud, rack-uri masive de servere pot rula în centrul de date de mare capacitate dedicat sistemului GIS în cloud-ul urban. Flexibilitatea arhitecturii cloud permite însă ca administratorii serverelor din Cloud să poată crește sau reduce capacitatea acestor servere în funcție de nevoi, permițând astfel o utilizare mai economică a resurselor.

Gruparea în contextul interfețelor utilizator a funcționalităților specifice GIS-ului urban integrate într-o singură platformă, va fi următoarea:

- **Funcționalități de asigurare a suportului spațial**, prin intermediul sistemului GIS integrat, **pentru maparea tuturor resurselor** de pe teritoriul Municipiului Bistrița, prin resursă înțelegându-se:
  (a)Infrastructuri aparținând furnizorilor de rețele de utilități, rețele de transport (mărfuri, călători)
  (b) Resurse materiale (echipamente, instalații), educaționale, culturale (școli/gradinițe etc)
  (c) Elemente de infrastructură teritorială de tip imobiliar (terenuri, clădiri) indiferent de tipul de proprietate
  (d) Capacități de procesare, depozitare, transport
  (e) Resurse turistice locale.

- Functionalitati de asigurare a suportului spațial, prin intermediul sistemului GIS integrat, **pentru identificarea constrângerilor urbanistice** care grevează un imobil (teren sau construcție)

- **Transpunerea spațială a actelor urbanistice** solicitate de cetățeni, respectiv a celor emise de către autoritățile locale

- **Asigurarea conectării cu deținătorii de date publice** (Agenția de Cadastru și Publicitate Imobiliară, Registrul Comerțului, Direcția de Evidență a Populației, deținătorii de rețele publice, ș.a.), si transpunerea spațială a acestor date

- **Tool-uri, analize, funcționalități menite a furniza suport pentru fundamentarea deciziilor si a politicilor publice**, in contextul unor planuri urbanistice strategice, integrate la nivel de Municipiu

- Funcționalități care permit **implementarea de noi instrumente de planificare**, ajustarea și integrarea celor existente

- Funcționalități de **accesare a bazelor de date GIS disponibile la diversele instituții și agenții publice**, asigurându-se transpunerea lor spațială și realizarea unor seturi de date necesare pe subdomenii, reunirea într-o singură platformă a mai multor seturi de date disponibile conducând și la asigurarea unei mai bune coordonări a activităților de amenajare a teritoriului, urbanismului, locuirii, dezvoltării economice, care pot concura la dezvoltarea unor noi seturi de politici publice

- **Accesare și interogare în timp real a datelor** de la toate nivelurile arhitecturii de date a sistemului GIS integrat

- **Procesarea datelor în vederea extragerii de informații suport pentru decizii**, plus tehnici avansate de coroborare/procesare a informațiilor.

In ceea ce priveşte sistemele moderne de achiziție a datelor geospațiale urbanistice de orice fel, se recomandă implicarea tehnologiilor moderne de scanare a întregului inventar urban, cum ar fi tehnologia **Infra3D** pentru scanarea resurselor/activelor urbane şi introducerea datelor direct în GIS.

Această tehnologia Infra3D poate fi utilizată de către serviciile din cadrul Primăriei după cum urmează:

1. **Serviciul Urbanism:**

- în cadrul Serviciului de Urbanism se pot face simulări pentru reamenajarea, remodelarea zonelor de interes (centrul orașului, pricipalele bulevarde, etc....)

- se poate verifica respectarea condițiilor cerute în autorizația de costrucție (fațade, înălțimi, lățimi, reclame publicitare, etc. ...), prin scanare 3D simultană cu măsurarea elementelor care constituie parametri reglementați

- există de asemenea layer pentru măsurarea distanțelor, diferitelor arii, suprafețe

- se pot elabora studii de fezabilitate pentru implementarea proiectelor imperios necesare pentru atragerea de fonduri europene.

2. **Serviciul Administrației Domeniului Public**:

- culegere date despre infrastructura rețelelor de utilități (apă, canal, gaz, fibră optică, rețeaua de distribuție a energiei electrice, etc)

- date de inventariere a mobilierului stradal (copaci, stâlpi de electricitate, semafoare, coșuri de gunoi, indicatoare rutiere, bănci, etc. ...)

- filmarea, procesarea și coroborarea datelor terestre cu cele aeriene (geospațiale), în puncte cloud

- posibilitatea procesării datelor în puncte cloud vizavi de o anumită adâncime.

3. **Serviciul Tehnic**

- cu ajutorul instrumentului de Scanare Laser se poate evalua starea drumului prin colectarea de date Infra3D şi migrarea acestora în platforma GIS integrată

- se pot extrage date despre lățimea drumului, lungimea acestuia, arii de interes (pentru lucrările de plombări, asfaltări, etc...)

- pe baza datelor colectate se pot calcula liste de cantități în perspectiva încheierii unui contract de construcții pe o anumită zonă

- tot pe baza datelor colectate, se poate evalua gradul de inundabilitate pe fiecare stradă în parte sau o pe anumite zone de interes, aceaste informații fiind extrem de importante în vederea eliminării riscului de inundații pe raza orașului.

Este important de menționat faptul că toate datele procesate pot fi descărcate în orice sistem operațional (GML, DXF, KML, ESRI Shape Files , precum și alte sisteme existente). Informațiile pot fi accesate și administrate foarte ușor de pe calculator, tabletă sau celular.

De asemenea interacționarea cu orice sistem GIS existent se poate efectua la cererea beneficiarului aproape instantaneu.

Fig. 1 Afişare Layer Utilități din GIS, pe baza datelor scanate cu tehnologia Infra3D; cod culoare: galben pt. conuctele de gaz, albastru pentru apa potabilă, rosu pt. comunicatii, verde pentru apa uzată

Arhitectura Sistem GIS integrata in cloud-ul urban

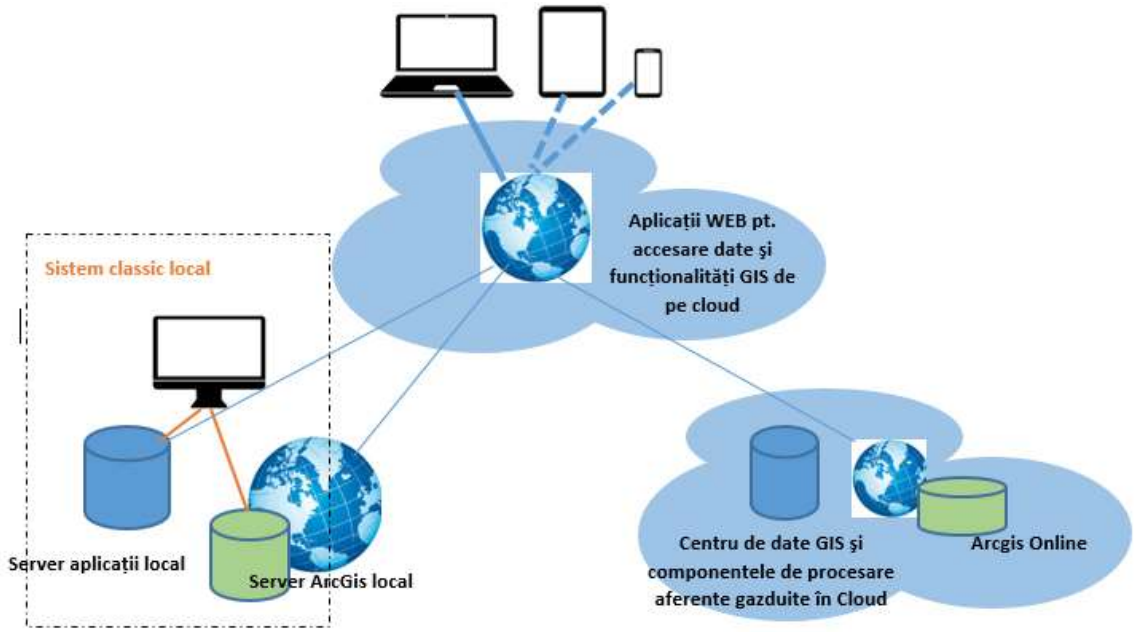


Fig. 2 Diagrama de Arhitectură a Sistemului GIS integrat în Cloud-ul urban

Sustenabilitate şi impact

Sustenabilitatea sistemului este dată de însăşi abordarea privind integrarea acestuia pe arhitectura cloud-ului urban descris în Fişa de proiect de infrastructură.

Impactul asupra dezvoltării comunității urbane Bistrița al sistemului GIS integrat pe cloud-ul urban va fi acela al unei dezvoltări urbanistice accelerate şi armonioase, de care Municipiul Bistrița are neapărată nevoie şi de care este pe deplin cababil, avându-se în vedere atât resursa umană cu un bun potențial şi capabilități conferite prin procesul educațional de bună calitate care se derulează în Municipiul Bistrița, cât şi oportunitățile datorate contextului geografic în care este amplasat Municipiul, acesta fiind de natură a încuraja în primul rând turismul, acesta fiind şi un domeniu de specializare inteligentă a oraşului Bistrița şi a regiunii în care se află.

FISA DE PROIECT FANION

Titlu:

“Sistem de urmărire în timp real a pericolelor din perimetrul unităților de învățământ folosind camere video şi Inteligență Artificială”

Coordonator din partea consultantului:

Paulina MITREA

I. Scop, context şi justificare. Obiective principale, beneficiari si rezultate generice aşteptate

In linia abordării care conferă o importanță deosebită pilonului educațional al Oraşului Inteligent, siguranța elevilor - asigurată prin securizarea unităților educaționale şi a proximității acestora - face parte din prioritățile sistemului general de Siguranță Publică, aflându-se de fapt la interferența pilonului educațional cu pilonul de siguranța publică (Public Safety Pillar) al Oraşului Inteligent.

Proiectul se înscrie în gama proiectelor de digitalizare situate pe nivelul cel mai înalt al Casei IT reprezentată în Fişa Proiectului Fanion de Management al Digitalizării/Transformării digitale a Municipiului Bistrița, anume pe cel de Organizare şi Cultură pentru digitalizare/Arhitectură IT, Infrastructură şi Portofoliu de Aplicații.

Obiectivele generice:

Administratorii și personalul școlilor din Municipiul Bistrița având responsabilități multiple, siguranța elevilor este o prioritate de prim rang. De aceea, se așteaptă ca școlile să mențină elevii în siguranță și să aibă sisteme adecvate pentru a-i proteja de orice, de la simplă hărțuire, la posibile agresiuni fizice, dar şi la urgențe precum dezastre naturale sau alte situații care pot necesita intervenție medicală – spre exemplu.

Peste tot în lume, această siguranță a elevilor este considerată o problemă prioritară, iar preocupările și presiunea părinților și societății au crescut în mod constant de-a lungul anilor.

Din acest motiv, supravegherea video devine deja o parte importantă a planului general de securitate/siguranță al școlilor, existând beneficii substanțiale în acest sens, după cum urmează:

- Sistemele de supraveghere video ale şcolilor pot îmbunătăți pregătirea și răspunsul în situații de urgență.

- Supravegherea video este în prima linie de apărare atunci când se pune problema protejării şcolilor, deoarece bazat pe aceste sisteme, orice școală poate fi mai proactivă în ceea ce privește siguranța arealului în care se află și poate ști în timp real când au loc activități suspecte.

- Supravegherea video îmbunătățește răspunsul în situații de urgență pentru școli și oferă un indiciu clar că școala apreciază siguranța, din aceste motive, majoritatea părinților tinzând să susțină existența camerelor de supraveghere atâta timp cât acestea sunt instalate în mod responsabil.

- Este esențial să existe informații fiabile și actualizate în timpul unei urgențe, iar securitatea video ajută la furnizarea acestor informații.

Ca atare, **obiectivele principale** ale proiectului vizează următoarele:

- Răspuns la posibilele incidente din perimetrul şcolilor în timp optim, qvasi-imediat, cu alerte automate în timp real.

- Partajarea cu ușurință a imaginilor live, în timp real, cu personalul de intervenție.

- Detecție pro-activă a comportamentelor suspecte, pe bază de analitice (inclusiv tehnologii AI).

- Descurajarea infracțiunilor de orice fel, precum furt, vandalism, furtul de mașini și alte potențialele amenințări, mai ales prin instalarea de camere de supraveghere la vedere, astfel încât orice persoană cu intenții de violență sau infracționalitate de orice fel să fie determinată a se gândi de două ori înainte de a comite o infracțiune, deoarece posibilitatea de a se confrunta cu repercusiuni juridice negative crește dramatic în prezența sistemului de supervizare video; în acest sens, camerele de tip „bullet" – prezentate în secțiunile care urmează - sunt o alegere bună pentru zonele în care școlile doresc să facă evident faptul că are montate camere de supraveghere video a zonelor de proximitate.

- Prevenirea escaladării agresivității de orice fel, prin detectarea automată a mișcărilor agresive şi chiar a luptelor fizice, în timp real.

- Rezolvare rapidă a investigațiilor pentru a proteja posibilele victime și pentru a conferi siguranța pedepsirii vinovaților în cazurile de infracționalitate comisă în proximitatea şcolii

- Tratarea tuturor incidentelor în mod corect, folosind dovezi video obiective pentru a verifica sau infirma posibilele acuzații de agresiune.

- Controlul video al accesului în clădirile şcolilor, atât în timpul orelor cât şi în afara acestora, acest lucru fiind deosebit de important deoarece cunoașterea faptului că nu există intruşi în sediul şcolilor/grădinițelor este crucială pentru siguranța întregului campus şcolar. Capacitatea de a detecta vizitatori neautorizați este un avantaj major al camerelor de supraveghere. Acestea facilitează ca personalul de pază şi ordine să țină

evidența elevilor și profesorilor și să înțeleagă mai bine cine ar trebui sau nu ar trebui să se afle pe perimetrul școlii.

- Funcțiile AI precum Recunoașterea Facială prin tehnologii de Pattern Recognition (Recunoaştere de forme), oferă școlilor și mai multă putere de a detecta în timp real vizitatorii neautorizați și de a îmbunătăți securitatea în acest fel.

- Camerele de supraveghere cele mai moderne au o rezoluție mult mai bună decât camerele din generațiile anterioare, calitatea video superioară facând posibilă monitorizarea eficientă a unor spații mari în aer liber, cum ar fi parcări, locuri de joacă, terenuri de sport, precum şi spațiul stradal din proximitatea şcolilor.

Fig. 1 Supraveghere cu camere video a zonelor din proximitatea unităților educaționale

- Camerele de supraveghere ale școlilor oferă inclusiv părinților liniște sufletească, deoarece nimic nu este mai important pentru părinți decât siguranța copiilor lor; părinții se pot baza astfel în totalitate pe școală pentru a-și menține copiii în siguranță și pot avea încredere în administrația școlii privitor la posibilitatea investigării în mod corespunzător a conflictelor, cât şi la un tratament corect aplicat copiiilor, în condițiile rezolvării rapide a posibilelor probleme de orice fel.

- Prezența camerelor de supraveghere demonstrează faptul că administrația școlii ia în serios prevenirea şi rezolvarea conflictelor și acordă prioritate siguranței elevilor și preocupărilor generale ale părinților; camerele de supraveghere permit, de asemenea,

administratorilor şi staff-ului şcolar să rezolve incidentele mai rapid și să ofere părinților răspunsuri prompte și satisfăcătoare.

II. Obiective şi rezultate detaliate

Realizarea obiectivelor principale menționate în cadrul secțiunii **I**, presupune în primul rând - ca obiectiv de detaliu de primă importanță - dezvoltarea, mai întâi la nivel structural, a unei **resurse de date video**, această resursă de date - structurată ca o bază de date de înaltă performanță - urmând a fi stocată într-un centru de date specializat, găzduit în contextul arhitecturii cloud care este menită a integra toate platformele/sistemele care digitalizează procesele specifice ale administrației locale a Municipiului Bistrița.

Resursa de date va avea rolul de a constitui baza necesară dezvoltării soluțiilor de Inteligență Artificială asociate sistemului de supraveghere.

In vederea populării resursei de date video, aceasta trebuie să fie **alimentată în mod continuu, în timp real, cu date video noi, transmise către aceasta în permanență.**

Un alt obiectiv de detaliu important constă în aceea că sistemul de supraveghere video trebuie să fie **accesibil online,** prin intermediul unor **interfețe utilizator prietenoase şi eficiente**, operabile pe baza unor **ierarhii riguroase de drepturi de acces specifice fiecărui tip de utilizator** din categoriile de urtilizatori cărora le este destinată platforma, după cum urmează:

- **Administratorii şcolilor**
- **Membrii managementului şcolar**
- **Părinții elevilor**
- **Poliția Locală**
- **Funcționarii Inspectoratului şcolar**
- **Funcționarii Primăriei care au responsabilități privitor la rețeaua şcolară a Municipiului Bistrița**

Detalii privind sistemul de supraveghere video a zonelor din proximitatea şcolilor

A. Supravegherea video bazată pe cloud

Supravegherea video bazată pe cloud este un tip de securitate video în care filmările capturate sunt stocate de la distanță în cloud și nu pe un server sau dispozitiv la fața locului.

Sistemele cloud combină funcționalitatea unui sistem tradițional de camere de securitate cu puterea și ușurința tehnologiei cloud, pentru că acestea oferă multe beneficii pe care sistemele

tradiționale nu le oferă, inclusiv accesul nativ la distanță, managementul centralizat și o reducere semnificativă a hardware-ului sistemului.

Diferența fundamentală dintre sistemele tradiționale și sistemele cloud constă în aceea că soluțiile traditionale „on-premise" folosesc servere locale (la fața locului) pentru a funcționa și stoca date, în timp ce soluțiile cloud folosesc servere cloud la distanță pentru a realiza același lucru într-o manieră mult mai elegantă şi eficientă – inclusiv sub aspectul costurilor.

Este deci de luat în considerare această schimbare tehnologică în industria supravegherii video, care ține cont de potențialul infrastructurii cloud – arhitectura IT recomandată pentru digitalizarea proceselor administrației publice a Municipiului Bistrița.

A.1 Modalitatea de funcționare a supravegherii video în cloud

Toate sistemele de camere de securitate captează imagini de supraveghere. Diferența de bază dintre ele constă în ceea ce se întâmplă cu materialul video odată ce este capturat - cum este transmis și cum este stocat.

Până de curând, toate sistemele de supraveghere video necesitau un video recorder la fața locului (NVR sau DVR) pentru a înregistra și stoca datele video. Un astfel de sistem este în general denumit sistem de supraveghere „la locație" sau „tradițional".

Sistemele bazate pe cloud elimină nevoia existenței unor recordere și servere locale - cu alte cuvinte, nu mai este nevoie de NVR-uri sau DVR-uri.

Practic, sistemele de supraveghere video transmit datele video capturate prin intermediul camerelor de luat vederi în cloud, unde sunt procesate (cloud computing) și stocate, permițând accesul video nativ de la distanță, de oriunde și de pe orice dispozitiv (stație de calcul legată la Internet, laptop, telefon mobil etc), acest lucru fiind ilustrat prin intermediul Figurii 2.

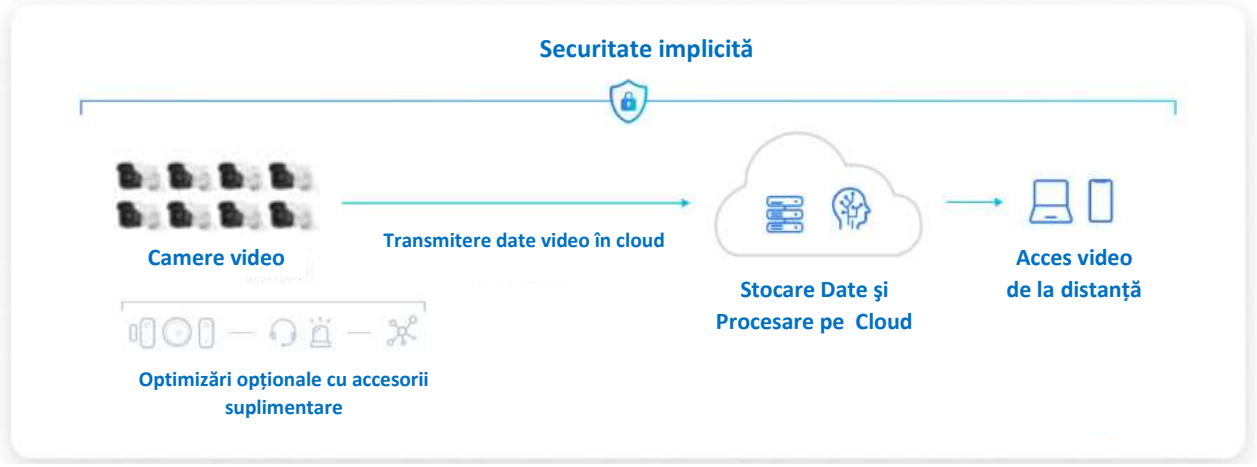


Fig. 2 Sistem VSaaS (Supraveghere Video ca Serviciu Cloud)

Supravegherea video bazată pe cloud funcționează prin transmiterea datelor video prin Internet pentru a stoca imaginile în cloud, propriu-zis într-unul din servere-le din care este format cloud-ul urban, spre deosebire de situația în care ar trebui să fie stocate pe un server local sau pe un hard disk, ceea ce ar necesita nişte costuri suplimentare de întreținere şi o utilizare mult mai complicată.

Pe lângă faptul că sistemele cloud sunt mult mai uşor de întreținut, software-ul de gestionare a videoclipurilor în cloud deblochează o serie întreagă de capabilități și caracteristici care conferă o putere mult mai mare gestionării securității, fiind vorba de fapt de acea securitate cibernetică implicită conferită de însuşi contextul cloud, care este pusă explicit în evidență şi în cadrul Figurii 2. Astfel, situația securizării proximității unităților educaționale poate fi urmărită atât în mod centralizat la nivel urban prin intermediul unui dispecerat care permite vizualizarea simultană a proximității tuturor unităților educaționsale, cât şi la nivelul local al acestora, pentru a se putea interveni rapid şi eficient în caz de pericol. Aceste tipuri de dispecerate sunt prezentate în ANEXE.

Comparativ cu soluția bazată pe cloud, soluțiile tradiționale, care nu sunt cuplate în cloud, necesită şi mult hardware suplimentar, ceea ce este ilustrat prin intermediul Figurii 3, după cum urmează:

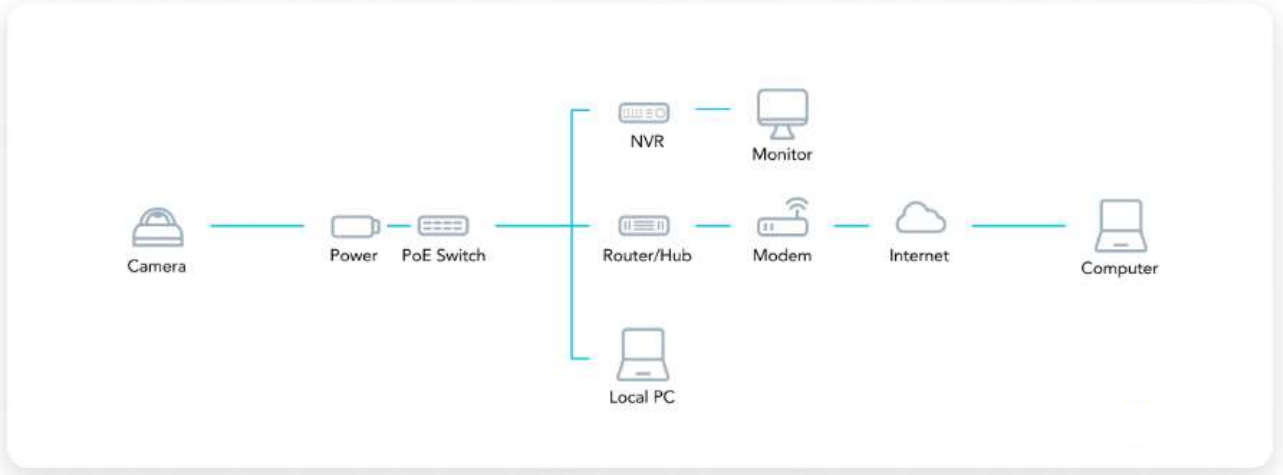


Fig. 3 Soluție tradițională locală, necuplată la cloud

Se observă, în cadrul Figurii 3, prezența unei multitudini de dispozitive absolut necesare în cazul unei soluții de tip strict local, toate acestea necesitând costuri suplimentare de achiziție, întreținere şi procesare, mai ales în situația în care se integrează în sistemul local şi algoritmii AI de recunoaştere facială, spre exemplu.

A.2 Componentele sistemului de supraveghere video bazat pe cloud

2.1Camere video de supraveghere cu IP în cloud

La fel ca şi camerele IP tradiționale, camerele cloud transmit date video folosind Internetul - o legătură Ethernet de rețea, Wi-Fi, LAN sau rețea celulară. Cu toate acestea, camerele cloud transmit și salvează datele video direct pe un server cloud la distanță, în loc să transmită datele video către un video recorder local (NVR sau DVR), de unde, pentru a putea fi centralizate la nivel de oraş, ar trebui să fie preluate şi migrate în entrele De Date şi Procesare de pe cloud – acest lucru fiind în mod clar ineficient

2.2 Software de procesare/management video în cloud (VMS – Video Management Software)

Software-ul de management video (VMS) este cel care facilitează utilizarea sistemului de supraveghere video, fiind capabil a genera analitice cât şi funcționalități bazate pe tehnologii de Inteligență Artificială precum Recunoaşterea Facială.
Acest software asigură de asemenea interfața prin care se vizualizează filmările efectuate cu camerele de luat vederi cuplate la sistem și se interacționează cu aceste filmări, conform funcționalităților implementate în acest software, după cum urmează:

- Efectuare de investigații
- Salvare video- clipuri și partajare filmări
- Managementul drepturilor de acces
- Managementul camerelor video
- Managementul setărilor de sistem
- Funcții de analiză aprofundată, inclusiv funcții de analiză bazate pe tehnologii de Inteligență Artificială

Software-ul de gestionare a videoclipurilor în cloud nu este legat de anumite dispozitive fizice. De obicei, se bazează pe aplicații sau pe browser și poate fi descărcat pe orice dispozitiv, acest lucru oferind mult mai multă flexibilitate comparativ cu sistemele de supraveghere video strict locale, necuplate la cloud.

2.3 Serviciile oferite prin intermediul sistemului VsaaS

„VSaaS" înseamnând „Video Surveillance as a Service" permite achiziționarea de licențe recurente în stilul abonamentelor lunare/anuale etc.

Licențele cloud acoperă de fapt soluții all-in-one, care includ următoarele componente şi funcționalități/servicii:

- Software-ul de management video (VMS)
- Stocare și arhivare în cloud

- Stocare locală pe cameră
- Acces la server-ul din cloud
- Actualizări automate
- Interacțiunile cu toți utilizatorii sistemului
- Funcții și analize avansate.

2.4 Funcții și analize avansate implementate în componenta software VMS a sistemului de supraveghere bazat pe cloud

Aceste funcții şi analize avansate valorifică de fapt puterea de procesare a infrastructurii cloud (*cloud computing*) care permite analiza unor cantități masive de videoclipuri fără nici un efort suplimentar din partea utilizatorului, permițând inclusiv navigarea rapidă în seturile de imagini, cât și primirea de alerte proactive în timp real.
Cu platforma cloud unificată la nivel urban, este simplu ca toate aceste funcții să fie utilizate la scară în mai multe locații simultan - de exemplu, se pot căuta imagini din proximitatea mai multor şcoli simultan, deci în același timp.

Caracteristicile avansate ale sistemului includ următoarele:

- Acces nativ de la distanță: accesul de la distanță este piatra de temelie a oricărui sistem de supraveghere în cloud, în sensul că se pot vizualiza filmările și poate fi folosit întregul sistem, de oriunde în lume, conferindu-se în acest mod un confort sporit în utilizarea lui, operațiuni mai fluide, flexibilitate şi economie de timp.

- Căutare inteligentă pentru investigații rapide, folosindu-se instrumente îmbunătățite de Inteligență Artificială pentru a naviga cu ușurință în fluxurile video și pentru a găsi rapid ceea ce se caută.

- Partajare ușoară a fluxurilor live și a clipurilor: cu accesul de la distanță bazat pe cloud, se pot partaja cu ușurință înregistrările de la distanță prin metode precum URL, SMS și e-mail.

- Analizele AI fac posibile căutările în toate camerele și locațiile folosind recunoașterea facială, recunoașterea vehiculelor și a plăcuțelor de înmatriculare, căutarea culorilor, numărarea persoanelor, detectarea zgomotului, analiza audio, detectarea comportamentului neobișnuit și multe altele.

- Actualizări automate: conectivitatea în cloud permite furnizorilor de soft-uri VMS să lanseze automat noi funcții și actualizări de securitate, făcând ca întreținerea

sistemului şi upgrade-urile acestuia să se efectueze fără efort şi fără lacune în securitatea cibernetică.

- Alerte în timp real pe orice dispozitiv, personalizabile în manieră dinamică.

- Aplicații mobile: contextul cloud permite accesarea de la distanță a sistemului de oriunde în lume, prin intermediul aplicațiilor mobile.

- Permisiuni de utilizare flexibile: software-ul cloud VMS permite setarea permisiunilor de utilizator personalizate, granulare, care corespund nevoilor unice ale fiecărei unități şcolare.

B. Utilizarea sistemelor de supraveghere video în şcolile din Municipiul Bistrița

La nivel mondial, multe școli ale lumii civilizate folosesc supravegherea video ca metodă de securitate. Spre exemplu, în America, camerele de securitate au fost folosite în 91% din școlile publice în 2019-2020. În comparație cu alte măsuri de siguranță a școlii, în școlile din America (spre exemplu) supravegherea video este a doua cea mai comună măsură de securitate în campus, după accesul controlat la clădiri.

In ceea ce priveşte tipurile de camere de luat vederi care sunt cel mai des utilizate, acestea pot fi:

• Camerele de supraveghere „Bullet School” care au o carcasă durabilă având formă de butoi

• Camere de supraveghere cu dom pentru școli, cu carcasă în formă de cupolă, care este mai discretă decât cea de tip „Bullet School”

• Camerele de supraveghere PTZ pentru școli, care se pot deplasa și înclina pentru a schimba locul/zona spre care este orientată camera, cu sirena, vedere color noaptea, posibilitate de rotire 360 gr.

• Camerele de securitate pentru școli de tip „Fisheye”, anume camere tip cupolă care captează imagini la 360° și oferă cea mai mare acoperire posibilă.

Planul de implementare

Planul de implementare cuprinde:

- Modelarea, proiectarea şi implementarea componentelor resursei de date, după cum urmează:

- Bazele de date video preluate de la fiecare unitate educaționala a Municipiului Bistrița, amplasate în Componenta Educațională a Centrului de Date.

- Depozite de Date video (DataWarehouse) şi componentele DataMart aferente – pentru stocarea datelor pe lungă durată în vederea aplicării mecanismelor de Inteligența Artificială pentru generarea rezultatelor pe termen lung.

- Identificarea setului exhaustiv de cazuri de utilizare ale platformei, care vor sta la baza proiectării şi implementării funcționalităților sistemului

- Definirea, proiectarea şi implementarea Interfețelor Utilizator cu capabilități avansate de interacțiune implementate cu tehnologii GUI bazată pe biblioteci de shape-uri grafice.

- Definirea, proiectarea şi implementarea componentelor de interfațare şi interoperabilitate cu celelalte sisteme/subsisteme ale contextului integrat de digitalizare a proceselor specifice ecosistemului IT al Mun Bistrița, cu găzduire pe infrastructura de cloud urban prezentată/recomandată în cadrul secțiunii referitoare la infrastructura hardware a Oraşului Inteligent Bistrița.

- Definirea, proiectarea şi implementarea funcționalităților bazate pe Inteligența Artificială, precum recunoaşterea de fețe, recunoaşterea numerelor de înmatriculare ale maşinilor, sesizarea situațiilor de agresiune bazată pe recunoaşterea unor şabloane comportamentale şi alarmarea automată necesară în astfel de situații.

Sustenabilitate şi impact

Privitor la elementele pe care se bazează sustenabilitatea, sistemele de supraveghere video care sunt necesare a fi instalate în toate unitățile educaționale ale Municipiului Bistrița prezintă următoarele garanții:

1. Gradul în care sunt capabile a furniza cunoştințe/cunoaştere privitoare la siguranța şcolară în mod continuu, este asigurat prin caracteristicile funcționale specifice ale sistemelor de supraveghere video conectate în cloud, care transmit date video zilnic, fără întrerupere, timp de 24 ore din 24.

2. Gradul în care aceste sisteme sunt adaptabile se bazează pe structura modulară a acestora, atât sub aspectul componentelor hardware cât şi a celor software.

3. Gradul de „offloading”, se referă la capabilitatea componentelor software bazate pe tehnologii AI, fie de a-şi autocorecta erorile sau neconcordanțele care pot să apară pe parcursul versionărilor succesiv evolutive, fie aceea de a permite efectuarea acestor corecții din mers, prin intervenția directă a specialiştilor IT, fără a fi nevoie de reimplementarea totală a sistemului.

In toate aceste trei sensuri, sustenabilitatea sistemelor de supraveghere video a unităților şcolare din oraşul Bistrița este conferită prin însăşi natura arhitecturii cloud a infrastructurii hardware pe care urmează a fi găzduite, dar şi prin intermediul componentelor structurale ale sistemului.

Impactul asupra dezvoltării comunității urbane Bistrița al sistemelor de supraveghere video a unităților educaționale din Municipiul Bistrița, este acela de a se putea monitoriza în permanență nivelul de siguranță atât pentru elevi cât şi pentru cadrele didactice, cu posibilitate de intervenție rapidă în cazurile de periculozitate, avându-se în vedere faptul că vor fi conectați în mod direct la sistem inclusiv reprezentanții şi angajații Poliției Locale, aceştia putând interveni, ca atare, cu maximă promptitudine în cazul semnalării de către sistem a oricărui tip de situație de periculozitate.

ANEXE

1. Dispecerat de supraveghere video centralizat la nivel urban, pe baza datelor video transmise direct în cloud:

2. Replică locala: dispecerat local pentru supravegere video a tuturor intrărilor şi zonelor de proximitate ale unității educaționale:

FIȘA DE PROIECT FANION

Titlu

“Digitalizarea planificării și aprobării bugetului, referatelor de necesitate și planului anual al achizițiilor publice”

Coordonator din partea consultantului:

Daniel HOMORODEAN

Context şi obiective

Prioritatea ridicată a acestui proiect pentru Primăria Municipiului Bistrița a fost evidențiată în cursul procesului de audit, prin analiza proceselor și schimburilor de informații din cadrul compartimentele instituției și între acestea. În mod particular au contribuit la identificarea necesității și definirea soluției analizele și discuțiile cu personalul structurilor Direcția economică, Serviciul Achiziții publice, Serviciul Audit intern. Implementarea proiectului are impact asupra întregii structuri organizatorice a instituției și este recomandabil să includă de asemenea și instituțiile subordonate, inclusiv cele care au personalitate juridică.

Implementarea proiectului în forma definită în continuare determină îmbunătățiri ale eficienței activității și reducerea riscurilor asociate unui număr mare de procese din cadrul Primăriei Municipiului Bistrita, printre cele mai importante fiind următoarele:

- Realizarea planificării bugetului pentru anul viitor prin colectarea necesităților și previziunilor de la nivelul fiecărui compartiment în parte
- Definirea necesităților care stau la baza achizitiilor care vor fi derulate în viitor, sub forma de referate de necesitate și specificații asociate
- Aprobarea și avizarea solicitărilor colectate din structura instituției, din perspectiva oportunității și din perspectiva disponibilități financiare
- Planificarea și urmărirea planificării realizării achizițiilor și implementării procedurilor competitive de achiziție publică, sub forma planului anual al achizițiilor publice, respectiv planuri de achiziții aferente proiectelor finanțate derulate, folosite ca instrumente manageriale și de suport în luarea deciziei
- Urmărirea relației cu furnizorii prin gestiunea contractelor și acordurilor cadru din perspectiva cantitativă și valorică, emiterea și urmarirea livrării comenzilor către furnizori și evidențierea în relație cu planul de achiziții a tuturor achizitiilor efectuate
- Realizarea proceselor de audit intern care implică verificarea și analiza informațiilor legate de activitățile derulate pentru realizarea achizițiilor publice în toate etapele acestora, de la aprobare, planificare, până la execuție, livrare și recepție.

Structurile interne cu cel mai ridicat grad de implicare în derularea și utilizarea acestui proiect sunt:

- Direcția economică, în special pentru planificarea bugetului
- Serviciul Achiziții publice, pentru planificarea și execuția achizițiilor, atât cumpărăturile directe cât și procedurile competitive implementate
- Serviciul Audit intern, pentru realizarea activităților de audit
- Serviciul implementare proiecte

Printre beneficiile așteptate în urma implementării proiectului avem în vedere următoarele:

- Îmbunătățirea semnificativă a comunicării între compartimente și între managerii acestora și structurile superioare de management și decizie implicate în aprobarea și avizarea planului de buget
- Îmbunătățirea capacității de prognoză și planificare la nivel managerial a necesităților bugetare prin posibilitatea analizei eficiente și rapide a datelor istorice și a corelațiilor dintre planificare și execuția efectivă din ciclurile financiare anterioare
- Asigurarea trasabilitatii și auditabilitatii schimbului de informații legat de planificarea bugetara, incluzând cine/ce/când a realizat fiecare propunere sau solicitare, cum a fost realizată analiza și aprobarea acesteia, în cât timp și cu ce rezoluție
- Asigurarea digitalizării întregului ciclu de viață (“end-to-end”) a activităților de planificare bugetară și execuție a achizițiilor publice, inclusiv cu posibilitatea generării automate a documentelor tipizate, posibilitatea semnării electronice și eliminarea sau reducerea necesității utilizării suportului hârtie
- Asigurarea standardizării modului în care sunt formulate solicitările din cadrul compartimentelor, în mod particular pentru produse și servicii, pentru a se asigura posibilitatea de aprobare rapidă, corelare și comasare a achizițiilor de produse sau servicii identice sau similare, asigurarea unor caracteristici tehnice comune și unitare a produselor achiziționate, cu impact inclusiv în efortul și costul de întreținere și înlocuire, pe tot ciclul de viață a produselor și serviciilor achiziționate
- Asigurarea posibilității de predicție valorică și de utilizare a costurilor obținute anterior pentru anumite produse sau servicii ca bază de estimare pentru planificare, inclusiv reducerea efortului și lipsei de acuratețe a estimărilor valorice care trebuie făcute la nivelul compartimentelor înainte de transmiterea propunerilor spre aprobare
- Reducerea timpilor necesari pentru analiza și aprobarea cererilor de includere în buget și a referatelor de necesitate, standardizarea acestor cereri și asigurarea completitudinii lor, scăderea numărului de corecturi și de reluări a procesului de aprobare datorită corecturilor sau adăugirilor necesare
- Asigurarea managementului unitar al planurilor de achiziție (planul anual al achizițiilor publice și planurile de achiziție aferente fiecărui proiect), asigurarea posibilității de lucru colaborativ pentru consultarea și actualizarea planurilor, asigurarea posibilității de a corela fiecare element planificat (poziție din plan, articol din cererea de alocare bugetară sau referat de necesitate) cu solicitarea și respectiv cu furnizarea, evidențiind diferențele între valorile estimate și valorile realizate, inclusiv per total valoarea economiilor realizate până la momentul respectiv că diferență între totalul estimat cumulat pe pozițiile planificate și executate și totalul valoric al achizițiilor aferente efectiv realizate. Aceasta vizibilitate asupra economiilor realizate duce la posibilitatea de realocare și replanificare ușoară în cursul exercițiului financiar a diferențelor economisite
- Asigurarea capacității de raportare în relație cu auditul intern și cu organismele de audit extern (Curtea de conturi, autorități de management pentru proiectele finanțate din fonduri Europene), prin posibilitatea generării de rapoarte și exportului de rapoarte în diverse formate, inclusiv procesabile direct informatic, pe bază de filtrări, selecții, căutări

în funcție de diverse criterii a elementelor planificate sau a celor executate/achiziționate din buget și din planul achizitiilor publice, atât cel anual cât și cele aferente proiectelor

- Posibilitatea introducerii de condiții, verificări, notificări și alterte în relație cu valori și termene calendaristice legate de planificarea și execuția achizițiilor, inclusiv praguri ale cumulului valoric aferent achizițiilor directe grupate în funcție de necesitate sau în funcție de similaritate (cod și grupă de coduri CPV), apropierea sau depășirea unor termene aferente calendarului de derulare a unor proceduri competitive de achiziție publică, apropierea termenelor calendaristice de expirare a contractelor cadru sau termenelor de eliberare a garanțiilor, etc
- Asigurarea implicită a respectării formatelor documentare, inclusiv a informațiilor minime necesare, pentru documentele generate în procesele de planificare bugetară și de achiziții publice
- Posibilitatea accesării de la distanță, prin internet, a informațiilor legate de planificarea bugetară și de achiziții, realizarea de la distanța a tuturor operațiunilor aferente, inclusiv completarea de solicitări, aprobare (cu posibilitatea de semnare electronică), planificare, raportare, comunicare cu furnizorii
- Reducerea semnificativa a riscurilor de corecție financiara aferente derulării unor proceduri de achiziție publică generate de depășirea unor termene calendaristice impuse de lege sau de depășirea pragurilor valorice prin cumularea de articole similare sau pentru aceeași necesitate, în cursul ciclului financiar sau în cadrul unui proiect
- Reducerea deosebit de substanțială a timpului necesar derulării proiectelor de audit intern asupra activităților legate de planificarea bugetară și de planificarea și execuția achizițiilor publice, creșterea eficientei generării rapoartelor de audit și a planurilor de remediere, urmărirea ușoară a implementării corecțiilor necesare
- Asigurarea capacității de control asupra planificării și stării execuției bugetare și realizării achizițiilor publice la nivelul subordonatelor, în cazul în care se va implementa posibilitatea recomandată de urmărire de la nivelul central al Primăriei Municipiului Bistrița a activității la nivelul subordonatelor prin mijloace informatice în timp real

Proiectul propus are că și componenta principala implementarea unui sistem informatic. Datorită impactului semnificativ pentru fluxurile de activitate din cadrul instituției și a implicării unei părți mari a personalului în utilizarea acestuia, proiectul implica și o componenta de educație și suport a personalului în vederea eficientizării adopției și ușurării transpunerii informațiilor din alte forme (informatice sau letrice) în cadrul sistemului.

Elementele funcționale principale ale proiectului sunt următoarele:

- Planificarea bugetară. Realizarea solicitărilor de alocare de bugete din partea compartimentelor
- Aprobarea solicitărilor și consolidarea planului bugetar
- Generarea referatelor de necesitate

- Gestiunea planului anual al achizițiilor publice. Gestiunea planurilor de achiziție pentru fiecare proiect finanțat.
- Gestiunea calendarelor de derulare a procedurilor competitive
- Gestiunea furnizorilor, contractelor, acordurilor cadru, comenzilor către furnizori, garanțiilor
- Generarea strategiilor de achiziție publica aferente procedurilor competitive planificate

Pentru fiecare dintre aceste etape detaliem principiile funcționale, pe baza cărora se poate construi specificația funcțională detaliata care va sta la baza abordării alese pentru implementare, fie printr-o achiziție de produs software care să corespundă cerințelor, fie de servicii de dezvoltare și configurare corespunzătoare.

Planificarea bugetară

Realizarea solicitărilor de alocare de bugete din partea compartimentelor și aprobarea acestora.

Prin aceasta funcționalitate se vă urmări standardizarea modului în care conducătorii departamentelor din cadrul instituției realizează și transmit solicitările pentru alocarea bugetului, indicând necesitățile și după caz valorile aferente prevăzute.

Colectarea și completarea acestor informații la nivelul compartimentului trebuie realizată pe baza unui formular tipizat în formă electronică disponibil online prin intermediul aplicației, care după completare să fie transmis spre aprobare urmând un flux de aprobare explicit definit în cadrul sistemului. Acest flux de aprobare trebuie să fie cunoscut și vizibil conducătorilor de compartiment așa încât să poată să prevadă cine trebuie să aprobe solicitarea și în ce ordine trebuie obținute aceste aprobări. Dat fiind că aprobările se vor da secvențial, se va putea urmări cine a aprobat și când, respectiv la cine a ajuns la aprobare și de când este în așteptare. Vizibilitatea statusului aprobării poate să fie disponibilă unor anumiți utilizatori selectați (cum ar fi managementul instituției, serviciul de audit intern) sau chiar și conducătorilor de compartiment care au înaintat solicitarea. Aceasta vizibilitate explicită are rolul de a conduce la o viteza mai mare în derularea procesului de analiză și aprobare, deci o scădere a timpului total necesar acestor operațiuni.

În funcție de caz, dacă justificările, explicațiile sau specificațiile aferente necesităților prevăzute și sumelor solicitate nu sunt suficiente pentru a sprijini luarea unei decizii favorabile, fie din perspectiva oportunității, fie din perspectiva disponibilității financiare sau a unor elemente tehnice în lipsa cărora acuratețea estimării financiare poate fi incertă, fiecare dintre persoanele care se afla pe lanțul de aprobare vor putea să respingă solicitarea pe baza de argumente care trebuie consemnate în sistem, aceasta respingere transmițând solicitarea înapoi la seful departamentului pentru realizarea clarificărilor, corecțiilor sau completaților necesare, după caz, și retransmiterea solicitării pe lanțul de aprobare.

Acest proces de solicitare și oferire de clarificări conduce la o îmbunătățire a comunicării în cadrul instituției în relație cu planificarea bugetului, asigurarea unui nivel ridicat de responsabilitate a celor care transmit solicitări deoarece orice lipsa (de justificare, de detaliere suficienta) duce la reluarea ciclului de aprobare și o prelungire a întregului proces, acest lucru fiind consemnat de către sistemul informatic.

Generarea și aprobarea referatelor de necesitate

Referatele de necesitate, care stau la baza constituirii planului anual al achizițiilor publice, pot să fie realizate, aprobate și consolidate în plan în ultimul trimestru al anului anterior pentru anul în curs (conform cu cerințele normative curente la nivel național), dar în practica se întâmplă frecvent ca acestea să fie completate, transmise și planificate în cursul anului ca urmare a identificării unor necesități suplimentare sau a unor evenimente neprevăzute. Indiferent de momentul la care acestea sunt completate, procesul de creare, transmisie și aprobare trebuie să fie trasabil, auditabil, standardizat și complet electronic, pentru a elimina riscurile de blocaje pe lanțul de aprobare și a întârzierilor aferente, riscul de pierdere efectivă care apare atunci când referatele sunt transmise în format letric, riscul de planificare a unor achiziții pentru care serviciul de achiziții să nu aibă suficiente informații pentru a putea realiza în mod eficient achiziția sau după că a derula procedura competitiva aferentă.Tot acest flux de lucru trebuie realizat în mod complet și exclusiv electronic, ideal cu incorporarea directă a posibilității de semnare electronică.

Gestiunea planului anual al achizițiilor publice, și în același mod a planurilor de achiziții asociate fiecărui proiect finantat pentru care se impune o gestiune proprie, este instrumentul managerial esențial pentru controlul, urmărirea și verificarea tuturor elementelor legate de planificarea și execuția achizițiilor, realizarea de rapoarte, analize și asigurarea suportului pentru luarea deciziilor, cum ar fi cele de realocare a unor sume ca urmare a realizării unor economii în cursul anului, prin diferențele între valorile estimate și valorile realizate.
Planul anual al achizițiilor publice trebuie să fie implementat pe baza unei componente informatice integrate în sistem, care să permită accesul direct la elementele de planificare pentru toate persoanele care au acest drept, pe deoparte pentru toți cei care la nivelul serviciului de specialitate trebuie să actualizeze planul, pe de alta pentru cei care au interesul să urmărească și să verifice realizarea lui (persoane din cadrul managementului instituției, fără posibilitatea de a realiza modificări) și să auditeze activitățile aferente (serviciul de audit intern, care să poată realiza căutări, sortări, filtrări pentru a obține rapoartele și alte informații, fără a putea modifica efectiv conținutul planului).

Pentru fiecare poziție din plan și fiecare articol din cadrul respectivei poziții trebuie să poată fi corelată și urmărită realizarea efectiva a achizitiilor, detaliilor legate de furnizare sau prestarea de servicii în funcție de caz, inclusiv cu elementele cantitative și valorice aferente, respectiv stadiul de derulare a procedurilor competitive asociate fiecărei poziții, inclusiv pe fiecare lot în

parte, daca este cazul. În acest fel fiecare poziție din PAAP va conține în mod complet întregul istoric al operațiunilor corelate, de la ce s-a planificat și aprobat, până la ce s-a achiziționat efectiv, de la ce furnizor, ce contracte sau acorduri cadru s-au realizat, care sunt diferențele de sume între ce s-a planificat și ce s-a realizat. Prin digitizarea și accesibilizarea informațiilor conținute în planul anual al achizițiilor poate fi asigurată posibilitatea urmăririi și auditării execuției achizițiilor în timp real pentru toate instituțiile subordonate. Aceasta vizibilitate trebuie să fie asigurata cel puțin pentru personalul serviciului de audit intern, dar impactul benefic cel mai semnificativ e asigurat atunci când disponibilitatea pentru vizualizare este dată și managementului superior din cadrul Primăriei Municipiului Bistrița. Pentru a reduce riscurile de reticență din partea instituțiilor subordonate, trebuie asumat în mod explicit la nivelul instituției că această vizibilitate are rolul de a eficientiza și sprijini activitățile subordonatelor, nu doar de a adaugă încă un nivel de control.

Gestiunea calendarelor de derulare a procedurilor competitive reprezintă un element important pentru asigurarea respectării normelor legale și eliminarea riscurilor de corecție induse de nerespectarea termenelor impuse de cadrul de reglementare. Pentru a se asigura respectarea tuturor termenelor calendaristice, în funcție de tipul de procedură ales, sistemul va trebui să poată realiza automat calcularea următorului termen calendaristic ținând cont de numărul de zile după caz calendaristice sau lucrătoare și indicând printr-un sistem de notificări și alerte apropierea și respectiv atingerea termenelor respective.

Gestiunea contractelor, acordurilor cadru, garanțiilor de bună execuție necesită o abordare specifică, pe care nu o putem regăsi într-un sistem de management a documentelor deoarece implică gestiunea din perspectiva cantitativă și valorică, respectiv calendaristică, a relației contractuale între instituție ca beneficiar și furnizorul căruia i s-a atribuit contractul și care și-a asumat obligația livrărilor sau prestărilor aferente.

Fiecare contract în derulare trebuie să fie gestionat astfel încât să permită evidențierea fiecărei livrări (cantitate, valoare, comandă aferentă, stare livrare, alte documente însoțitoare după caz), să permită vizualizarea diferenței între cantitățile și valorile consumate (livrate) și cele care rămân în continuare disponibile, să permită notificări sau alerte în cazul apropierii, atingerii sau depășirii termenelor de valabilitate a contractelor, respectiv notificări și alerte care să permită instituției să gestioneze ușor perioada de valabilitate a garanțiilor de bună execuție constituite, forma prin care au fost constituite și dacă e cazul să consemneze eliberarea garanțiilor constituite.

Sistemul implementat trebuie să respecte în mod obligatoriu cel puțin următoarele caracteristici care țin de posibilitățile pe care instituția le va dobândi pentru a exploata sistemul și a dispune de datele generate și utilizate în sistem, pe întregul sau ciclu de viață. Aceste elemente minime trebuie în mod obligatoriu să se regăsească în documentația aferentă procedurii de achiziție a sistemului sau a serviciilor de dezvoltare prin care acesta va fi realizat, respectiv a contractului între Primăria Municipiului Bistrița și furnizorul sistemului

Astfel, sistemul informatic trebuie sa fie

- Extensibil, permițând adăugarea de funcționalități suplimentare și extinderea celor deja implementate. Trebuie avut în vedere în mod special posibilitatea de a putea dezvolta rapoarte sau analize.
- Complet auditabil, așa încât utilizatorii cu roluri specifice de audit să poată vedea toate detaliile legate de activitățile tuturor utilizatorilor din sistem, adică în mod complet cine/ce/când a realizat, incluzând operațiuni de introducere de informații sau modificare a acestora
- Interfațabil, sau integrabil, însemnând că sistemul trebuie să poată fi integrat informatic în mod direct cu alte sisteme informatice existente sau viitoare operate de către instituție. Printre cele care trebuie avute în vedere în mod explicit se numără sistemele prin care se gestionează documentele, planificarea și execuția bugetară, magazia și inventarul, contabilitatea
- Toate informațiile structurate și toate documentele generate prin utilizarea sistemului trebuie să poată fi exportabile în mod direct și fără intervenția furnizorului sistemului în formate care să poată fi vizualizate și procesate fără necesitatea unor aplicații informatice specializate. Pentru orice tip de informații structurate, cel puțin una din formele de export disponibile să fie CSV (Excel), cel puțin pentru planul anual al achizițiilor publice și planurile achizițiilor per proiect finanțat, achizițiile realizare, rapoartele.

Utilizarea semnaturii electronice în derularea activităților reflectate în sistemul informatic este importantă și de natură să îmbunătățească semnificativ eficiența sistemului și să reducă în mod major necesitatea realizării unor acțiuni suplimentare de procesare în format letric, deci în forma fizică, tiparite, a unor documente care deja există în forma digitală fiind generate de aplicații. Modul optim de lucru este prin folosirea semnării la distanță pe baza de certificate stocate pe serverul furnizorului de servicii de încredere (furnizorul de certificate calificate pentru semnătură electronică), astfel încât documentele să nu mai fie nevoie să fie descărcate, semnate electronic și reîncărcate în sistem, ci direct semnate printr-o acțiune asumată explicit și autorizata pe baza unui token mobil.

Etapele implementării proiectului

Dat fiind că proiectul implică mai multe compartimente din cadrul instituției, este necesar ca acestea să fie corespunzător implicate și coordonate în toate fazele implementării proiectului, pentru a se asigura o implementare optimă, o adoptie si introducere in utilizare eficiente si fără frictiuni sau reticențe din partea unor compartimente sau persoane, și o utilizare corespunzătoare în mod constant.

Aceste etape sunt:

- Detalierea specificatiilor funcționale și tehnice pentru pregatirea caietului de sarcini care stă la baza implementării procedurii aferente achiziției platformei informatice sau serviciilor de dezvoltare a acesteia
- Derularea procedurii de achiziție pentru alegerea furnizorului platformei informatice
- Instruirea utilizatorilor platformei, incluzând toate tipurile de utilizatori: conducătorii compartimentelor (care transmit solicitările), managementul instituțional (care realizează funcția de aprobare), personalul serviciilor de specialitate de achiziție publica și audit intern
- Introducere în utilizare a platformei, cu supravegherea directă și suport constant oferit utilizatorilor pentru o cât mai eficienta adaptare la specificul noului mod de lucru

Trebuie avut în vedere că o astfel de platforma necesită mentenanță continuă, inclusiv modificări tehnice atunci când este necesar (de exemplu atunci când apar modificări în cadrul de reglementare la nivel național) și când este oportun inclusiv pentru interfațarea sistemului cu alte aplicații informatice care vor fi implementate în viitor în cadrul instituției.

Costurile implementării și mentenanței proiectului

Estimam costurile de implementare la 500,000 RON. Consideram oportună o bugetare anuala a activitatilor de modificare, extindere și interfatare la nivelul a 80,000 RON.

Durata de implementare pentru un astfel de proiect ar fi de aproximativ 6 luni, perioada care se poate scurta în cazul implementării unui produs deja existent în piața care trebuie configurat și integrat cu sistemele informatice ale instituției. Trebuie avuta în vedere necesitatea unei perioade de învățare și acomodare a personalului cu noul sistem, de circa o lună, care ar trebui sprijinită prin sesiuni formale de training realizate de către furnizor.

Riscuri aferente implementării proiectului

Risc: Reticența personalului de a utiliza sistemul.Reticența unei părți a personalului este riscul cel mai semnificativ și cu impactul cel mai mare. Dat fiind că implementarea unui astfel de sistem implică o schimbare a modului de lucru de la forma tradițională, bazată pe documente letrice, completate și transmise fizic și semnate olograf, la o abordare digitala, inclusiv eventual cu semnare electronică, există riscul ca unii membri ai personalului să refuze utilizarea sistemului sau să nu îl utilizeze în mod disciplinat și responsabil, să nu realizeze activitățile care le sunt asignate prin sistem sau să se autentifice cu mare întârziere. Beneficiile implementării proiectului sunt obținute atunci când toți utilizatorii lui, în particular conducătorii departamentelor, managementul superior al instituției și angajații serviciului de specialitate (achiziții publice) îl folosesc în mod consecvent. Altfel, există riscul ca fluxurile de lucru să se blocheze, în fazele de aprobare sau de planificare.

Reducerea riscului: Conducerea instituției trebuie să dea un mesaj ferm și consistent de susținere a utilizării sistemului, inclusiv probând prin propriul exemplu importanța pe care o acordă

introducerii și utilizării lui. Procedurile interne de lucru trebuie actualizate cu mențiunea obligației utilizării sistemului informatic pentru realizarea unor activități specifice cum ar fi de exemplu transmiterea cererilor de planificare bugetară dinspre departamente, transmiterea referatelor de necesitate, consemnarea achizițiilor efectuate. Personalul trebuie instruit înainte de introducerea în producție a sistemului și tuturor utilizatorilor trebuie să li se acorde suportul necesar, care pentru unele persoane poate fi mai semnificativ, pentru a trece peste reticența la schimbare și dificultatea de adaptare la o nouă formă de lucru.

Risc: Indisponibilitatea îndelungată a unui utilizator cu sarcini esențiale în sistem.Fluxurile de lucru configurate în sistem pot fi dependente de anumiți utilizatori nominali, de exemplu personal din cadrul managementului în cursul procesului de aprobare a unei cereri de planificare buget, a unui referat de necesitate, sau șeful serviciului achiziții. Reducerea riscului: Fiecare utilizator să poată fi înlocuibil prin configurarea sistemului astfel încât atunci când o persoana devine indisponibila din orice motiv pentru o perioada funcția specifică utilizatorului (de aprobare, de planificare) să poată fi delegata altui utilizator, care îi preia rolul în cadrul fluxurilor de lucru.

Sustenabilitate și impact

Sistemul informatic pentru planificarea bugetului și gestiunea achizițiilor publice este de natură să determine un impact pozitiv semnificativ în instituție, prin creșterea eficienței comunicării interne, creșterea nivelului de responsabilitate a personalului implicat, scăderea timpilor de lucru și de așteptare, creșterea nivelului de control, scăderea riscurilor de corecție sau de cheltuire ineficientă a sumelor disponibile și îmbunătățirea majoră a procesului de audit intern.

Asigurarea impactului pozitiv depinde în mod esențial de semnalul hotărât și consecvent pe care îl dă conducerea instituției privind necesitatea și oportunitatea utilizării sistemului pentru toate operațiunile pentru care suportul informatic vă fi implementat, astfel încât să nu existe o dublare a activităților în alte forme (pe suport hârtie) sau în alte sisteme, fie complexe fie de tip Excel sau Word.

Anumite elemente care țin de modul în care este folosit sistemul, inclusiv de nivelul de cuprindere a sistemului în contextul instituțional local, pot extinde în mod semnificativ impactul pozitiv pe care acesta îl aduce.

Aceste elemente sunt

- Extinderea utilizării sistemului în cadrul și în relație cu toate instituțiile subordonate, cu asigurarea posibilității de auditare completa de către utilizatorii autorizați
- Introducerea în mod explicit a sistemului informatic că suport în procesele de audit intern

- Implementarea completă a semnăturilor electronice la distanța prin utilizarea certificatelor calificate stocate la nivel de server
- Folosirea PAAP că instrument managerial prin consemnarea în mod consecvent și completă a tuturor achizițiilor realizate în relație cu pozițiile planificate

Efectele benefice ale utilizării sistemului sunt cumulative în timp. Inerent în prima fază de după introducerea sistemului în utilizare, instruirea utilizatorilor și popularea cu date a sistemului, unii membri ai personalului ar putea resimți o creștere a presiunii de învățare și adaptare, dar după aceasta prima etapă utilizarea consecventă a sistemului vă duce la regăsirea și reutilizarea mult mai rapidă a informației, analize și raportări rapide și eficiente, decizii corecte bazate pe informații la zi și per ansamblu riscuri mai mici și un confort mai bun pentru întregul personal din cadrul instituției.

FISA DE PROIECT FANION

Titlu

Transformarea digitală în Primăria Bistrița

Coordonator din partea consultantului

Stelian Brad

Transformarea digitală

Transformarea digitală a unei primării se referă la utilizarea tehnologiilor digitale și a datelor pentru a îmbunătăți modul în care instituția publică livrează valoare publică cetățenilor și comunității locale. Această transformare implică implementarea de soluții tehnologice și digitale care să sprijine procesele interne ale primăriei, să optimizeze interacțiunea cu cetățenii și să îmbunătățească livrarea serviciilor publice.

De exemplu, o primărie poate implementa soluții digitale pentru a îmbunătăți procesele interne de gestionare a datelor și documentelor, pentru a simplifica și accelera procedurile de aplicare și eliberare a certificatelor și actelor necesare cetățenilor, pentru a facilita comunicarea și interacțiunea online cu cetățenii, pentru a dezvolta platforme de participare civică și consultare online sau pentru a implementa soluții de monitorizare a infrastructurii și serviciilor publice, astfel încât să poată fi identificate și remediate rapid eventualele probleme. Toate acestea conduc la îmbunătățirea calității și eficienței serviciilor publice, precum și la creșterea satisfacției și încrederii cetățenilor în instituția publică.

Astfel, transformarea digitală a unei primării presupune utilizarea tehnologiei și a inovațiilor digitale pentru a îmbunătăți serviciile publice oferite cetățenilor, pentru a crește eficiența și transparența administrației și pentru a stimula dezvoltarea economică și socială a comunității locale.

Transformarea digitala nu este posibila inainte de maturizarea procesului de digitalizare, de crestere a capacitatii de securitate cibernetica, si de implementare a unui sistem de management al digitalizarii.

Transformarea digitală se aplică pentru a crea valoare publică. Valoarea publică se referă la valoarea creată de administratia locala prin servicii, hotarari, reglementări și alte acțiuni subsumate strategiei de dezvoltare locala. Este realizata de catre functionarii publici care navighează cu succes într-un spatiu strategic ce are ca finalitate producerea unui impact cu valoare adaugata pentru comunitate, in limitele resurselor și capacității disponibile, intr-un mediu autorizat de jurisdictie formala si informala, intr-un mandat legal si un cadru legal.

Dimensiunile valorii publice:

1. Satisfacția comunitatii locale
2. Valoare economică – generarea de activitate economică si locuri de munca in comunitate
3. Valoare socială și culturală – dezvoltarea capitalului social si a coeziunii intre categoriile sociale si profesionale
4. Valoare politică - dialog democratic si participare publică
5. Valoare ecologică - dezvoltare durabilă, reducerea poluării, reciclarea deșeurilor, actiuni in intampinarea efectelor încălzirii globale
6. Prestarea serviciului - preluare, satisfacție, alegere, corectitudine, cost, calitatea serviciilor
7. Performanță financiară - venituri, valoarea pentru banii publici cheltuiti, eficiență
8. Performanță nefinanciară - eficiență, satisfacția tuturor actorilor implicati
9. Valoare socială din perspectiva utilizatorului, valoare economică tangibilă din perspectiva administrației, valoare economică necorporală din perspectiva administrației
10. Încredere și legitimitate
11. Protejarea drepturilor cetățenilor

Inovatiile digitale trebuie subordonate generarii de valoare publica. Inovatiile digitale au 3 dimensiuni – toate sunt necesare.

Digitizarea este procesul de conversie a informațiilor care există la un moment în format fizic de tip analogic într-un format digital, având ca rezultat reprezentarea unui obiect fizic, imagine, sunet, document sau semnal audio sau video de tip analogic într-o formă digitală.

Exemple:

- Digitizarea arhivei si arhivarea electronica a documentelor
- Digitizarea automata a minutelor sedintelor de lucru
- Digitizarea documentelor fizice primite la registratura
- MS Office si orice aplicatii care conduc la introducerea datelor manual

Digitalizarea este procesul de utilizare a tehnologiei digitale pentru a colecta date din procese organizaționale și de a derula activități cu ajutorul tehnologiei digitale în vederea creșterii performanțelor referitoare la eficienta, calitate, trasabilitate, responsivitate, etc. și în vederea vizualizării și înțelegerii mai bune a modului în care se derulează diversele procese in cadrul organizatiei. Digitizarea este parte a digitalizării.

Exemple:

- Platforma de management integrat a proiectelor de investitii
- Platforma de management intern al documentelor
- Platforma pentru achizitii publice

Transformarea digitală este procesul de transformare structurală a unei organizații și de redefinire semnificativă a strategiei sale prin adopția pe scară largă a digitalizării la nivelul organizației într-o formă în care tehnologia digitală nu este văzută ca o funcție suport, ci ca o competență strategică, în care cultura organizațională este condusă de digitalizare și modelul de relaționare cu beneficiarii este unul nou, bazat pe digitalizare în fundamentarea valorii publice și în asigurarea unei calități ridicate.

Exemple:

- Operarea in cloud a tuturor aplicatiilor si aplicarea conceptului de institutie “paperless”, flexibilizarea muncii si tele-muncii
- Utilizarea asistentilor virtuali si platformelor online mobile de relatii, cu functii de trasabilitate si semnaturi digitale pentru asigurarea serviciilor catre cetatean 24/7
- Aplicarea conceptului “once-only” in relatia cu cetateanul
- Colectare, management, analiza volume mari de date si informatii cu IA, IoT, sisteme expert pentru optimizare alocare si distributie bugetara
- Adoptie aplicatii digitale sub forma SaaS
- Securitatea, trasabilitatea si managementul datelor cu caracter personal
- E-voting pentru proiectele majore ale comunității (mobil, blockchain)
- Informarea online pe mobil a tuturor cetățenilor despre fiecare aprobare de dezvoltare urbana

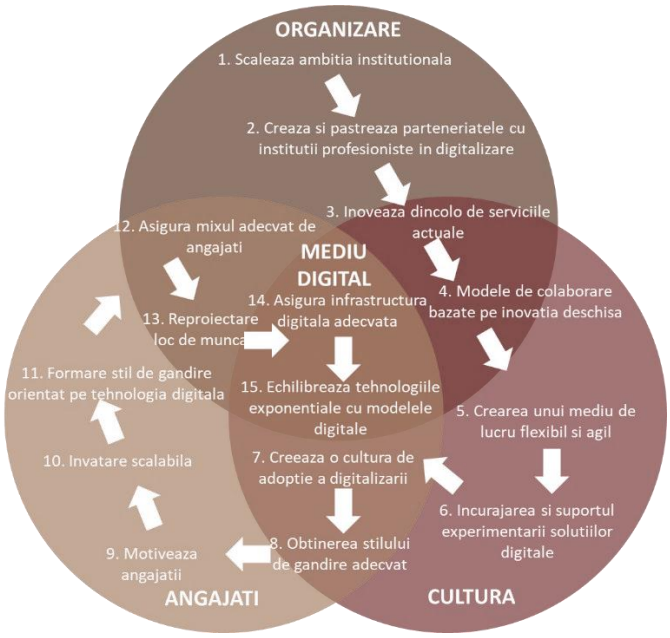
Pașii transformării digitale

Transformarea digitală a Primăriei Bistrița trebuie sa includă următorii pași și activități:

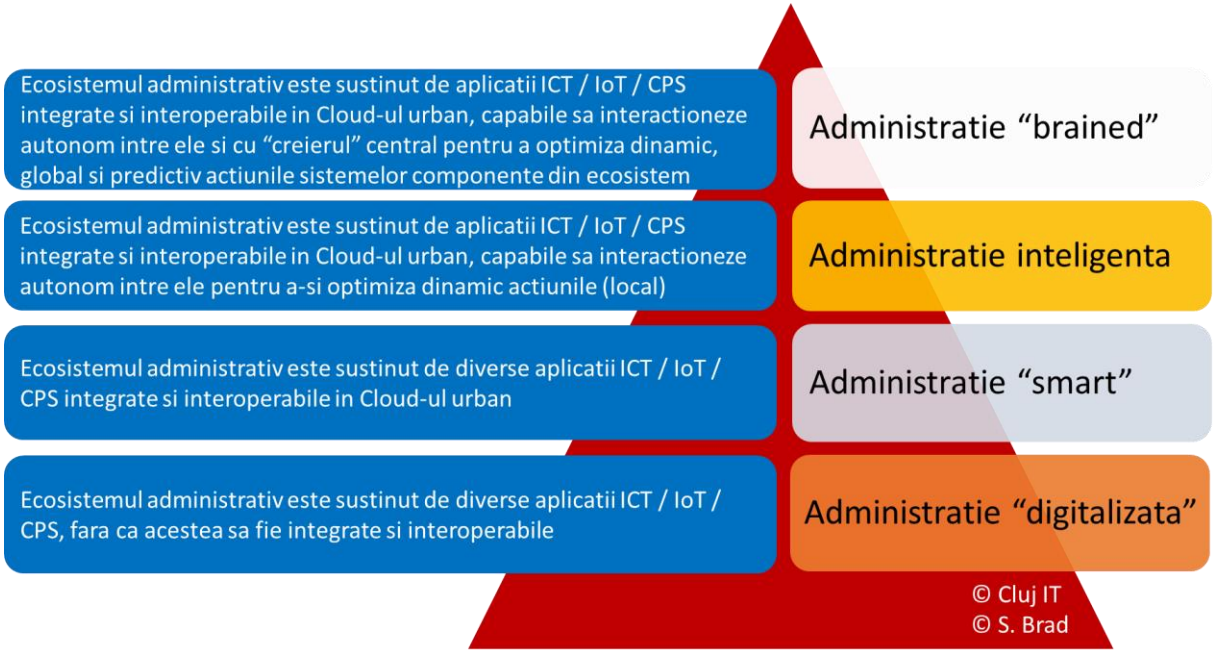
1. Evaluarea actualului sistem informatic al primăriei - Această etapă implică evaluarea sistemului informatic existent al primăriei, inclusiv hardware, software și aplicații utilizate. În primul rând, este necesară o evaluare a stadiului actual al primăriei în ceea ce privește utilizarea tehnologiilor digitale. Această evaluare ar trebui să includă analiza proceselor și a sistemelor existente, precum și a gradului de digitalizare al serviciilor oferite.
2. Definirea obiectivelor de transformare digitală - Se va defini un plan de transformare digitală care să includă obiective clare și măsurabile, cum ar fi creșterea eficienței, îmbunătățirea experienței utilizatorilor și reducerea costurilor. În funcție de rezultatele evaluării inițiale, este

necesar să se planifice transformarea digitală. Aceasta implică definirea obiectivelor și a priorităților, precum și alocarea resurselor necesare pentru implementarea acestora. De asemenea, este important să se ia în considerare și implicarea angajaților și a cetățenilor în procesul de transformare.

3. Selectarea echipei de proiect - Se va forma o echipă de proiect formată din membrii cheie ai personalului primăriei, care vor coordona și implementa proiectul.
4. Identificarea soluțiilor de tehnologie potrivite - Se vor identifica soluțiile de tehnologie care vor fi implementate pentru a ajuta la îndeplinirea obiectivelor de transformare digitală.
5. Implementarea soluțiilor de tehnologie - Implementarea soluțiilor tehnologice este un pas crucial în procesul de transformare digitală. Soluțiile identificate vor fi implementate, cum ar fi implementarea unui sistem integrat de gestionare a documentelor sau crearea unei aplicații mobile pentru cetățeni. Aceasta poate include si introducerea unui sistem integrat de management al informațiilor, implementarea de aplicații și platforme digitale pentru serviciile publice, precum și actualizarea echipamentelor și infrastructurii IT.
6. Testarea și validarea soluțiilor - Toate soluțiile de tehnologie implementate vor fi testate și validate pentru a se asigura că funcționează corect și că îndeplinesc obiectivele de transformare digitală.
7. Formarea și instruirea personalului - Toți membrii ai personalului vor fi instruiți cu privire la noile soluții de tehnologie și vor primi instruire pentru a putea utiliza noile aplicații și sisteme. Pentru a asigura succesul transformării digitale, este important să se ofere training și dezvoltare a competențelor digitale pentru angajați și cetățeni. Aceasta poate include training pentru utilizarea noilor tehnologii, dezvoltarea abilităților de comunicare digitală și de management al datelor.
8. Comunicarea cu cetățenii - Se va comunica cu cetățenii cu privire la noile soluții digitale implementate, inclusiv prin intermediul unui portal online sau a unei aplicații mobile.
9. Monitorizarea și evaluarea performanței - Se va monitoriza și evalua performanța sistemului informatic actualizat, precum și impactul transformării digitale asupra eficienței, experienței utilizatorilor și costurilor. Este important să se monitorizeze și să se evalueze performanțele transformării digitale. Aceasta poate include analiza feedback-ului cetățenilor, măsurarea eficienței și eficacității noilor servicii digitale, precum și identificarea și remedierea eventualelor probleme sau deficiențe.
10. Îmbunătățiri și actualizări continue - Se vor continua eforturile de îmbunătățire a sistemului informatic al primăriei și de actualizare a soluțiilor digitale pentru a îndeplini în continuare obiectivele de transformare digitală.



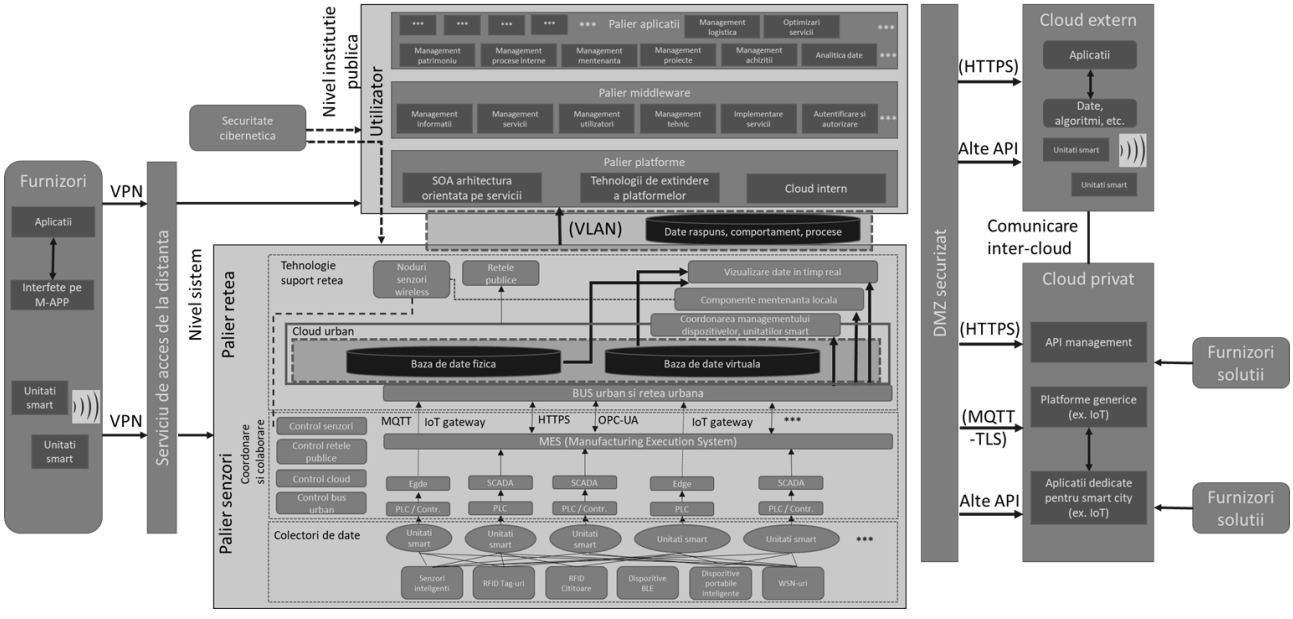
Transformarea digitală din perspectivă procesuală



Planificare pentru digitalizare Ce vrem? De ce vrem? Unde vrem sa ajungem?	**Strategie digitalizare** Optiuni si tactici Prioritizari	**Executie strategie digitalizare** Fise proiecte Atragere resurse	**Indeplinire preconditii** Proiecte suport Reinginerie procese	**Implementare proiecte** Executie proiecte Integrare rezultate
Constientizare context	Viziune	Fise proiecte "antibiotic"	Constientizare personal	Derulare proiecte
Constientizare provocari	Optiuni de evolutie	Fise proiecte "analgezic"	Educatie digitala	Implementare rezultate
Definire indicatori de progres	Analiza SWOT	Fise proiecte "vitamina"	Arhitectura si infrastructura	Consolidare
Audituri pe diverse paliere	Selectie traiectorie progres	Identificare surse de finantare	Securitate cibernetica	
Evaluare riscuri	Analiza de impact	Pregatire documentatie	Regandire procese	
Evaluare bariere	Proiecte si bugete	Aplicare pentru finantare	Aplicatii SaaS	
Solutii impotriva barierelor	Prioritizarea proiectelor			
Solutii impotriva riscurilor	Optimizarea resurselor			
Calibrare ambitii				

Abordarea structurată a digitalizării primăriei

Arhitectura de referință pentru ca primăria să poată atinge nivelul avansat de digitalizare



Arhitectura suport pentru transformarea digitală

Proiecte pentru susținerea transformării digitale

Exemple de proiecte aliniate cu transformare digitală a unei primării includ:

1. Crearea unui portal online pentru servicii publice - un site web sau o aplicație mobilă care permite cetățenilor să acceseze și să solicite servicii publice de la primărie în mod electronic, fără a fi necesară deplasarea fizică la sediul instituției. Buget: 50.000 - 100.000 euro, durata: 6 - 12 luni.
2. Implementarea sistemelor de e-guvernare - utilizarea tehnologiei pentru a gestiona documentele, plățile și alte aspecte administrative ale primăriei, precum și pentru a îmbunătăți interacțiunea între cetățeni și instituție. Buget: 100.000 - 200.000 euro, durata: 12 - 18 luni.
3. Utilizarea senzorilor și a Internetului lucrurilor (IoT) pentru a colecta și analiza date despre trafic, poluare, iluminat public, colectarea deșeurilor și alte aspecte ale vieții urbane pentru a îmbunătăți eficiența și calitatea serviciilor publice. Buget: 150.000 - 300.000 euro, durata: 12 - 24 luni.
4. Implementarea sistemelor de vot electronic - permiterea cetățenilor să voteze online pentru alegeri sau referendumuri, ceea ce poate crește participarea și implicarea cetățenilor în procesul democratic. Buget: 50.000 - 100.000 euro, durata: 6 - 12 luni.
5. Integrarea tehnologiei blockchain pentru securitatea și transparența tranzacțiilor și a documentelor, inclusiv pentru gestionarea cadastrului și a altor aspecte legate de proprietatea imobiliară. Buget: 100.000 - 200.000 euro, durata: 12 - 18 luni.
6. Dezvoltarea aplicațiilor de realitate augmentată sau virtuală pentru turismul local, educație și alte domenii care pot spori atractivitatea orașului. Buget: 50.000 - 100.000 euro, durata: 6 - 12 luni.
7. Utilizarea inteligenței artificiale pentru a îmbunătăți procesele administrative, inclusiv pentru asistență virtuală și chatbot-uri pentru a răspunde la întrebările cetățenilor sau pentru a efectua evaluări automatizate ale documentelor. Buget: 100.000 - 200.000 euro, durata: 12 - 18 luni.
8. Implementarea sistemelor de facturare electronică pentru taxe și impozite, pentru a facilita procesul de plată și a reduce timpul și costurile administrative. Buget: 50.000 - 100.000 euro, durata: 6 - 12 luni.
9. Dezvoltarea unei platforme online pentru gestionarea și monitorizarea proiectelor de dezvoltare urbană și pentru implicarea cetățenilor în procesul decizional. Buget: 150.000 - 300.000 euro, durata: 12 - 24 luni.
10. Implementarea sistemelor de monitorizare a calității aerului și a poluării, pentru a lua măsuri pentru reducerea poluării și îmbunătățirea calității vieții în oraș. Buget: 100.000 - 200.000 euro, durata: 12 - 18 luni.
11. Utilizarea tehnologiei de recunoaștere facială și a altor tehnologii de securitate pentru îmbunătățirea siguranței în oraș, inclusiv în locații publice, cum ar fi piețe sau parcuri. Buget: 500.000 – 1.000.000 euro, durata: 12 - 24 luni.
12. Implementarea sistemelor de monitorizare și gestionare a traficului, inclusiv a semafoarelor inteligente și a sistemelor de parcare inteligente, pentru a îmbunătăți circulația în oraș. Buget: 2.000.000 – 3.000.000 euro, durata: 24 - 36 luni.
13. Dezvoltarea unei platforme online pentru angajare și recrutare, care să ofere o interfață ușor de utilizat pentru căutarea de locuri de muncă și recrutarea de personal pentru Primărie. Buget: 100.000 – 200.000 euro, durata: 6 - 12 luni.
14. Dezvoltarea unui sistem de management al documentelor și al arhivei electronice, pentru a reduce timpul și costurile administrative și a îmbunătăți eficiența proceselor de gestionare a documentelor. Buget: 500.000 – 1.000.000 euro, durata: 12 - 24 luni.
15. Implementarea unui sistem de monitorizare a consumului de energie în clădirile Primăriei și a sistemelor de iluminat, pentru a reduce costurile și a îmbunătăți eficiența energetică. Buget: 500.000 – 1.000.000 euro, durata: 12 - 24 luni.
16. Utilizarea tehnologiei de realitate virtuală pentru a crea modele și simulări ale dezvoltării urbane, pentru a ajuta la luarea deciziilor și la planificarea dezvoltării urbane durabile. Buget: 1.000.000 – 2.000.000 euro, durata: 24 - 36 luni.

17. Dezvoltarea unei aplicații mobile pentru informarea cetățenilor despre evenimente, servicii și noutăți locale, inclusiv despre programul de colectare a deșeurilor și despre starea traficului. Buget: 100.000 – 200.000 euro, durata: 6 - 12 luni.
18. Utilizarea tehnologiei de automatizare a proceselor de gestionare a resurselor umane, inclusiv pentru recrutare, evaluare și formare. Buget: 5.000 – 20.000 euro, durata: 6 - 8 luni.
19. Implementarea unui sistem de gestionare a flotei de vehicule și de echipamente, pentru a reduce costurile și a îmbunătăți eficiența proceselor administrative. Buget: 50.000 – 200.000 euro, durata: 6 - 12 luni.
20. Dezvoltarea unui sistem de urmărire a calității serviciilor publice, inclusiv a feedback-ului cetățenilor și a soluțiilor propuse pentru îmbunătățirea serviciilor publice. Buget: 5.000 – 20.000 euro, durata: 6 - 12 luni.
21. Utilizarea tehnologiei de Internet of Things (IoT) pentru a monitoriza și gestiona starea și utilizarea clădirilor publice - utilizarea senzorilor pentru a monitoriza temperatura, umiditatea, iluminatul și alte variabile în clădiri pentru a îmbunătăți confortul și eficiența energetică, precum și pentru a identifica problemele de mentenanță înainte ca acestea să devină critice. De asemenea, prin intermediul IoT se poate gestiona eficient utilizarea clădirilor și a resurselor aferente, prin detectarea prezenței umane și ajustarea sistemelor de iluminat și climatizare în consecință, precum și prin gestionarea eficientă a spațiilor de parcare și a altor facilități din clădiri. Buget: 100.000 – 200.000 euro, durata: 6 - 12 luni.
22. Utilizarea soluțiilor de analiză de date pentru îmbunătățirea serviciilor publice și planificarea urbană - aceasta implică colectarea și analiza datelor din diverse surse, inclusiv senzori, sisteme GPS și alte aplicații pentru a înțelege mai bine nevoile cetățenilor și pentru a planifica îmbunătățiri ale serviciilor publice și dezvoltării urbane. Buget: 50.000 – 100.000 euro, durata: 3 - 6 luni.
23. Implementarea tehnologiei smart parking - prin utilizarea senzorilor și a aplicațiilor mobile, se poate îmbunătăți disponibilitatea locurilor de parcare și reducerea traficului în oraș. Buget: 50.000 – 100.000 euro, durata: 3 - 6 luni.
24. Integrarea sistemelor de monitorizare video pentru a îmbunătăți securitatea publică și pentru a preveni infracțiunile. Buget: 50.000 – 100.000 euro, durata: 3 - 6 luni.
25. Utilizarea tehnologiei cloud pentru stocarea și gestionarea datelor primăriei - aceasta poate duce la reducerea costurilor și la creșterea eficienței administrative. Buget: 20.000 – 50.000 euro, durata: 1 - 3 luni.
26. Utilizarea soluțiilor de automatizare a proceselor pentru a reduce munca manuală și pentru a îmbunătăți eficiența administrativa. Buget: 50.000 – 100.000 euro, durata: 3 - 6 luni.
27. Implementarea tehnologiei de învățare automată pentru îmbunătățirea proceselor administrative și a planificării urbane - prin analiza datelor și a comportamentului cetățenilor, se pot identifica modele și se pot lua decizii informate pentru îmbunătățirea serviciilor publice. Buget: 100.000 – 200.000 euro, durata: 6 - 12 luni.
28. Utilizarea sistemelor de analiză a datelor (big data) pentru a identifica modele și tendințe în datele colectate, precum și pentru a realiza previziuni și pentru a optimiza procesele administrative și serviciile publice oferite. Aceasta poate include analiza datelor despre traficul rutier, consumul de energie sau de apă, poluarea și alte variabile pentru a îmbunătăți eficiența și calitatea serviciilor oferite de primărie. Buget: 100.000 – 200.000 euro, durata: 6 - 12 luni.
29. Dezvoltarea aplicațiilor mobile pentru a îmbunătăți accesul cetățenilor la serviciile publice și pentru a facilita interacțiunea cu instituția. Aceste aplicații pot fi utilizate pentru a obține informații despre evenimentele locale, programarea de întâlniri cu autoritățile publice, solicitarea serviciilor publice, depunerea de petiții sau reclamații, achitarea taxelor și impozitelor online, și multe altele. Buget: 20.000 – 50.000 euro, durata: 4 - 6 luni.
30. Implementarea tehnologiei de recunoaștere facială și de monitorizare video pentru a îmbunătăți securitatea în zonele publice și pentru a combate infracțiunile. Aceasta poate include instalarea de camere de supraveghere conectate la un sistem centralizat de monitorizare, utilizarea de tehnologii de recunoaștere facială pentru a identifica persoanele suspecte și pentru a monitoriza fluxul de oameni în zonele aglomerate. Buget: 100.000 – 500.000 euro, durata: 6 - 12 luni.

31. Utilizarea tehnologiei de blockchain pentru a asigura integritatea și transparența datelor colectate și a proceselor administrative. Aceasta poate include utilizarea de smart contract-uri pentru a automatiza procesele și pentru a asigura conformitatea cu reglementările, precum și utilizarea tehnologiei de blockchain pentru a gestiona documentele și tranzacțiile. Buget: 50.000 – 100.000 euro, durata: 6 - 12 luni.
32. Dezvoltarea unei platforme digitale de comunicare cu cetățenii pentru a îmbunătăți transparența și implicarea acestora în procesul decizional. Aceasta poate include utilizarea de forumuri online, sondaje și petiții, precum și organizarea de consultări publice și de dezbateri pentru a permite cetățenilor să-și exprime opinia și să participe la procesul de luare a deciziilor. Buget: 10.000 – 30.000 euro, durata: 3 - 6 luni.
33. Implementarea soluțiilor de smart city - folosirea tehnologiei și a datelor pentru a gestiona și îmbunătăți aspecte urbane precum iluminatul public, mobilitatea, parcurile și spațiile verzi, dar și pentru a încuraja turismul și pentru a crește calitatea vieții locuitorilor. Buget: 1.000.000 – 5.000.000 euro, durata: 24 - 36 luni.
34. Integrarea sistemelor de facturare și plată online - permiterea cetățenilor să plătească taxele și impozitele online, reducând astfel timpul și costurile asociate plății fizice la ghișeele primăriei. Buget: 5.000 – 30.000 euro, durata: 1 - 3 luni.
35. Implementarea soluțiilor de e-learning - folosirea tehnologiei pentru a oferi cursuri online pentru cetățeni în diverse domenii, precum și pentru a spori eficiența și calitatea învățământului în școlile publice. Buget: 50.000 – 200.000 euro, durata: 6 - 12 luni.
36. Utilizarea roboților și a automatizării pentru a gestiona procesele administrative - de exemplu, folosirea roboților software pentru a prelucra și a gestiona documente, pentru a efectua apeluri automate către cetățeni sau pentru a trimite mesaje automate. Buget: 10.000 – 100.000 euro, durata: 6 - 12 luni.
37. Integrarea serviciilor de transport inteligent - de exemplu, utilizarea tehnologiei pentru a monitoriza traficul și pentru a oferi sugestii de trasee alternative sau pentru a optimiza programul de transport în comun. Buget: 10.000 – 100.000 euro, durata: 6 - 12 luni.
38. Implementarea soluțiilor de securitate cibernetică pentru protejarea datelor și a infrastructurii IT împotriva atacurilor cibernetice. Buget: 50.000 – 500.000 euro, durata: 6 - 12 luni.

Alte proiecte posibile:

1. Implementarea de soluții de energie verde și durabilă, cum ar fi panourile solare, pentru a reduce costurile și impactul asupra mediului. Costurile și timpul de implementare depind de nivelul de infrastructură necesar pentru a instala și a opera soluțiile de energie verde și durabilă. Buget: 5.000.000 – 10.000.000 euro, durata: 12 - 24 luni.
2. Dezvoltarea de soluții de turism inteligent, cum ar fi ghiduri turistice inteligente sau aplicații mobile pentru turiști, pentru a îmbunătăți experiența turiștilor și pentru a crește veniturile din turism. Costurile și timpul de implementare depind de caracteristicile necesare ale soluțiilor de turism inteligent și de nivelul de infrastructură necesar pentru a le opera. Buget: 300.000 – 1.500.000 euro, durata: 24 - 36 luni.
3. Utilizarea tehnologiei de blockchain pentru a gestiona și a monitoriza procesele de achiziții publice și pentru a îmbunătăți transparența și securitatea acestora. Buget: 500.000 – 2.000.000 euro, durata: 18 - 24 luni.
4. Utilizarea de drone pentru monitorizarea și gestionarea diferitelor aspecte urbane, cum ar fi traficul, poluarea și starea clădirilor publice. Costurile și timpul de implementare depind de echipamentele și software-ul necesare și de gradul de infrastructură necesară pentru a opera dronele în mod eficient. Buget: 200.000 – 1.500.000 euro, durata: 12 - 24 luni.
5. Implementarea de soluții de automatizare a serviciilor publice, cum ar fi sistemul de apeluri automate pentru a notifica cetățenii cu privire la diferitele servicii sau alerte. Costurile și timpul de implementare depind de tipul de soluție de automatizare utilizată și de nivelul de infrastructură necesar pentru a o implementa. Buget: 300.000 – 2.000.000 euro, durata: 6 - 12 luni.

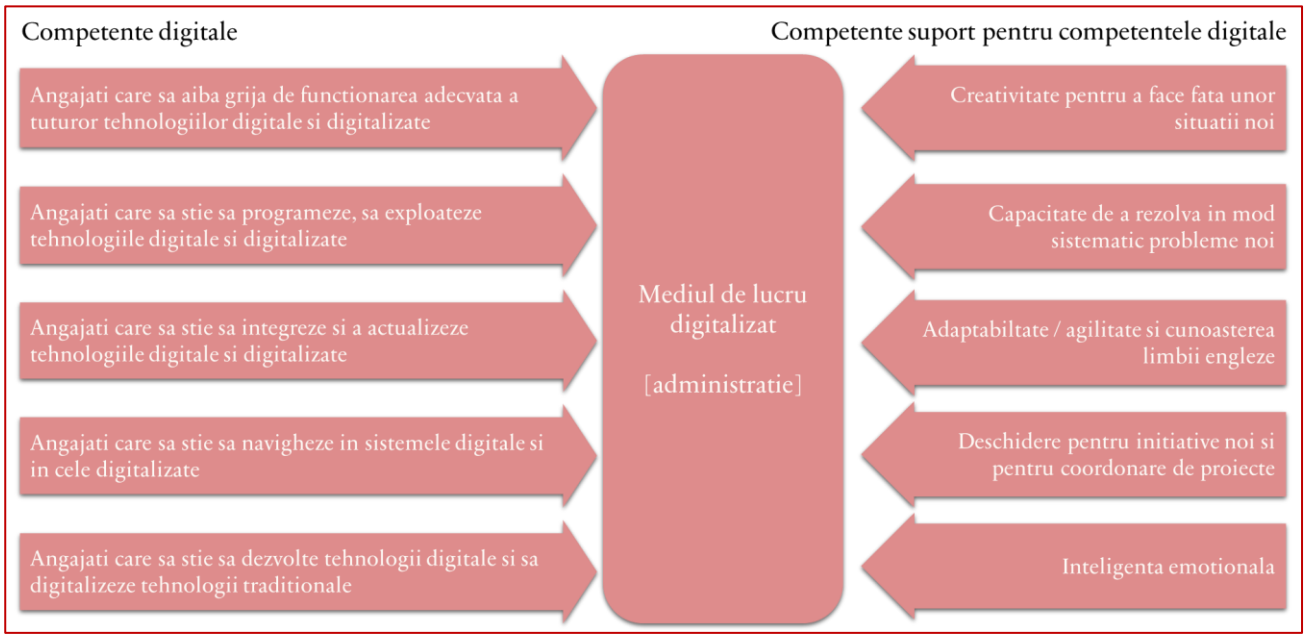
6. Implementarea soluțiilor de chatbot pentru a răspunde rapid la întrebările și solicitările cetățenilor cu privire la serviciile publice oferite. Buget: 200.000 – 1.000.000 euro, durata: 12 - 24 luni.
7. Dezvoltarea de aplicații mobile pentru a monitoriza și a gestiona activitățile de voluntariat din oraș. Buget: 50.000 – 100.000 euro, durata: 6 - 12 luni.
8. Dezvoltarea de aplicații mobile pentru a îmbunătăți accesul la servicii de sănătate publică, precum programări la medic sau informații despre vaccinare. Buget: 100.000 – 150.000 euro, durata: 12 - 18 luni.
9. Utilizarea tehnologiei de realitate augmentată pentru a oferi instruire și formare angajaților primăriei și a cetățenilor. Buget: 50.000 – 100.000 euro, durata: 6 - 12 luni.

Educația digitală a angajaților pentru a susține transformarea digitală

Dezvoltarea competentelor digitale trebuie sa mearga in tandem cu transformarea digitala a primăriei. Asteptarile privind capabilitatile digitale in primărie sunt:

- Abilitatea de a intelege, analiza, pune in aplicare acte normative, incluzand legi, norme de implementare, instructiuni, prin asistare cu platforme IT specializate
- Abilitatea de a intelege, analiza, pune in aplicare proceduri operationale informatizate si de a contribui la realizarea si actualizarea acestora
- Capacitatea de a analiza si documenta un proces operational curent informatizat cu care persoana respectiva este familiarizata, abilitatea de a identifica obiectivele, activitatile, rolurile persoanelor implicate in cadrul procesului
- Capacitatea de a colecta observatiile persoanelor deservite de procesele operationale de e-Guvernare (cetateni) si a persoanelor implicate in derularea acestora (functionari publici) in vederea evaluarii si eventualei imbunatatiri a activitatilor
- Capacitatea de a evalua rezultatele derularii activitatilor informatizate in comparatie cu ceea ce s-a planificat sau asteptat

La ce se refera competentele digitale?



Specificul muncii intr-o primarie digitalizata

Alfabetizarea digitala: Abilitatea de a gasi, evalua, utiliza, prelua si crea continut folosind tehnologia informatiei si Internetul

Competentele digitale: Sunt orice competente care ii confera unei persoane calitatea de literat digital - de la abilitatea de a gasi o informatie pe Internet folosind un telefon mobil sau un calculator, la crearea si utilizarea unui cont de email, la instalarea unei aplicatii pe telefonul mobil si pe calculator, la navigarea intr-o platforma cu documente, la utilizarea unui editor de text si a unui utilitar de prezentare, la posibilitatea de a folosi un sistem software pentru proiectare asistata, la configurarea unei platforme de management a proiectelor, la operarea intr-o platforma de munca colaborativa, la sondarea pietei prin platforme web, la programarea unor masini si echipamente, la manipularea unor echipamente digitalizate si pana la crearea unui blog, a unui site web, culminand cu utilizarea unor limbaje de programare si tehnologii digitale pentru dezvoltarea de sisteme software pentru Internet, pentru dispozitive mobile sau pentru sisteme fizico-cibernetice, etc.

Competențe digitale de bază pentru funcționarii publici

- Preconditie: cunoasterea limbii engleze cel putin la un nivel de baza … apoi
- Utilizarea adecvata a email-ului
- Dezvoltarea unor strategii eficace de investigare pe Internet si cautare de informatii
- Utilizarea de software statistic (ex. Excel)
- Crearea unor formate online de sondare a unui public tinta (ex. Google Forms)
- Folosirea unor editoare pentru a produce si prezenta materiale scrise (ex. MS Word)
- Navigarea intr-un sistem de operare pe calculator (ex. Windows)
- Dezvoltarea si livrarea unor prezentari vizuale [text, grafica, imagini] (ex. PowerPoint, Prezi)
- Administrarea identitatii personale in medii online [retele sociale] (ex. LinkedIn)
- Utilizarea unei game largi de tehnologii de tele-comunicare (ex. Skype, Slack)
- Utilizarea tehnologiilor care permit munca colaborativa prin Internet (ex. Google Drive)
- Crearea si editarea de imagini si clipuri video (ex. Camtasia)
- Utilizarea instrumentelor de “bookmarking” online pentru a imbunatati productivitatea online (ex. FireFox)
- Operarea in oricare platforma de management a fluxurilor de baza din organizatie [ex. registratura online, incarcare date in sistemele de raportare, semnatura electronica etc.]
- Utilizarea instrumentelor de traducere automata in medii online (ex. Google Translate)
- Operarea in mai multe browsere pentru Internet (ex. Microsoft Edge, Mozilla FireFox, etc.)
- Administrarea fisierelor pe calculator
- Instalarea unei aplicatii pe calculator si telefon mobil

Asigurarea infrastructurii tehnice în relație cu cloud-ul guvernamental

- Trebuie definite clar și pragmatic elementele de infrastructură de care este nevoie. Alegerile trebuie să fie justificate obiectiv și corelate cu disponibilitatea resurselor umane pentru gestiunea lor corespunzătoare.
- Direcția clară este utilizarea tuturor aplicațiilor prin browser, la distanță, cu găzduire în infrastructuri scalabile și extensibile gestionate profesional în condiții ridicate de securitate și performanță.
- Evoluăm spre standardizare funcțională și tehnică, arhitecturi modulare “plug-and-play”, reutilizarea componentelor informatice, înlocuirea lor ușoară și rapidă, achiziție în comun și utilizare comună (“multi-tenant”) din infrastructuri puse la dispoziție unui număr mare de utilizatori.
- Nu este fezabil să așteptăm dezvoltarea infrastructurii și a implementării sistemelor la nivel central.
- Deocamdată lipsește inițiativa unui standard al modelelor de proces în administrația publică, informatizarea unitară și standardizată nu este încă susținută strategic.

- Nu avem o ontologie informațională națională, nici un plan în acest sens, pentru a asigura standardizarea structurilor de date, a utilizării lor, a interoperabilității semantice.
- Cloud-ul Guvernamental este mai mult decât o infrastructură fizică dar deocamdată ecosistemul de aplicații este un orizont prea îndepărtat.
- PCUe, portalul central de acces la toate serviciile publice, va fi regândit și reimplementat, integrarea tuturor instituțiilor va fi necesară.

Organigrama IT în cazul transformării digitale a primăriei

Pentru o primărie a unui oraș care tinde spre 100.000-150.000 locuitori, organigrama departamentului de IT trebuie să arate în felul următor:

1. Director IT

├── 1.1. Manager Infrastructură și Suport Tehnic

│ ├── 1.1.1. Administrator Sistem

│ ├── 1.1.2. Specialist Rețele

│ └── 1.1.3. Tehnician Suport Tehnic

├── 1.2. Manager Dezvoltare Software și Aplicații

│ ├── 1.2.1. Dezvoltator Software

│ ├── 1.2.2. Specialist Baze de Date

│ └── 1.2.3. Specialist Web și UX/UI

├── 1.3. Manager Securitate și Conformitate

│ ├── 1.3.1. Expert Securitate Cibernetică

│ ├── 1.3.2. Asistent Securitate Cibernetică

│ └── 1.3.3. Ofițer GDPR

├── 1.4. Manager Proiecte și Transformare Digitală

│ ├── 1.4.1. Expert GIS

│ ├── 1.4.2. Expert Arhivă Electronică

│ └── 1.4.3. Expert Management Sistem de Digitalizare

└── 1.5. Coordonator Soluții Informatice Dedicate

├── 1.5.1. Specialist Comunicare Digitală

└── 1.5.2. Asistent Comunicare și Suport Tehnic

Organigrama propusă este adecvată și necesară pentru a aborda complexitatea și amploarea transformării digitale a unei primării a unui oraș cu 100.000-150.000 locuitori. Ea asigură eficiența, scalabilitatea, securitatea, inovația și orientarea către cetățean, care sunt aspecte esențiale ale transformării digitale într-un astfel de context. Argumentele pentru care organigrama propusă este adecvată și necesară în raport cu transformarea digitală a primăriei.

1. Amploarea transformării digitale: Transformarea digitală a primăriei implică numeroase procese, tehnologii și sisteme care trebuie să fie implementate, gestionate și întreținute. Aceasta necesită o echipă multidisciplinară capabilă să facă față diverselor aspecte ale

transformării, de la infrastructură, dezvoltare de software, securitate cibernetică, până la managementul proiectelor și comunicarea digitală.

2. Scalabilitatea și eficiența: Într-un oraș cu 100.000-150.000 de locuitori, cerințele IT vor fi în creștere pe măsură ce mai multe servicii devin digitale și populația orașului crește. O organigramă bine structurată asigură că departamentul IT poate scala și evolua pentru a face față acestor cerințe, evitând blocaje și întârzieri care ar putea afecta implementarea și funcționarea serviciilor digitale.
3. Securitatea și conformitatea: Un aspect esențial al transformării digitale este protejarea datelor și asigurarea conformității cu reglementările, cum ar fi GDPR. În acest context, este necesar să se aibă o echipă dedicată pentru a se asigura că securitatea și conformitatea sunt respectate în toate aspectele tehnologice ale primăriei.
4. Inovația și adaptabilitatea: Transformarea digitală este un proces în continuă evoluție, iar tehnologiile și soluțiile se schimbă rapid. Organigrama propusă include specialiști în diferite domenii care pot aduce expertiza și perspectiva necesară pentru a identifica și implementa cele mai recente și eficiente soluții IT.
5. Servicii și comunicare orientate către cetățean: Transformarea digitală a primăriei are drept scop îmbunătățirea serviciilor și a interacțiunii cu cetățenii. Prin includerea unor roluri precum Specialist Comunicare Digitală și Asistent Comunicare și Suport Tehnic, organigrama reflectă această prioritate și asigură că echipa IT poate răspunde eficient nevoilor cetățenilor și așteptărilor acestora.

Situația actuală suprapusă peste organigrama recomandată arată astfel:

1. Director IT

├─ 1.1. Manager Infrastructură și Suport Tehnic (Pozitie Vacanta)

│ ├── 1.1.1. Administrator Sistem

│ ├── 1.1.2. Specialist Rețele

│ └── 1.1.3. Tehnician Suport Tehnic

├─ 1.2. Manager Dezvoltare Software și Aplicații (Pozitie Vacanta)

│ ├── 1.2.1. Dezvoltator Software

│ ├── 1.2.2. Specialist Baze de Date

│ └── 1.2.3. Specialist Web și UX/UI - (Pozitie Vacanta)

├─ 1.3. Manager Securitate și Conformitate (Pozitie Vacanta)

│ ├── 1.3.1. Expert Securitate Cibernetică - (Pozitie Vacanta)

│ ├── 1.3.2. Asistent Securitate Cibernetică

│ └── 1.3.3. Ofițer GDPR - (Pozitie Vacanta)

├─ 1.4. Manager Proiecte și Transformare Digitală (Pozitie Vacanta)

│ ├── 1.4.1. Expert GIS - (Pozitie Vacanta)

│ ├── 1.4.2. Expert Arhivă Electronică - (Pozitie Vacanta)

│ └── 1.4.3. Expert Management Sistem de Digitalizare - (Pozitie Vacanta)

└─ 1.5. Coordonator Soluții Informatice Dedicate (Pozitie Vacanta)

├── 1.5.1. Specialist Comunicare Digitală - (Pozitie Vacanta)

└── 1.5.2. Asistent Comunicare și Suport Tehnic - (Pozitie Vacanta)

Pentru a prezenta o argumentație financiară privind costurile directe și ascunse în primărie, dacă organigrama este acoperită parțial, doar cu pozițiile curente, se analizează economiile și costurile suplimentare care pot rezulta din lipsa celorlalte poziții.

Economii:

1. Salarii și beneficii: Reducerea numărului de poziții în organigramă va duce la o reducere a costurilor cu salariile și beneficiile pentru angajații IT. Acest lucru poate fi considerat o economie directă în bugetul primăriei.
2. Costuri operaționale: Cu un număr mai mic de angajați, primăria poate economisi și la costurile operaționale, cum ar fi spațiul de birou, utilitățile și resursele tehnologice necesare pentru fiecare angajat.

Costuri suplimentare și ascunse:

1. Limitarea capacității de inovație și adaptabilitate: Cu un număr redus de specialiști și lipsa unor roluri-cheie în domeniul transformării digitale, primăria ar putea întâmpina dificultăți în a implementa și menține soluții IT inovatoare. Acest lucru ar putea duce la costuri ascunse, precum implementarea unor soluții depășite sau ineficiente, care ar putea afecta în mod negativ experiența cetățenilor și eficiența serviciilor.
2. Suprasolicitarea personalului IT: Dacă responsabilitățile rolurilor lipsă sunt distribuite către personalul IT existent, acesta ar putea fi suprasolicitat, ceea ce ar putea duce la erori și întârzieri în implementarea proiectelor. Aceasta ar putea genera costuri ascunse, precum repararea greșelilor sau angajarea de consultanți externi pentru a prelua unele sarcini.
3. Probleme de securitate și conformitate: Fără o echipă dedicată securității și conformității, primăria ar putea fi mai expusă riscurilor de securitate cibernetică și nerespectării reglementărilor, cum ar fi GDPR. Aceste vulnerabilități pot duce la costuri suplimentare și ascunse, precum pierderi financiare cauzate de breșe de securitate, amenzi pentru nerespectarea reglementărilor și pierderea încrederii cetățenilor.
4. Lipsa de coordonare și comunicare: Fără rolurile de coordonator și asistent de comunicare digitală, primăria ar putea întâmpina dificultăți în a comunica eficient cu cetățenii și a promova serviciile digitale. Acest lucru poate duce la costuri ascunse, precum percepții negative din partea cetățenilor și utilizarea insuficientă a serviciilor digitale, limitând astfel eficiența transformării digitale.

Analiza cost-beneficiu a organigramei

Analiza cost-beneficiu pentru cele două cazuri - acoperire parțială și acoperire integrală a organigramei IT – trebuie sa compare costurile și beneficiile asociate fiecărei situații pentru a ajuta la luarea unei decizii informate.

Acoperire parțială (situația curentă):

Costuri:

1. Salarii și beneficii: Reduse, comparativ cu acoperirea integrală.
2. Costuri operaționale: Reduse, comparativ cu acoperirea integrală.

Beneficii:

1. Economii bugetare imediate datorate costurilor reduse cu personalul și operațiunile.
2. O structură organizațională mai simplă și mai ușor de gestionat.

Costuri ascunse și riscuri:

1. Limitarea capacității de inovație și adaptabilitate.
2. Suprasolicitarea personalului IT și posibile întârzieri în implementarea proiectelor.
3. Probleme de securitate și conformitate.
4. Lipsa de coordonare și comunicare cu cetățenii.

Acoperire integrală (organigrama completă propusă):

Costuri:

1. Salarii și beneficii: Mai mari, comparativ cu acoperirea parțială.
2. Costuri operaționale: Mai mari, comparativ cu acoperirea parțială.

Beneficii:

1. O echipă multidisciplinară capabilă să gestioneze toate aspectele transformării digitale.
2. Scalabilitate și eficiență în funcționarea serviciilor digitale.
3. Protecție sporită a datelor și asigurarea conformității cu reglementările.
4. Inovație și adaptabilitate la noile tehnologii și soluții IT.
5. Comunicare și interacțiune eficientă cu cetățenii.

Costuri ascunse și riscuri:

1. Buget mai mare necesar pentru salariile și costurile operaționale.
2. O structură organizațională mai complexă, care poate necesita o coordonare și o gestionare mai atentă.

Decizia între cele două cazuri depinde de prioritățile și resursele primăriei. Acoperirea parțială poate aduce economii bugetare și o structură mai simplă, dar poate avea costuri ascunse și riscuri în ceea ce privește inovația, securitatea și comunicarea. Pe de altă parte, acoperirea integrală poate implica costuri mai mari, dar oferă o echipă multidisciplinară capabilă să gestioneze toate aspectele transformării digitale, asigurând o mai bună scalabilitate, eficiență și conformitate.

Autoritățile locale trebuie să analizeze aceste aspecte și să decidă care caz se potrivește cel mai bine nevoilor locale și strategiei de transformare digitală pe termen lung.

Abordarea îngustă – incorectă

O evaluare cantitativă a costurilor și beneficiilor pentru cele două cazuri. Luăm în considerare un salariu mediu net de 1.500 euro/lună și estimăm costurile directe și ascunse pentru ambele scenarii pe parcursul unui an.

Acoperire parțială (organigrama actuală):

Costuri directe:

1. Salarii și beneficii: 7 roluri x 1.500 euro x 12 luni = 126.000 euro/an
2. Costuri operaționale: Estimăm economii de 20% comparativ cu acoperirea integrală (valoare estimată): 0,2 * 50.000 euro = 10.000 euro/an

Costuri ascunse:

1. Suprasolicitarea personalului IT și întârzieri în proiecte: Estimare 10% din costul salarial = 12.600 euro/an
2. Probleme de securitate și conformitate (inclusiv amenzi): Estimare = 10.000 euro/an
3. Lipsa de coordonare și comunicare (consultanți externi, costuri oportunitate): Estimare = 8.000 euro/an

Cost total acoperire parțială organigramă: 126.000 + 10.000 + 12.600 + 10.000 + 8.000 = 166.600 euro/an

Acoperire integrală (organigrama completă propusă):

Costuri directe:

1. Salarii și beneficii: 20 roluri x 1.500 euro x 12 luni = 360.000 euro/an
2. Costuri operaționale: Estimare 50.000 euro/an (valoare aproximativă)

Costuri ascunse:

1. Potențiale costuri suplimentare de coordonare și management: Estimare 5% din costul salarial = 12.600 euro/an

Cost total acoperire integrală organigramă: 360.000 + 50.000 + 12.600 = 422.600 euro/an

Acoperirea parțială a organigramei ar costa primăria 166.600 euro/an, în timp ce acoperirea integrală ar costa 422.600 euro/an. Diferența dintre cele două cazuri este de 256.000 euro/an, reprezentând costurile suplimentare pentru a avea o echipă IT completă și multidisciplinară.

Este important să reținem că aceste estimări sunt aproximative și pot varia în funcție de condițiile locale, precum costurile de tarifele pentru consultanță și alte cheltuieli operaționale. În plus, estimările costurilor ascunse și ale riscurilor sunt bazate pe ipoteze și pot varia în funcție de performanța echipei IT și de circumstanțele locale.

Abordarea moderată – insuficientă, deci incorectă

Evaluarea pierderilor financiare estimate cauzate de lipsa întregii organigrame se poate realiza prin analiza costurilor ascunse și a riscurilor asociate cu acoperirea parțială a organigramei. Deși este dificil să cuantificăm cu exactitate aceste pierderi, putem estima valori aproximative în baza riscurilor menționate anterior.

Pierderi estimate:

1. Limitarea capacității de inovație și adaptabilitate: Pierderile pot fi determinate de investițiile ineficiente în tehnologie și întârzieri în implementarea proiectelor. Estimare: 10.000 euro/an.
2. Suprasolicitarea personalului IT și întârzieri în proiecte: Pierderile pot fi cauzate de productivitatea redusă și de costurile pentru remedierea greșelilor și angajarea consultanților externi. Estimare: 12.600 euro/an (conform calculelor anterioare).
3. Probleme de securitate și conformitate: Pierderile pot fi rezultatul breșelor de securitate, al pierderilor de date și al amenzilor pentru nerespectarea reglementărilor (inclusiv GDPR). Estimare: 10.000 euro/an (conform calculelor anterioare).
4. Lipsa de coordonare și comunicare cu cetățenii: Pierderile pot fi asociate cu o utilizare insuficientă a serviciilor digitale, o experiență negativă a utilizatorilor și o imagine deteriorată a primăriei. Estimare: 8.000 euro/an (conform calculelor anterioare).

Pierderi totale estimate: 10.000 + 12.600 + 10.000 + 8.000 = 40.600 euro/an

Aceste estimări sunt aproximative și pot varia în funcție de circumstanțele locale și de situația specifică a primăriei. De asemenea, pierderile estimate pot fi mai mari sau mai mici în funcție de evenimentele care pot apărea pe parcursul unui an și de măsura în care lipsa întregii organigrame afectează performanța departamentului de IT și serviciile oferite cetățenilor.

Este important să analizăm toate aspectele înainte de a lua o decizie. Comparând costurile totale pentru ambele scenarii și pierderile estimate, putem observa următoarea situație:

Costuri totale acoperire parțială + pierderi estimate: 166.600 euro/an + 40.600 euro/an = 207.200 euro/an Costuri totale acoperire integrală: 422.600 euro/an

Pe baza acestor calcule, costurile acoperirii parțiale și pierderile estimate sunt mai mici decât costurile acoperirii integrale. Cu toate acestea, trebuie să luăm în considerare și alte aspecte care nu pot fi cuantificate în mod direct în termeni financiari:

1. Transformarea digitală a primăriei: O echipă IT completă și multidisciplinară poate contribui la o transformare digitală mai eficientă și eficace, îmbunătățind serviciile publice și calitatea vieții cetățenilor.
2. Reziliența organizațională: O echipă IT extinsă poate îmbunătăți capacitatea primăriei de a se adapta la schimbările tehnologice și de a face față provocărilor viitoare.
3. Reputația primăriei: Un departament de IT bine organizat și eficient poate contribui la consolidarea încrederii cetățenilor în instituțiile publice și la o relație mai bună între administrație și cetățeni.
4. Proiecte pe termen lung: O echipă IT completă poate fi mai capabilă să gestioneze și să implementeze proiecte pe termen lung, care pot aduce beneficii semnificative în viitor.

Prin urmare, este important să analizăm atât aspectele financiare, cât și aspectele ne-monetare ale deciziei. Autoritățile locale trebuie să evalueze întreaga situație, să ia în considerare resursele și obiectivele lor pe termen lung și să aleagă soluția care le servește cel mai bine interesele și nevoile cetățenilor.

Trebui să luăm în considerare pierderile asociate cu productivitatea redusă a celorlalți 400 de angajați ai primăriei datorită neacoperirii integrale a organigramei IT. Având în vedere un salariu net lunar de 1.200 euro pentru acești angajați, putem estima pierderile ca urmare a unei productivități reduse.

Estimăm într-un scenariu optimist că lipsa unei organigrame IT complete duce la o reducere a productivității angajaților cu 5%. Această reducere a productivității se traduce în pierderi financiare ascunse pentru primărie.

Pierderi asociate cu productivitatea redusă a celor 400 de angajați:

Salarii anuale ale celor 400 de angajați: 400 x 1.200 euro x 12 luni = 5.760.000 euro/an Pierderi datorate reducerii productivității cu 5%: 5.760.000 euro x 0,05 = 288.000 euro/an

Adăugând aceste pierderi la calculul anterior:

Costuri totale acoperire parțială + pierderi estimate + pierderi datorate productivității reduse: 166.600 euro/an + 40.600 euro/an + 288.000 euro/an = 495.200 euro/an

Costuri totale acoperire integrală: 422.600 euro/an

Comparând costurile totale pentru ambele scenarii, inclusiv pierderile datorate productivității reduse a celorlalți angajați, costurile acoperirii parțiale devin semnificativ mai mari decât costurile acoperirii integrale. În acest caz, acoperirea integrală a organigramei IT ar fi o soluție mai eficientă din punct de vedere financiar și ar putea duce la o mai bună funcționare a primăriei și a serviciilor publice oferite cetățenilor.

Abordarea exhaustivă – corectă

Trebuie să includem riscul crescut de atacuri cibernetice și timpul suplimentar pierdut de cetățeni în lipsa unei transformări digitale superioare. Vom ajusta estimările privind pierderile de securitate și conformitate și vom adăuga costurile asociate timpului suplimentar pierdut de cetățeni.

1. Ajustarea pierderilor de securitate și conformitate:

Dacă riscul de atacuri cibernetice este mai mare, putem crește estimarea pierderilor de securitate și conformitate de la 10.000 euro/an la 20.000 euro/an.

2. Calculul costurilor asociate timpului suplimentar pierdut de cetățeni:

Să presupunem că în urma neacoperirii integrale a organigramei IT, cetățenii pierd în medie 5.000 de ore în plus pe an din cauza unor servicii publice mai puțin eficiente. La o rată medie de 5 euro/oră, costurile asociate acestui timp pierdut sunt:

5.000 ore x 5 euro/oră = 25.000 euro/an

Acum, vom recalcula costurile totale pentru ambele scenarii:

Costuri totale acoperire parțială + pierderi estimate ajustate + pierderi datorate productivității reduse + costurile timpului suplimentar pierdut de cetățeni: 166.600 euro/an + 50.600 euro/an (pierderi estimate ajustate) + 288.000 euro/an + 25.000 euro/an = 530.200 euro/an

Costuri totale acoperire integrală: 422.600 euro/an

După ajustarea calculelor, costurile acoperirii parțiale, incluzând riscul crescut de atacuri cibernetice și timpul suplimentar pierdut de cetățeni, rămân semnificativ mai mari decât costurile acoperirii integrale. În acest scenariu, acoperirea integrală a organigramei IT continuă să fie o soluție mai eficientă din punct de vedere financiar și ar putea duce la o mai bună funcționare a primăriei și a serviciilor publice oferite cetățenilor.

Descrierea rolurilor în organigrama propusă

1. Director IT:
Responsabilitățile sale includ planificarea, coordonarea și supervizarea întregului departament IT al primăriei. Directorul IT asigură implementarea și mentenanța tehnologiei în cadrul primăriei și este responsabil pentru elaborarea strategiei departamentului IT. Directorul IT trebuie să aibă o înțelegere profundă a tehnologiilor și tendințelor IT, precum și o perspectivă largă asupra impactului tehnologic asupra organizației și a modului în care tehnologia poate fi folosită pentru a îmbunătăți serviciile oferite către cetățeni și angajați. Directorul IT trebuie să colaboreze strâns cu ceilalți directori din primărie pentru a identifica nevoile și oportunitățile în ceea ce privește utilizarea tehnologiei în diferite departamente și proiecte. Printre responsabilitățile directorului IT se numără:

- Planificarea și coordonarea activităților de implementare și mentenanță a infrastructurii IT, inclusiv rețele, echipamente hardware și software, servicii de comunicare și stocare de date;

- Coordonarea dezvoltării și implementării aplicațiilor software personalizate, bazelor de date și sistemelor de informații geografice;
- Asigurarea securității informațiilor și conformității cu regulamentele și politicile de securitate cibernetică și protecție a datelor personale;
- Identificarea și gestionarea riscurilor de securitate cibernetică și prevenirea atacurilor cibernetice;
- Supervizarea proiectelor de transformare digitală și implementarea soluțiilor digitale pentru optimizarea fluxurilor de lucru și serviciilor oferite către cetățeni;
- Coordonarea și supervizarea echipei de IT, asigurându-se de dezvoltarea profesională a membrilor echipei și de buna lor colaborare;
- Comunicarea și colaborarea strânsă cu ceilalți directori din primărie, precum și cu furnizorii de servicii IT, pentru a identifica nevoile și oportunitățile în ceea ce privește utilizarea tehnologiei în diferite departamente și proiecte;
- Asigurarea bugetului departamentului IT, urmărirea cheltuielilor și monitorizarea resurselor și performanțelor departamentului;
- Altele în conformitate cu fișa postului.

1.1. Manager Infrastructură și Suport Tehnic:
Acest manager este responsabil pentru gestionarea și menținerea infrastructurii IT, inclusiv servere, rețele și echipamente hardware. De asemenea, coordonează echipa de suport tehnic, care oferă asistență și suport tehnic utilizatorilor de sisteme informatice din cadrul primăriei. Printre responsabilitățile Managerului Infrastructură și Suport Tehnic se numără:
- Gestionarea și menținerea infrastructurii IT, inclusiv servere, rețele și echipamente hardware, precum și coordonarea echipei de suport tehnic;
- Gestionarea și asigurarea bunei funcționari a serverelor și a sistemelor de operare;
- Administrarea echipamentelor de rețea și asigurarea conexiunii stabile și securizate între diferitele sisteme și utilizatori;
- Coordonarea echipei de suport tehnic, care oferă asistență și suport pentru utilizatorii de sisteme informatice din cadrul primăriei, rezolvând problemele legate de hardware și software;
- Implicarea în achiziționarea de echipamente și soluții IT și gestionarea contractelor de mentenanță și de servicii pentru telefonie fixă, mobilă și internet;
- Monitorizarea performanțelor și disponibilității infrastructurii IT și colaborarea cu celelalte roluri IT pentru a asigura o funcționare coezivă și eficientă a întregului sistem IT al primăriei;
- Altele în conformitate cu fișa postului.

1.1.1. Administrator Sistem:
Administratorul sistemului este responsabil pentru instalarea, configurarea și menținerea sistemelor de operare și serverelor, asigurându-se de buna funcționare a acestora. De asemenea, administrează mașinile suport de virtualizare și mașinile virtuale, gestionează contractele de mentenanță a programelor informatice dedicate și efectuează alte sarcini legate de mentenanța sistemelor informatice. Printre atribuții se numără:
- Se ocupă de administrarea mașinilor suport de virtualizare (5 echipamente în acest moment) și mașinilor virtuale (cca 25 în acest moment);
- Este responsabil de actualizarea și upgrade-ul sistemelor de operare suport de virtualizare (Debian/Proxmox în acest moment);
- Creează, modifică, șterge și arhivează mașini virtuale cu sisteme de operare diferite (Windows Server, diferite distribuții Linux);
- Se asigură că există un back-up redundant (pe HDD extern) zilnic și la alte termene pentru mașinile virtuale și bazele de date;
- Gestionează contractele de mentenanță a programelor informatice dedicate (asigură buget, întocmește documente de achiziție, urmărește procedura, verifică contracte înainte de încheiere, monitorizează derularea contractelor pe parcursul anului);
- Realizează alte sarcini aferente postului: va fi implicat și în alte sarcini, cum ar fi administrarea și mentenanța sistemelor de operare ale stațiilor de lucru și a laptopurilor, achiziția de

calculatoare, imprimante și alte echipamente IT, precum și actualizarea permanentă a portalului WEB și monitorizarea funcționării acestuia și a serviciilor electronice;
- Altele în conformitate cu fișa postului.

Administratorul de sistem trebuie să fie familiarizat cu diversele tehnologii și soluții IT, să fie atent la detalii și să aibă abilități bune de rezolvare a problemelor și de gestionare a timpului.

1.1.2. Specialist Rețele:
Specialistul în rețele proiectează, implementează și menține rețelele de comunicații ale primăriei, asigurându-se de conexiunea și securitatea acestora. De asemenea, gestionează sistemul de telefonie, administrarea contractului de telefonie mobilă și a infrastructurii de cabluri și prize, precum și gestionarea contractelor de servicii de telefonie fixă, mobilă și Internet. Pentru postul Specialist Rețele, responsabilitățile includ:
- Proiectarea, implementarea și menținerea rețelelor de comunicații ale primăriei, asigurându-se de conexiunea și securitatea acestora;
- Administrează sistemul de telefonie al primăriei, inclusiv centrala telefonică și aparatele analogice sau digitale conectate la rețeaua de date existentă - sistemul de telefonie are în prezent o centrală telefonică cu 600 de interioare și aparate analoage sau digitale conectate la rețeaua de date existentă;
- Administrarea contractelor de servicii de telefonie fixă, mobilă (în prezent (cca 100 de numere) și Internet, urmărind procedurile de achiziție și verificând contractele înainte de încheiere;
- Administrarea rețelei de comunicații a primăriei, inclusiv switch-urile, router-ele, infrastructura de cabluri și prize, dulapuri și alte echipamente de rețea;
- Se asigură că sunt respectate contractele de servicii de telefonie fixă, mobilă, Internet (asigură buget, întocmește documente de achiziție, urmărește procedura, verifică contracte înainte de încheiere, monitorizează derularea contractelor pe parcursul anului);
- Realizează alte sarcini aferente postului.

El trebuie să fie familiarizat cu diversele tehnologii și soluții IT și să aibă abilități bune de gestionare a timpului și de rezolvare a problemelor. De asemenea, trebuie să fie capabil să comunice clar și eficient cu membrii echipei și cu utilizatorii de sisteme informatice din cadrul primăriei.

1.1.3. Tehnician Suport Tehnic:
Tehnicianul de suport tehnic oferă asistență și suport tehnic pentru utilizatorii de sisteme informatice din cadrul primăriei, rezolvând problemele legate de hardware și software. Acesta se ocupă de depanarea software și hardware la stațiile de lucru, împreună cu efectuarea mici lucrări de extindere sau întreținere la rețeaua de date și gestionează achiziția calculatoarelor, multifuncționalelor, imprimantelor și altele. Pentru postul Tehnician Suport Tehnic, responsabilitățile includ:
- Oferirea de asistență și suport tehnic pentru utilizatorii de sisteme informatice din cadrul primăriei, rezolvând problemele legate de hardware și software;
- Depanarea software (până la un anumit nivel și hardware) la stațiile de lucru (cca 370 în acest moment) și laptop-uri, gestionarea multifuncționalelor de rețea (cca 35 în acest moment) și a altor echipamente IT, inclusiv achiziționarea și actualizarea lor;
- Actualizarea permanentă a portalului web și monitorizarea funcționării acestuia și a serviciilor electronice, iar în caz că apar probleme, anunță furnizorul de asistență tehnică (firma Indeco în acest moment);
- Efectuează mici lucrări de extindere sau întreținere la rețeaua de date;
- Altele în conformitate cu fișa postului.

El trebuie să fie familiarizat cu diverse tehnologii și soluții IT și să aibă abilități bune de gestionare a timpului și de rezolvare a problemelor. De asemenea, trebuie să fie capabil să comunice clar și eficient cu membrii echipei și cu utilizatorii de sisteme informatice din cadrul primăriei.

1.2. Manager Dezvoltare Software și Aplicații:
Acest manager este responsabil pentru supravegherea dezvoltării, implementării și întreținerii aplicațiilor software și a bazelor de date. În plus, acesta asigură funcționarea corespunzătoare a sistemului electronic de votare și se ocupă de administrarea sistemului de poștă electronică. Pentru postul Manager Dezvoltare Software și Aplicații, responsabilitățile include:

- Supervizarea dezvoltării, implementării și întreținerii aplicațiilor software și a bazelor de date ale primăriei;
- Coordonarea activităților echipei de dezvoltare software, asigurându-se că acestea sunt realizate în timp și buget, că se încadrează în cerințele specificate și că respectă cele mai bune practici de dezvoltare software;
- Asigurarea că aplicațiile dezvoltate respectă normele de securitate și de protecție a datelor;
- Dezvoltarea împreună cu echipa de securitate IT pentru a implementa soluții adecvate;
- Altele în conformitate cu fișa postului.

1.2.1. Dezvoltator Software:
Dezvoltatorul de software proiectează, dezvoltă și testează aplicații software personalizate pentru nevoile primăriei. Acesta se ocupă de administrarea sistemului de votare, organizează ședințele de consiliu local și administrează la nivel de interfață WEB server-ul de poștă electronică Zimbra. Pentru postul Dezvoltator Software, responsabilitățile includ:

- Proiectarea, dezvoltarea și testarea aplicațiilor software personalizate pentru nevoile primăriei;
- Lucrul împreună cu echipa de securitate IT pentru a se asigura că aplicațiile sunt securizate și să respecte normele de protecție a datelor;
- Pe lângă sistemul propriu de ședințe, organizează și ședințele de consiliu local (și cele pe comisii) care se țin pe Zoom, precum și alte ședințe pe Zoom (CTATU, CTE, etc.);
- Administrează la nivel de interfață WEB server-ul de poștă electronică Zimbra (475 de căsuțe de email în acest moment) – creează, modifică șterge căsuțe de email, arhivează email, etc.;
- Gestionează contracte de asistență la sistemul de vot al consiliului local;
- Altele în conformitate cu fișa postului.

Dezvoltatorul trebuie să aibă o cunoaștere solidă a diferitelor limbaje de programare, precum și o înțelegere aprofundată a principiilor de dezvoltare software și a metodelor de testare. El trebuie să fie capabil să traducă cerințele de afaceri în specificații tehnice și să creeze cod robust și scalabil.

1.2.2. Specialist Baze de Date:
Responsabilitățile acestui post includ proiectarea, implementarea și menținerea bazelor de date ale primăriei, asigurându-se că acestea sunt întotdeauna accesibile, fiabile și în conformitate cu cerințele de securitate și reglementările aplicabile. Printre sarcinile de zi cu zi se numără:

- Administrează și menține sistemul electronic de pontaj al primăriei, asigurându-se că acesta funcționează corespunzător și este actualizat în mod regulat (în prezent, 750 de angajați, în 21 de imobile în tot orașul – 21 de cititoare la venire și 21 la plecare + 42 de camere de supraveghere orientate spre cititoare);
- Administrează cele patru sisteme de monitorizare video existente în primărie, cu peste 100 de camere, asigurându-se de buna funcționare și securitatea lor;
- Ajută în perioada de achiziții, oferind expertiză în ceea ce privește cerințele și specificațiile tehnice necesare pentru achiziționarea de echipamente și software-uri noi;
- Gestionează contracte de mentenanță pentru centrul de date al primăriei, inclusiv întreținerea sistemelor de climatizare, controlul accesului și alarmele la incendiu;
- Identifică și implementează măsuri de protecție împotriva pierderii, coruperii sau accesului neautorizat la datele primăriei;
- Colaborează cu celelalte departamente ale primăriei pentru a dezvolta și implementa strategii și politici referitoare la bazele de date și la modul în care acestea sunt utilizate;
- Monitorizează performanța și integritatea bazelor de date, rezolvând problemele care apar și optimizând performanța acestora;

- Asigură accesul la date și informații pentru angajații primăriei și colaborează cu aceștia pentru a identifica și implementa noi cerințe și funcționalități pentru bazele de date ale primăriei;
- Altele conform fișei postului.

1.2.3. Specialist Web și UX/UI:
Specialistul Web și UX/UI este responsabil de proiectarea, dezvoltarea și optimizarea site-urilor web și aplicațiilor web ale primăriei, precum și interfețele grafice ale acestora. Acesta trebuie să asigure o experiență de utilizare plăcută și eficientă pentru utilizatorii finali, să respecte cele mai bune practici de UX/UI și să mențină site-urile web și aplicațiile web la cele mai recente standarde și tehnologii. Responsabilitățile specialistului Web și UX/UI includ:
- Proiectarea și dezvoltarea interfețelor grafice ale site-urilor web și aplicațiilor web ale primăriei, folosind cele mai bune practici de UX/UI;
- Asigurarea unei experiențe de utilizare plăcută și eficientă pentru utilizatorii finali prin optimizarea site-urilor web și aplicațiilor web ale primăriei;
- Colaborarea cu managerul dezvoltare software și aplicații și cu alți membri ai echipei IT pentru a asigura că site-urile web și aplicațiile web ale primăriei sunt dezvoltate în conformitate cu standardele și tehnologiile actuale;
- Actualizarea și întreținerea site-urilor web și aplicațiilor web ale primăriei pentru a se asigura că acestea rămân la cele mai recente standarde și tehnologii;
- Monitorizarea și analizarea performanței site-urilor web și aplicațiilor web ale primăriei și elaborarea de rapoarte periodice privind utilizarea acestora;
- Testarea și depanarea site-urilor web și aplicațiilor web ale primăriei pentru a identifica și remedia problemele legate de funcționalitate și securitate;
- Colaborarea cu alți membri ai echipei IT pentru a dezvolta și implementa noi funcționalități ale site-urilor web și aplicațiilor web ale primăriei în funcție de necesități;
- Identificarea și implementarea celor mai bune practici de UX/UI pentru site-urile web și aplicațiile web ale primăriei, precum și pentru alte materiale digitale;
- Întreținerea și actualizarea documentației tehnice relevante pentru site-urile web și aplicațiile web ale primăriei;
- Altele în conformitate cu fișa postului.

1.3. Manager Securitate și Conformitate:
Managerul de Securitate și Conformitate are responsabilitatea de a supraveghea și coordona activitățile legate de securitatea informatică și conformitatea cu reglementările în vigoare. Managerul de Securitate și Conformitate are următoarele responsabilități:
- Identifică riscurile de securitate informatică și dezvoltă strategii pentru protejarea sistemelor informaționale și a datelor primăriei;
- Supervizează activitățile legate de conformitate cu reglementările privind protecția datelor personale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR) și alte reglementări aplicabile;
- Coordonează cu echipa IT pentru a dezvolta și implementa politici și proceduri adecvate pentru asigurarea securității sistemelor informatice și protejarea datelor;
- Colaborează cu alte departamente ale primăriei pentru a identifica riscuri de securitate și pentru a dezvolta planuri de acțiune corespunzătoare;
- Implementează și monitorizează sistemele de securitate, cum ar fi sistemele de detectare a intruziunilor, sistemele de gestionare a vulnerabilităților și alte soluții de securitate informatică;
- Asigură formarea și informarea angajaților cu privire la politici și proceduri de securitate și conformitate, pentru a crește gradul de conștientizare a acestora;
- Coordonează cu furnizorii externi pentru a asigura securitatea și confidențialitatea datelor în cadrul acordurilor de servicii;
- Identifică și implementează cele mai bune practici pentru securitatea și conformitatea cu reglementările, prin urmărirea evoluțiilor tehnologice și a schimbărilor legislative;
- Realizează audituri periodice pentru a verifica respectarea politicilor și procedurilor de securitate și conformitate și pentru a identifica și remedia eventualele probleme;

- Asigură raportarea incidentelor de securitate și analizează cauzele și implicațiile acestora, pentru a dezvolta soluții de îmbunătățire a sistemelor și procedurilor de securitate;
- Altele în conformitate cu fișa postului.

1.3.1. Expert Securitate Cibernetică:
Expertul cu Securitatea Cibernetică este responsabil pentru identificarea și monitorizarea riscurilor de securitate cibernetică și implementarea măsurilor de protecție adecvate pentru a preveni atacurile cibernetice și a asigura integritatea sistemelor informatice ale primăriei. Acesta trebuie să fie la curent cu cele mai noi tehnologii și tendințe din domeniul securității cibernetice și să își adapteze strategiile și planurile în consecință. Expertul în securitate cibernetică trebuie să:
- Elaboreze politici de securitate cibernetică;
- Gestioneze controalele de securitate cibernetică;
- asigure conformitatea cu standardele de securitate cibernetică relevante;
- Efectueze teste de penetrare;
- Analizeze rapoartele de securitate cibernetică pentru a identifica punctele vulnerabile ale sistemelor informatice și să ia măsuri pentru a le proteja;
- Colaboreze cu celelalte echipe din cadrul departamentului IT;
- Ofere formare și suport pentru a asigura un nivel adecvat de securitate cibernetică în întreaga primărie;
- Altele în conformitate cu fișa postului.

1.3.2. Asistent Securitate Cibernetică:
Rolul Asistentului de Securitate Cibernetică este de a asista Expertul de Securitate Cibernetică în monitorizarea și evaluarea riscurilor de securitate cibernetică și în implementarea măsurilor de protecție. În special, responsabilitățile sale includ următoarele:
- Monitorizarea sistemului de antivirus: asistentul de securitate cibernetică trebuie să verifice starea sistemului de antivirus și să se asigure că acesta este actualizat și funcționează corect pentru a detecta și preveni atacurile malware;
- Politici de securitate: asistentul de securitate cibernetică ajută la implementarea și menținerea politicilor de securitate cibernetică, inclusiv politici de autentificare, acces, criptare și gestionarea parolelor;
- Implementare Active Directory: asistentul de securitate cibernetică poate fi implicat în configurarea și administrarea serviciului Active Directory pentru a gestiona identitățile și accesul utilizatorilor în rețea;
- Asistență în incidente de securitate: asistentul de securitate cibernetică poate fi implicat în analiza și rezolvarea incidentelor de securitate cibernetică, inclusiv identificarea cauzelor și aplicarea de remedieri adecvate;
- Actualizarea și îmbunătățirea măsurilor de securitate: asistentul de securitate cibernetică poate fi implicat în evaluarea și îmbunătățirea măsurilor de securitate existente și în identificarea și implementarea de noi tehnologii și metode pentru a proteja rețeaua și sistemele informatice ale primăriei;
- Monitorizarea conformității: asistentul de securitate cibernetică ajută la monitorizarea conformității cu politici și reglementări de securitate cibernetică, inclusiv GDPR și alte legi și regulamente aplicabile în domeniul securității informatice;
- Altele în conformitate cu fișa postului.

1.3.3. Ofițer GDPR:
Ofițerul GDPR poate avea și alte atribuții în departamentul de IT, însă pe linia GDPR întreprinde următoarele:
- Asigură implementarea și respectarea regulamentului general privind protecția datelor cu caracter personal (GDPR) în cadrul primăriei și a altor reglementări specifice privind protecția datelor;
- Elaborează și implementează politici și proceduri privind protecția datelor personale, inclusiv evaluarea riscurilor și măsurile de securitate adecvate;

- Monitorizează implementarea acestor politici și proceduri și își asumă responsabilitatea pentru conformitatea cu reglementările aplicabile în domeniul protecției datelor;
- Acordă asistență și sfaturi cu privire la protecția datelor cu caracter personal pentru toți angajații din cadrul primăriei, inclusiv cu privire la drepturile persoanelor vizate;
- Colaborează cu alte departamente din cadrul primăriei pentru a asigura conformitatea cu GDPR și cu alte reglementări specifice privind protecția datelor;
- Altele în conformitate cu fișa postului.

1.4. Manager Proiecte și Transformare Digitală:
Managerul Proiecte și Transformare Digitală este responsabil pentru coordonarea și implementarea proiectelor de digitalizare și transformare digitală în cadrul primăriei. Acesta trebuie să aibă o viziune clară asupra direcției în care se îndreaptă organizația în ceea ce privește tehnologia și să fie capabil să gestioneze cu succes echipele de proiecte și resursele alocate. Mai precis, sarcinile principale ale Managerului Proiecte și Transformare Digitală includ:
- Identificarea oportunităților de digitalizare și îmbunătățire a proceselor prin utilizarea tehnologiei;
- Pregătirea cererilor de finanțare, a studiilor de fezabilitate pentru proiecte de transformare digitală, în mod individual, cu echipa din subordine sau cu asistență externă;
- Dezvoltarea și gestionarea bugetului și a resurselor alocate pentru proiecte;
- Asigurarea implementării cu succes a proiectelor și îndeplinirea obiectivelor de proiect;
- Identificarea și gestionarea riscurilor asociate cu proiectele și stabilirea măsurilor adecvate de reducere a riscurilor;
- Asigurarea comunicării adecvate și transparente cu toate părțile implicate în proiecte;
- Monitorizarea și raportarea progresului proiectelor;
- Asigurarea implementării adecvate a politicilor și procedurilor de management al proiectelor în cadrul departamentului IT;
- Coordonarea cu alte departamente din cadrul primăriei pentru a asigura alinierea și sincronizarea activităților de proiecte;
- Altele în conformitate cu fișa postului.

1.4.1. Expert GIS:
Gestionează și dezvoltă sistemele de informații geografice, integrând datele spațiale în aplicațiile și serviciile digitale ale primăriei. Responsabilitățile includ:
- Crearea și dezvoltarea de aplicații de informare geografică pentru utilizatori;
- Utilizarea tehnologiilor și a instrumentelor GIS pentru dezvoltarea de soluții personalizate pentru utilizatori;
- Actualizarea și menținerea bazei de date spațiale;
- Crearea de hărți, rapoarte și analize bazate pe datele spațiale;
- Identificarea și implementarea de noi tehnologii și produse în cadrul sistemelor de informare geografică;
- Altele în conformitate cu fișa postului.

1.4.2. Expert Arhivă Electronică:
Gestionează și menține arhiva electronică a primăriei, asigurând stocarea, accesibilitatea și securitatea documentelor digitale. Responsabilitățile includ:
- Crearea și menținerea arhivei electronice a documentelor în conformitate cu cerințele legale și cu politicile organizaționale;
- Asigurarea că toate documentele și datele sunt stocate într-un mod sigur și accesibil;
- Dezvoltarea și implementarea de politici și proceduri de gestionare a documentelor;
- Crearea și actualizarea de rapoarte și analize privind starea arhivei electronice;
- Altele în conformitate cu fișa postului.

1.4.3. Expert Management Sistem de Digitalizare:
Supervizează procesele de digitalizare a documentelor și coordonează implementarea soluțiilor digitale pentru optimizarea fluxurilor de lucru și automatizarea proceselor. Responsabilitățile includ:

- Implementarea sistemului de management al digitalizării;
- Dezvoltarea și implementarea de strategii și planuri pentru digitalizarea documentelor și proceselor în cadrul primăriei;
- Coordonarea procesului de digitalizare și asigurarea că toate documentele sunt convertite în format digital în conformitate cu cerințele legale și cu politicile organizaționale;
- Dezvoltarea și implementarea de soluții pentru optimizarea fluxurilor de lucru și automatizarea proceselor;
- Crearea și actualizarea de rapoarte și analize privind procesul de digitalizare și performanța sistemelor digitale;
- Altele în conformitate cu fișa postului.

1.5. Coordonator Soluții Informatice Dedicate:
Gestionează comunicarea și relațiile publice pentru departamentul IT, promovând serviciile digitale oferite de primărie și asigurând o comunicare eficientă cu publicul și mass-media. Responsabilitățile includ:

- Crearea și implementarea de strategii și planuri pentru promovarea serviciilor digitale ale primăriei;
- Crearea și actualizarea de conținut digital, precum și dezvoltarea și implementarea de campanii de marketing online;
- Gestionarea relațiilor cu publicul și mass-media în ceea ce privește serviciile digitale ale primăriei;
- Dezvoltarea și implementarea de sondaje și studii de piață pentru a evalua satisfacția utilizatorilor cu serviciile digitale ale primăriei.
- Altele în conformitate cu fișa postului.

1.5.1. Specialist Comunicare Digitală:
Concepe și implementează strategii de comunicare digitală, precum și crearea și promovarea conținutului digital pentru canalele de comunicare ale primăriei. Prin alte sarcini include:

- Identifică canale noi de comunicare și promovare a serviciilor digitale ale primăriei;
- Creează și administrează conținutul de pe paginile web ale primăriei, de pe rețelele sociale (Facebook, Twitter, Instagram, etc.) și de pe alte canale digitale;
- Gestionează campanii de promovare a serviciilor și proiectelor digitale ale primăriei;
- Analizează datele de trafic și interacțiune cu utilizatorii pentru a optimiza strategiile de comunicare digitală;
- Asigură interacțiunea cu publicul prin intermediul canalelor digitale, răspunzând la întrebări și feedback-ul utilizatorilor și colaborând cu celelalte departamente din primărie pentru a îmbunătăți serviciile oferite;
- Altele în conformitate cu fișa postului.

1.5.2. Asistent Comunicare și Suport Tehnic:
Oferă asistență în comunicarea digitală și susține echipa în activitățile de relații publice, precum și în oferirea suportului tehnic utilizatorilor și publicului. Printre alte atribuții menționăm:

- Asigură suport tehnic utilizatorilor în ceea ce privește utilizarea serviciilor digitale ale primăriei și în rezolvarea problemelor tehnice;
- Susține echipa de comunicare digitală în crearea și promovarea conținutului digital;
- Colaborează cu celelalte departamente din primărie pentru a îmbunătăți serviciile oferite și pentru a identifica noi nevoi ale utilizatorilor;
- Asigură interacțiunea cu publicul prin intermediul canalelor digitale, răspunzând la întrebări și feedback-ul utilizatorilor;
- Altele în conformitate cu fișa postului.

Este de asemenea important să se ia în considerare că ajustările, actualizările sau diversificările acestor roluri pot fi necesare în orice moment, în funcție de noile nevoi ale primăriei și a schimbărilor din domeniul IT. În general, aceste ajustări se fac în urma unei analize atente a activităților și a rezultatelor obținute, iar decizia finală este luată în urma unei discuții și aprobării din partea directorului IT și a altor factori decizionali relevanți.

Colaborarea între rolurile din organigramă

În cazul situațiilor critice sau de urgență, colaborarea între diferitele funcții din organigrama departamentului IT este esențială pentru asigurarea continuității operaționale a primăriei. În astfel de situații, coordonarea activităților și comunicarea între membrii echipei trebuie să fie foarte bine organizată și să se desfășoare într-un mod rapid și eficient.

În general, responsabilitățile echipei IT se împart în funcție de natura situației. În cazul unei defecțiuni tehnice sau a unei probleme legate de infrastructură, managerul infrastructurii și suportului tehnic și administratorul sistemului vor fi responsabili pentru identificarea problemei și remedierea acesteia. În cazul unei probleme legate de securitate, expertul în securitate cibernetică va fi responsabil pentru identificarea și prevenirea oricăror atacuri cibernetice, iar ofițerul GDPR va asigura conformitatea cu reglementările privind protecția datelor personale.

De asemenea, în cazul situațiilor critice, este important ca echipa să colaboreze cu celelalte departamente ale primăriei pentru a asigura că toate nevoile și cerințele sunt îndeplinite în timp util. În astfel de situații, se poate institui o sală de criză unde reprezentanții din diferite departamente și funcții se pot întâlni și colabora pentru a găsi soluții eficiente și rapide.

Pe lângă aceste măsuri, echipa IT poate lua și alte măsuri de precauție pentru a se asigura că este pregătită să facă față situațiilor critice. Aceste măsuri pot include dezvoltarea unui plan de gestionare a situațiilor de urgență, pregătirea resurselor de backup și implementarea unor soluții de securitate suplimentare pentru a preveni eventuale atacuri cibernetice sau defecțiuni tehnice.

În cazul unor situații critice, cum ar fi atacurile cibernetice sau pierderea datelor, toate funcțiile trebuie să colaboreze îndeaproape pentru a gestiona situația și a minimiza impactul asupra primăriei și comunității sale. Este important ca toți membrii echipei să fie pregătiți să acționeze rapid și eficient în astfel de situații, iar managerul de proiecte și transformare digitală să coordoneze eforturile pentru a asigura o soluție adecvată și promptă.

În cazul proiectelor de transformare digitală din primărie, colaborarea între diferitele funcții din organigramă este esențială pentru pregătirea, implementarea și asigurarea sustenabilității acestora. Primul pas este identificarea nevoii de transformare digitală și stabilirea obiectivelor proiectului de către managerul de proiecte și transformare digitală. Expertul în securitate cibernetică și asistentul de securitate cibernetică trebuie implicați încă de la începutul proiectului pentru a asigura securitatea sistemelor și a datelor.

În timpul procesului de implementare, managerul de proiecte și transformare digitală trebuie să colaboreze strâns cu responsabilul GDPR pentru a se asigura că toate aspectele de protecție a datelor cu caracter personal sunt luate în considerare. În același timp, managerul trebuie să colaboreze cu directorul IT și echipa sa pentru a asigura implementarea eficientă a soluțiilor digitale și integrarea acestora cu sistemele existente.

După finalizarea proiectului, asigurarea sustenabilității soluțiilor digitale devine responsabilitatea managerului de proiecte și transformare digitală, în colaborare cu directorul IT și echipa sa. Expertul în securitate cibernetică și asistentul de securitate cibernetică trebuie să asigure securitatea sistemelor și a datelor în continuare, iar responsabilul GDPR trebuie să se asigure că procesele de protecție a datelor cu caracter personal sunt respectate.

Pentru rolurile din organigramă trebuie elaborate fișele de post. O fișă de post este un document care descrie în detaliu responsabilitățile, cerințele și sarcinile specifice asociate cu un anumit loc de muncă. Acest document este utilizat în procesul de recrutare și selecție pentru a asigura că candidații care aplică pentru un anumit post sunt potriviți pentru acesta. De asemenea, fișa de post servește și ca un instrument de evaluare a performanței angajaților, întrucât definește așteptările și criteriile de performanță pentru acel post. În general, o fișă de post conține următoarele informații:

- Titlul postului
- Scopul și obiectivele postului
- Responsabilitățile și sarcinile specifice ale postului
- Cerințele de calificare și experiență
- Competențele și abilitățile necesare pentru a realiza sarcinile postului
- Indicatorii de performanță și criteriile de evaluare a performanței
- Informații despre beneficiile, compensațiile și alte avantaje ale postului
- Programul de lucru, orele și orice alte detalii specifice ale postului.

Fișa de post trebuie elaborată de către managerul departamentului IT în colaborare cu departamentul de resurse umane ale primăriei și este actualizată periodic în funcție de nevoile primăriei și de modificările postului. Deoarece nu este în cerințele prezentului proiect să definim fișele de post pentru rolurile din organigrama propusă, cu scop orientativ prezentăm mai jos fișa postului pentru Director IT în cadrul Primăriei Bistrița:

- Titlul postului: Director IT
- Scopul și obiectivele postului: Coordonează și supervizează întregul departament IT, asigură implementarea și mentenanța tehnologiei și elaborează strategia departamentului IT în cadrul primăriei.
- Responsabilitățile și sarcinile specifice ale postului: conform celor deja prezentate
  Responsabilitățile includ planificarea, coordonarea și supervizarea întregului departament IT al primăriei. Directorul IT asigură implementarea și mentenanța tehnologiei în cadrul primăriei și este responsabil pentru elaborarea strategiei departamentului IT. Directorul IT trebuie să aibă o înțelegere profundă a tehnologiilor și tendințelor IT, precum și o perspectivă largă asupra impactului tehnologic asupra organizației și a modului în care tehnologia poate fi folosită pentru a îmbunătăți serviciile oferite către cetățeni și angajați. Directorul IT trebuie să colaboreze strâns cu ceilalți directori din primărie pentru a identifica nevoile și oportunitățile în ceea ce privește utilizarea tehnologiei în diferite departamente și proiecte. Printre responsabilitățile directorului IT se numără:
  - Planificarea și coordonarea activităților de implementare și mentenanță a infrastructurii IT, inclusiv rețele, echipamente hardware și software, servicii de comunicare și stocare de date;
  - Coordonarea dezvoltării și implementării aplicațiilor software personalizate, bazelor de date și sistemelor de informații geografice;
  - Asigurarea securității informațiilor și conformității cu regulamentele și politicile de securitate cibernetică și protecție a datelor personale;
  - Identificarea și gestionarea riscurilor de securitate cibernetică și prevenirea atacurilor cibernetice;
  - Supervizarea proiectelor de transformare digitală și implementarea soluțiilor digitale pentru optimizarea fluxurilor de lucru și serviciilor oferite către cetățeni;
  - Coordonarea și supervizarea echipei de IT, asigurându-se de dezvoltarea profesională a membrilor echipei și de buna lor colaborare;
  - Comunicarea și colaborarea strânsă cu ceilalți directori din primărie, precum și cu furnizorii de servicii IT, pentru a identifica nevoile și oportunitățile în ceea ce privește utilizarea tehnologiei în diferite departamente și proiecte;
  - Asigurarea bugetului departamentului IT, urmărirea cheltuielilor și monitorizarea resurselor și performanțelor departamentului;

- Cerințele de calificare și experiență: Studii superioare în domeniul IT, cel puțin 5 ani de experiență într-un rol de conducere în IT, cunoștințe avansate în tehnologii și tendințe IT, experiență în gestionarea proiectelor de transformare digitală.
- Competențele și abilitățile necesare pentru a realiza sarcinile postului: Capacitatea de a lidera și coordona echipe, gândire strategică, abilități de comunicare și colaborare, adaptabilitate, capacitate de a identifica și gestiona riscuri, competențe analitice și de planificare.
- Indicatorii de performanță și criteriile de evaluare a performanței: Realizarea obiectivelor IT, implementarea proiectelor în termenele stabilite, nivelul de satisfacție al angajaților și cetățenilor, eficiența operațională și financiară a departamentului IT, nivelul de securitate și conformitate în domeniul IT.
- Informații despre beneficiile, compensațiile și alte avantaje ale postului: Salariu competitiv, pachet de beneficii, oportunități de dezvoltare profesională, mediu de lucru dinamic și provocator.
- Programul de lucru, orele și orice alte detalii specifice ale postului: Program de lucru normal, 8 ore pe zi, de luni până vineri, cu posibilitatea de a lucra suplimentar în cazul unor proiecte sau situații de urgență.

Viziunea rezultatului ideal final pentru reper de comparație în transformare digitală

O primărie puternic digitalizată și cu un grad ridicat de transformare digitală este aceea care își optimizează și eficientizează serviciile pentru cetățeni prin intermediul tehnologiei și inovării. O astfel de primărie își poate îmbunătăți semnificativ operațiunile și interacțiunile cu cetățenii. Iată câteva aspecte esențiale care caracterizează o astfel de primărie:

- Infrastructura digitală: O primărie digitalizată are o infrastructură tehnologică solidă, incluzând o rețea de internet de mare viteză, servere securizate și dispozitive inteligente. Această infrastructură permite accesul rapid și sigur la informații și servicii pentru cetățeni și angajați.
- Platformă online: O primărie digitalizată dispune de o platformă online accesibilă și ușor de utilizat. Această platformă permite cetățenilor să acceseze servicii, să obțină informații și să efectueze diverse operațiuni, cum ar fi plata taxelor, înregistrarea proprietăților, solicitarea autorizațiilor de construcție și multe altele.
- Automatizarea proceselor: Procesele interne ale primăriei sunt optimizate și automatizate, reducând astfel timpul și efortul necesar pentru îndeplinirea sarcinilor. Automatizarea poate fi realizată prin intermediul sistemelor de management al documentelor, soluțiilor de colaborare și a inteligenței artificiale.
- Transparență și deschidere: O primărie digitalizată este transparentă și oferă acces la informații publice printr-o platformă de date deschise. Cetățenii pot vizualiza și descărca date privind cheltuielile publice, proiectele de dezvoltare și alte informații relevante.
- Comunicare și interacțiune: Primăria digitalizată oferă canale de comunicare eficiente și moderne, cum ar fi rețele de socializare, aplicații mobile și chatbots, care permit cetățenilor să comunice cu reprezentanții primăriei și să obțină răspunsuri rapide la întrebări și probleme.
- Servicii personalizate: Cu ajutorul analizei datelor și a tehnologiei, primăria digitalizată poate oferi servicii personalizate cetățenilor, adaptate nevoilor și preferințelor acestora.
- Smart City și IoT: O primărie avansată în transformarea digitală poate implementa proiecte de Smart City și soluții IoT (Internet of Things) pentru a îmbunătăți calitatea vieții și a eficientiza utilizarea resurselor urbane, cum ar fi iluminatul public, managementul traficului și colectarea deșeurilor.
- Capacități de analiză a datelor: Prin colectarea și analiza datelor, primăria poate identifica tendințele și problemele existente în comunitate, astfel încât să poată lua decizii informate și să dezvolte politici eficiente. Instrumentele de analiză a datelor pot ajuta primăria să evalueze performanța serviciilor și să identifice domenii care necesită îmbunătățiri.
- Educație și formare digitală: O primărie digitalizată investește în dezvoltarea competențelor digitale ale angajaților și cetățenilor. Acest lucru poate fi realizat prin organizarea de cursuri, ateliere și programe de formare care vizează îmbunătățirea abilităților digitale și promovarea utilizării tehnologiei în viața de zi cu zi.

- Securitate și protecția datelor: O primărie puternic digitalizată pune un accent deosebit pe securitatea cibernetică și protecția datelor personale ale cetățenilor. Aceasta implementează măsuri de securitate adecvate pentru a preveni atacurile cibernetice și a asigura confidențialitatea informațiilor.
- Parteneriate și colaborare: O primărie avansată în transformarea digitală colaborează cu alte entități guvernamentale, organizații non-guvernamentale, sectorul privat și comunitățile locale pentru a dezvolta și implementa soluții inovatoare și eficiente. Aceste parteneriate pot stimula creșterea economică și dezvoltarea durabilă în comunitate.
- Agilitate și adaptabilitate: O primărie digitalizată este capabilă să se adapteze rapid la schimbări și să adopte noi tehnologii și practici. Aceasta încurajează inovația și gândește în mod proactiv, luând în considerare evoluțiile tehnologice și nevoile în continuă schimbare ale cetățenilor.

O primărie puternic digitalizată și cu un grad ridicat de transformare digitală își îmbunătățește constant serviciile și operațiunile prin tehnologie și inovație, oferind cetățenilor acces ușor și rapid la informații și servicii, sporind transparența și eficiența.

Descrierea unor situații posibile între cetățean și o primărie puternic digitalizată

În continuare se prezintă o serie de situații care vizualizează unde trebuie să se ajungă cu efortul de digitalizare și transformare digitală a primăriei. Aceste scenarii ilustrează diverse tipuri de interacțiuni pe care cetățenii le pot avea cu o primărie digitalizată și eficientă. Prin implementarea unor astfel de soluții, primăriile pot îmbunătăți calitatea și accesibilitatea serviciilor oferite, reducând birocrația și oferind o experiență mai plăcută cetățenilor. Situațiile nu sunt comprehensive, ci doar orientative.

O listă exhaustivă a tuturor situațiilor de interacțiune între cetățeni și primărie este dificil de realizat, deoarece acestea variază în funcție de necesitățile și contextul local. Cu toate acestea, mai jos este elaborată o listă cu multe dintre interacțiunile comune pe care le-ar putea avea cetățenii cu primăria:

1. Plata taxelor și impozitelor.
2. Obținerea autorizațiilor de construcție.
3. Rezervarea sălii de sport sau altor facilități publice.
4. Raportarea problemelor legate de infrastructură, cum ar fi gropi, iluminat defectuos sau semne de circulație deteriorate.
5. Participarea la consultări publice și procesul decizional local.
6. Înregistrarea animalelor de companie.
7. Solicitarea ajutoarelor sociale sau a altor forme de asistență.
8. Înscrierea copiilor la grădiniță sau școală.
9. Rezervarea locurilor de parcare.
10. Actualizarea cărții de identitate.
11. Depunerea unei cereri pentru obținerea de informații publice.
12. Deschiderea unei activități comerciale pe un spațiu public.
13. Organizarea unui marș de protest sau a altor adunări publice.
14. Reclamarea comportamentelor neadecvate ale angajaților primăriei.
15. Înscrierea în programe de voluntariat și implicarea în proiecte comunitare.
16. Obținerea de autorizații pentru organizarea de evenimente în spațiul public.
17. Solicitarea informațiilor referitoare la planurile urbanistice și zonele protejate.
18. Înregistrarea și transferul dreptului de proprietate asupra unui imobil.
19. Obținerea certificatelor de urbanism și de atestare a conformității construcțiilor.
20. Înregistrarea căsătoriei, nașterii sau decesului.
21. Obținerea certificatelor de rezidență sau de domiciliu.
22. Înregistrarea și modificarea datelor privind starea civilă.

23. Solicitarea de autorizații pentru desfășurarea de activități economice specifice (de exemplu, terase, taximetrie, etc.).
24. Înregistrarea și gestionarea contractelor de închiriere pentru locuințele sociale.
25. Obținerea autorizațiilor de mediu și rapoartelor privind impactul asupra mediului.
26. Înregistrarea și gestionarea solicitărilor privind serviciile de salubritate.
27. Participarea în programe de educație și informare în domeniul protecției mediului.
28. Înregistrarea și gestionarea solicitărilor de intervenție a serviciilor de urgență.
29. Depunerea de petiții și propuneri de inițiative cetățenești.
30. Obținerea de informații și înscrierea în programe de formare profesională sau cursuri de dezvoltare personală organizate de primărie.
31. Înregistrarea pentru votul prin corespondență sau schimbarea secției de votare.
32. Participarea la programe de prevenire și sănătate publică.
33. Solicitarea ajutorului pentru victimele violenței domestice sau alte situații de risc.
34. Înregistrarea și gestionarea solicitărilor pentru serviciile de asistență socială și consiliere.
35. Participarea la programe de sprijin pentru antreprenorii locali și dezvoltarea afacerilor.
36. Înregistrarea și gestionarea sesizărilor privind nerespectarea normelor de conviețuire și siguranță publică.
37. Obținerea de informații și înscrierea în programele culturale, sportive și recreative organizate de primărie.
38. Solicitarea de informații și înscrierea în programe de sprijin pentru accesul la locuințe.
39. Înregistrarea și gestionarea solicitărilor privind transportul în comun și serviciile de mobilitate.
40. Raportarea și gestionarea sesizărilor privind degradarea patrimoniului cultural și istoric.
41. Participarea la proiecte de parteneriat public-privat pentru dezvoltarea locală.
42. Înregistrarea și gestionarea solicitărilor de intervenție pentru îmbunătățirea spațiilor verzi și amenajarea parcurilor.
43. Solicitarea și obținerea de informații despre oportunitățile de finanțare și granturi disponibile pentru proiecte locale.
44. Aflarea aprobărilor de construcții într-o zonă a orașului de către orice cetățean pentru a limita frauda
45. Înregistrarea copilului la școală sau la grădiniță

Aceasta este o listă cuprinzătoare, dar nu exhaustivă, deoarece interacțiunile pot varia în funcție de legislația și reglementările locale, precum și de nevoile specifice ale comunității.

Scenariu 1: Plata taxelor și impozitelor online Maria este o cetățeancă care dorește să-și plătească taxele și impozitele anuale. Accesează platforma online a primăriei și se autentifică cu ajutorul unui cont de utilizator. Navighează prin meniuri și găsește secțiunea dedicată plății taxelor. Aici, ea poate verifica suma datorată și poate efectua plata direct prin intermediul platformei, folosind un card bancar sau un sistem de plăți online. Maria primește o confirmare a plății și poate descărca chitanța în format PDF.

Scenariu 2: Obținerea unei autorizații de construcție Ion deține un teren pe care dorește să construiască o casă. Pentru a obține autorizația de construcție, Ion accesează platforma online a primăriei și completează un formular electronic cu datele personale, detaliile terenului și proiectul de construcție. Încarcă documentele necesare în format digital și trimite cererea. Ulterior, Ion primește notificări prin e-mail cu privire la progresul cererii și, în cele din urmă, un răspuns cu privire la aprobarea autorizației.

Scenariu 3: Rezervarea unei săli de sport Ana este profesor de fitness și dorește să organizeze un eveniment sportiv într-o sală de sport administrată de primărie. Ea accesează platforma online, verifică disponibilitatea sălii și rezervă data și ora dorită. După ce efectuează plata taxei de închiriere, Ana primește o confirmare a rezervării și un cod QR pe e-mail, pe care îl va prezenta la intrarea în sala de sport.

Scenariu 4: Raportarea unei probleme legate de infrastructură Mihai observă o groapă periculoasă în drumul din fața casei sale și dorește să raporteze problema primăriei. Accesează aplicația mobilă a primăriei și selectează opțiunea "Raportează o problemă". Folosind GPS-ul telefonului, Mihai marchează locația exactă a problemei și atașează o fotografie. Descrie problema în câteva cuvinte și trimite raportul. Ulterior, Mihai primește o notificare când problema a fost rezolvată.

Scenariu 5: Participarea la consultări publice Elena este o cetățeancă activă și dorește să participe la procesul decizional local. Pe platforma online a primăriei, ea găsește informații despre proiectele de dezvoltare urbană și consultările publice. Se înregistrează pentru a participa la un webinar despre un proiect de amenajare a unui parc în cartierul său. În timpul webinarului, Elena poate adresa întrebări și își poate exprima opinia și preocupările legate de proiect. Ulterior, rezultatele consultării sunt publicate pe platforma online, iar Elena poate vedea cum contribuția ei a fost luată în considerare în planul final.

Scenariu 6: Înregistrarea unui animal de companie Andrei are un câine nou și dorește să-l înregistreze la primărie, conform reglementărilor locale. Se conectează la platforma online și completează un formular cu datele personale și informațiile despre câine, inclusiv rasa, vârsta, sexul și numărul de microcip. Andrei primește un certificat digital de înregistrare, pe care îl poate descărca și printa pentru a-l păstra în arhiva personală.

Scenariu 7: Solicitarea unui ajutor social Laura este o mamă singură care are nevoie de asistență financiară din partea primăriei pentru a-și crește copilul. Accesează platforma online a primăriei și găsește informații despre diferitele programe de asistență socială disponibile. Laura completează un formular cu informațiile necesare și atașează documentele solicitate. După evaluarea cererii, Laura primește un răspuns prin e-mail cu privire la eligibilitatea și cuantumul ajutorului acordat.

Scenariu 8: Înscrierea copilului la grădiniță Cristina dorește să-și înscrie copilul la grădinița locală administrată de primărie. Pe platforma online, ea găsește lista grădinițelor și numărul de locuri disponibile pentru anul următor. Cristina completează un formular de înscriere cu datele personale și preferințele sale legate de grădiniță. După ce a trimis cererea, Cristina primește un e-mail de confirmare și va fi notificată în momentul în care se va face repartizarea locurilor.

Scenariu 9: Rezervarea locurilor de parcare Adrian dorește să rezerve un loc de parcare în apropierea locuinței sale. Accesează platforma online a primăriei și navighează în secțiunea dedicată parcărilor. Verifică disponibilitatea locurilor și selectează perioada de timp pentru care dorește să rezerve parcare. Efectuează plata taxei aferente și primește un permis digital pe e-mail, pe care îl va afișa în parbrizul mașinii.

Scenariu 10: Actualizarea cărții de identitate Carmen are nevoie să-și actualizeze cartea de identitate, deoarece a expirat. Accesează platforma online a primăriei și completează un formular cu datele personale și motivele actualizării. Încarcă o fotografie recentă și atașează o copie a documentelor necesare. Primește o programare la ghișeul de evidență a persoanelor, unde se va prezenta cu documentele originale pentru a finaliza procesul.

Scenariu 11: Depunerea unei cereri pentru informații publice Bogdan este jurnalist și dorește să obțină informații despre un proiect de infrastructură finanțat de primărie. Accesează platforma online și completează un formular de solicitare a informațiilor publice, specificând datele și documentele de interes. După evaluarea cererii, Bogdan primește informațiile solicitate în format electronic, pe care le poate utiliza pentru a realiza un material jurnalistic.

Scenariu 12: Deschiderea unei activități comerciale pe un spațiu public Irina dorește să deschidă un chioșc de alimentație pe o alee pietonală din oraș. Accesează platforma online a primăriei și completează un formular de cerere pentru autorizația de funcționare a chioșcului. Atașează un

plan al spațiului, un meniu și alte documente solicitate. După ce autorizația este aprobată, Irina poate începe să-și desfășoare activitatea comercială în conformitate cu reglementările locale.

Scenariu 13: Organizarea unui marș de protest Oana și un grup de cetățeni doresc să organizeze un marș de protest în centrul orașului. Accesează platforma online a primăriei și completează un formular de notificare a adunării publice, specificând data, ora, locul și scopul protestului. Primăria verifică cererea și emite o autorizație, asigurându-se că evenimentul respectă normele de siguranță și ordine publică.

Scenariu 14: Reclamarea comportamentelor neadecvate ale angajaților din primărie Diana a avut o experiență neplăcută cu un angajat al primăriei și dorește să depună o reclamație. Accesează platforma online a primăriei și găsește secțiunea dedicată reclamațiilor și sesizărilor. Completează un formular în care descrie incidentul, specifică numele angajatului și atașează orice dovadă relevantă, cum ar fi fotografii sau înregistrări. Trimite reclamația, iar primăria își asumă responsabilitatea de a investiga incidentul și a lua măsurile adecvate. Diana primește ulterior un răspuns prin e-mail care explică acțiunile întreprinse în urma sesizării sale.

Scenariu 15: Înscrierea în programe de voluntariat și implicarea în proiecte comunitare Ana dorește să se implice într-un proiect de voluntariat pentru a ajuta la amenajarea unui parc în cartierul său. Accesează platforma online a primăriei și caută secțiunea dedicată programelor de voluntariat. Se înscrie în proiectul dorit și primește un e-mail de confirmare cu detalii despre data, ora și locul de întâlnire pentru a participa la activitate.

Scenariu 16: Obținerea autorizațiilor pentru organizarea de evenimente în spațiul public Mihai dorește să organizeze un concert în aer liber într-un parc local. Accesează platforma online a primăriei și completează un formular pentru obținerea autorizației necesare, specificând data, ora, locația și detaliile evenimentului. După ce primăria aprobă cererea, Mihai primește autorizația în format electronic și poate începe să pregătească evenimentul.

Scenariu 17: Solicitarea informațiilor referitoare la planurile urbanistice și zonele protejate Laura intenționează să construiască o casă și dorește să afle dacă terenul ales se află într-o zonă protejată. Accesează platforma online a primăriei și navighează către secțiunea cu informații despre planurile urbanistice și zonele protejate. Introduce adresa terenului și primește informațiile necesare, care îi permit să înțeleagă dacă proiectul său este viabil în acea zonă.

Scenariu 18: Înregistrarea și transferul dreptului de proprietate asupra unui imobil Andrei tocmai și-a vândut apartamentul și dorește să transfere dreptul de proprietate către noul proprietar. Accesează platforma online a primăriei și completează un formular pentru transferul de proprietate, atașând documentele necesare, cum ar fi contractul de vânzare-cumpărare. După ce transferul este procesat, noul proprietar primește o confirmare a înregistrării dreptului de proprietate.

Scenariu 19: Obținerea certificatelor de urbanism și de atestare a conformității construcțiilor Ion dorește să extindă casa sa și are nevoie de un certificat de urbanism și de atestare a conformității construcției. Accesează platforma online a primăriei și completează formularul necesar, atașând planurile și documentele solicitate. Odată ce cererea este aprobată, Ion primește certificatul în format electronic, pe care îl poate folosi pentru a demara lucrările de construcție.

Scenariu 20: Înregistrarea căsătoriei, nașterii sau decesului Gabriela dorește să înregistreze nașterea fiicei sale. Accesează platforma online a primăriei și completează formularul necesar pentru înregistrarea nașterii, atașând certificatul medical eliberat de spital și alte documente solicitate. Gabriela primește un e-mail de confirmare a înregistrării nașterii, iar certificatul de naștere al fiicei sale este trimis în format electronic sau prin poștă, în funcție de preferințele sale.

Scenariu 21: Obținerea certificatelor de rezidență sau de domiciliu Sorin are nevoie de un certificat de rezidență pentru a dovedi că locuiește într-un anumit oraș. Accesează platforma online a primăriei și completează un formular pentru obținerea certificatului, atașând documentele necesare, cum ar fi copia cărții de identitate. Odată ce cererea este procesată, Sorin primește certificatul de rezidență în format electronic sau prin poștă, în funcție de preferințele sale.

Scenariu 22: Înregistrarea și modificarea datelor privind starea civilă Elena s-a căsătorit recent și dorește să-și schimbe numele de familie în documentele oficiale. Accesează platforma online a primăriei și completează un formular pentru modificarea datelor privind starea civilă, atașând certificatul de căsătorie și o copie a cărții de identitate. După ce cererea este procesată, Elena primește un e-mail de confirmare și poate solicita actualizarea cărții de identitate cu noul nume de familie.

Scenariu 23: Solicitarea de autorizații pentru desfășurarea de activități economice specifice Marius dorește să deschidă o terasă în centrul orașului. Accesează platforma online a primăriei și completează formularul necesar pentru obținerea autorizației, atașând documentele solicitate și planurile terasei. După ce cererea este aprobată, Marius primește autorizația în format electronic și poate începe să amenajeze și să exploateze terasa.

Scenariu 24: Înregistrarea și gestionarea contractelor de închiriere pentru locuințele sociale Ioana se află pe lista de așteptare pentru o locuință socială și a primit recent o ofertă. Accesează platforma online a primăriei și completează formularul necesar pentru a semna contractul de închiriere, atașând documentele solicitate. După ce contractul este procesat, Ioana primește o copie în format electronic și poate să se mute în noua locuință.

Scenariu 25: Obținerea autorizațiilor de mediu și rapoartelor privind impactul asupra mediului Bogdan intenționează să construiască o fabrică și are nevoie de o autorizație de mediu și de un raport privind impactul asupra mediului. Accesează platforma online a primăriei și completează formularele necesare, atașând documentele și planurile solicitate. Odată ce cererea este aprobată, Bogdan primește autorizația și raportul în format electronic, iar lucrările de construcție pot începe.

Scenariu 26: Înregistrarea și gestionarea solicitărilor privind serviciile de salubritate Alexandra observă că strada sa nu a fost curățată în ultimele zile. Accesează platforma online a primăriei și completează un formular pentru a raporta problema privind serviciile de salubritate. Primăria procesează cererea și trimite o echipă de curățenie în zona indicată.

Scenariu 27: Participarea în programe de educație și informare în domeniul protecției mediului Cristina este pasionată de protecția mediului și dorește să se implice în programe de educație și informare organizate de primărie. Accesează platforma online a primăriei și se înscrie la un curs despre reciclare și gestionarea deșeurilor. Primește un e-mail cu detaliile cursului și participă la sesiunile de instruire.

Scenariu 28: Înregistrarea și gestionarea solicitărilor de intervenție a serviciilor de urgență Petre observă o situație de urgență în cartierul său, cum ar fi un incendiu sau o inundație. Accesează platforma online a primăriei și completează un formular pentru a raporta situația și a solicita intervenția serviciilor de urgență. Echipele de intervenție sunt alertate și se deplasează în zona indicată pentru a gestiona situația.

Scenariu 29: Depunerea de petiții și propuneri de inițiative cetățenești Nicolae dorește să propună o inițiativă pentru construirea unui nou parc în zona sa. Accesează platforma online a primăriei și completează un formular pentru a depune o petiție sau o propunere de inițiativă cetățenească. Primăria analizează propunerea și, în funcție de susținerea comunității și de resursele disponibile, poate decide să includă proiectul în planurile de dezvoltare urbană.

Scenariu 30: Obținerea de informații și înscrierea în programe de formare profesională sau cursuri de dezvoltare personală organizate de primărie Loredana este în căutarea unui curs de dezvoltare personală sau de formare profesională organizat de primărie. Accesează platforma online a primăriei și navighează către secțiunea dedicată programelor de formare și cursurilor. Alege un curs care i se potrivește și se înscrie, primind ulterior un e-mail cu detalii despre data, ora și locul desfășurării cursului.

Scenariu 31: Înregistrarea pentru votul prin corespondență sau schimbarea secției de votare Dan este plecat din țară în perioada alegerilor și dorește să voteze prin corespondență. Accesează platforma online a primăriei și completează formularul necesar, atașând o copie a cărții sale de identitate și alte documente solicitate. După ce cererea este aprobată, Dan primește pachetul de vot prin corespondență și își poate exercita dreptul la vot.

Scenariu 32: Participarea la programe de prevenire și sănătate publică Adriana vrea să se implice în programe de prevenire și sănătate publică organizate de primărie. Accesează platforma online a primăriei, se informează despre programele disponibile și se înscrie la unul dintre ele. Primește un e-mail cu detaliile programului și participă la sesiunile de instruire și activitățile propuse.

Scenariu 33: Solicitarea ajutorului pentru victimele violenței domestice sau alte situații de risc Camelia este victimă a violenței domestice și are nevoie de ajutor și protecție. Accesează platforma online a primăriei și completează un formular pentru a solicita sprijin. Serviciile sociale ale primăriei o contactează și o direcționează către resursele și serviciile disponibile pentru a o ajuta să iasă din situația de risc.

Scenariu 34: Înregistrarea și gestionarea solicitărilor pentru serviciile de asistență socială și consiliere Mihaela trece printr-o perioadă dificilă și are nevoie de consiliere și sprijin. Accesează platforma online a primăriei și completează un formular pentru a solicita serviciile de asistență socială și consiliere. Este contactată de un consilier social și participă la ședințe de consiliere pentru a-și îmbunătăți situația.

Scenariu 35: Participarea la programe de sprijin pentru antreprenorii locali și dezvoltarea afacerilor Florin este antreprenor și dorește să își dezvolte afacerea locală. Accesează platforma online a primăriei și se înscrie într-un program de sprijin pentru antreprenori. Participă la cursuri de formare și mentorat pentru a învăța cum să își crească afacerea și să beneficieze de oportunitățile locale.

Scenariu 36: Înregistrarea și gestionarea sesizărilor privind nerespectarea normelor de conviețuire și siguranță publică Laura observă că vecinii săi deranjează liniștea publică și nu respectă normele de conviețuire. Accesează platforma online a primăriei și completează un formular pentru a raporta problemele întâmpinate. Primăria analizează sesizarea și trimite o echipă de control pentru a evalua situația și a lua măsurile necesare pentru restabilirea liniștii și respectarea normelor.

Scenariu 37: Obținerea de informații și înscrierea în programele culturale, sportive și recreative organizate de primărie Andrei vrea să se înscrie într-un program sportiv organizat de primărie. Accesează platforma online a primăriei, caută informații despre programele disponibile și se înscrie într-unul dintre ele. Primește un e-mail cu detaliile programului și participă la activitățile sportive propuse.

Scenariu 38: Solicitarea de informații și înscrierea în programe de sprijin pentru accesul la locuințe Elena caută o locuință accesibilă și dorește să beneficieze de un program de sprijin pentru accesul la locuințe. Accesează platforma online a primăriei, se informează despre programele disponibile și se înscrie într-unul dintre ele. Primește un e-mail cu detaliile programului și urmează pașii necesari pentru a accesa locuința dorită.

Scenariu 39: Înregistrarea și gestionarea solicitărilor privind transportul în comun și serviciile de mobilitate Mihai are nevoie de informații despre transportul în comun și serviciile de mobilitate disponibile în oraș. Accesează platforma online a primăriei și caută informații despre rute, tarife și orare. Dacă are nevoie de asistență sau vrea să facă o sesizare, completează un formular online și primește răspuns în cel mai scurt timp posibil.

Scenariu 40: Raportarea și gestionarea sesizărilor privind degradarea patrimoniului cultural și istoric Diana observă că un monument istoric din oraș este în stare de degradare. Accesează platforma online a primăriei și completează un formular pentru a raporta problema. Primăria analizează sesizarea și ia măsurile necesare pentru a proteja și conserva patrimoniul cultural și istoric.

Scenariu 41: Participarea la proiecte de parteneriat public-privat pentru dezvoltarea locală Cătălin este un om de afaceri interesat să participe la proiecte de parteneriat public-privat pentru dezvoltarea locală. Accesează platforma online a primăriei, se informează despre oportunitățile disponibile și se înscrie într-unul dintre proiecte. Colaborează cu autoritățile locale și alte entități private pentru a contribui la dezvoltarea comunității.

Scenariu 42: Înregistrarea și gestionarea solicitărilor de intervenție pentru îmbunătățirea spațiilor verzi și amenajarea parcurilor Ion observă că un parc din oraș are nevoie de îmbunătățiri și întreținere. Accesează platforma online a primăriei și completează un formular pentru a solicita intervenția autorităților în vederea îmbunătățirii spațiilor verzi și amenajării parcului. Primăria analizează sesizarea și trimite o echipă de specialiști pentru a evalua situația și a efectua lucrările necesare.

Scenariu 43: Solicitarea și obținerea de informații despre oportunitățile de finanțare și granturi disponibile pentru proiecte locale Gabriela este implicată într-un proiect local și dorește să afle despre oportunitățile de finanțare și granturi disponibile. Accesează platforma online a primăriei, se informează despre sursele de finanțare și granturile disponibile pentru proiecte similare și completează un formular pentru a solicita informații suplimentare. Primește un răspuns detaliat de la primărie cu informații despre cum să aplice pentru finanțare și granturi, precum și despre criteriile de eligibilitate și procedurile aferente.

Scenariu 44: Aflarea aprobărilor de construcții într-o zonă a orașului de către orice cetățean pentru a limita frauda Bogdan locuiește într-un cartier în care a observat o creștere a construcțiilor noi. El dorește să se asigure că aceste construcții sunt legale și au primit toate aprobările necesare. Pentru a verifica informațiile, Bogdan accesează platforma online a primăriei și se autentifică cu contul său de cetățean. Odată autentificat, Bogdan navighează spre secțiunea dedicată autorizațiilor de construcție și selectează zona în care locuiește. Aici, poate vizualiza un registru actualizat al tuturor proiectelor de construcție aprobate, incluzând informații precum adresa, tipul construcției, durata proiectului și numărul autorizației. Bogdan observă o construcție în apropierea locuinței sale și dorește să verifice dacă aceasta are aprobările necesare. Introduce adresa în căutarea registru și îi sunt prezentate informațiile despre proiectul respectiv. Se asigură astfel că proiectul are toate autorizațiile și că respectă reglementările în vigoare. În cazul în care Bogdan descoperă un proiect care nu are autorizația necesară sau nu respectă reglementările, poate raporta acest lucru direct pe platforma online a primăriei. Prin intermediul unui formular dedicat, Bogdan descrie problema și atașează eventuale fotografii sau dovezi ale neregulii. Sesizarea este trimisă către autoritățile competente pentru investigații și măsuri ulterioare.

Scenariu 45: Înregistrarea copilului la școală sau la grădiniță Ioana este mama unui copil care urmează să înceapă școala sau grădinița în curând. Pentru a-și înregistra fiul în instituția de învățământ potrivită, Ioana accesează platforma online a primăriei și se autentifică cu contul său de cetățean. După autentificare, Ioana navighează spre secțiunea dedicată înregistrării copiilor la școală sau grădiniță. Aici, ea găsește informații despre procesul de înregistrare, precum și despre

criteriile de eligibilitate și documentele necesare. Ioana completează formularul online de înscriere, furnizând toate datele solicitate, inclusiv datele de identificare ale copilului și ale părinților, precum și preferințele în ceea ce privește instituțiile de învățământ. Înainte de a trimite formularul, Ioana atașează documentele necesare în format electronic, cum ar fi certificatul de naștere al copilului, dovada adresei de domiciliu și, dacă este cazul, documente privind nevoile speciale de educație ale copilului. Ea se asigură că toate informațiile furnizate sunt corecte și complete, apoi trimite formularul. După trimiterea formularului, Ioana primește un e-mail de confirmare cu un număr de înregistrare și un sumar al datelor furnizate. Primăria procesează cererea și, în funcție de locurile disponibile și de criteriile de admitere, alocă un loc copilului la școală sau grădiniță. Ioana este notificată despre rezultatul înregistrării prin e-mail sau prin intermediul platformei online a primăriei și primește informații despre următorii pași în procesul de admitere.

Aceste scenarii ilustrează diferitele tipuri de interacțiune pe care cetățenii le pot avea cu o primărie puternic digitalizată și cu un grad ridicat de transformare digitală. Prin utilizarea tehnologiei și platformelor online, procesele și serviciile devin mai accesibile, eficiente și transparente, facilitând participarea cetățenilor și îmbunătățind calitatea vieții în comunitate

Descrierea unor situații de digitizare în primărie

Mai jos prezentăm o listă de proiecte de digitizare care pot fi implementate într-o primărie:

1. Digitizarea arhivei și arhivarea electronică a documentelor
2. Digitizarea automată a minutelor ședințelor de lucru
3. Digitizarea documentelor fizice primite la registratură
4. Utilizarea instrumentelor software pentru reducerea efortului necesar în introducerea datelor în MS Office sau alte aplicații

Scenariu 1: Digitizarea arhivei și arhivarea electronică a documentelor Primăria începe procesul de digitalizare a arhivei sale de documente, în scopul creșterii eficienței și reducerea costurilor asociate depozitării documentelor fizice. Procesul începe prin scanarea documentelor fizice și încărcarea acestora într-un sistem de gestionare a documentelor electronice. Documentele sunt clasificate și arhivate astfel încât să poată fi ușor identificate și recuperate atunci când este necesar. Sistemul de gestionare a documentelor permite căutarea rapidă a documentelor și recunoașterea caracterelor textului (OCR), ceea ce facilitează căutarea și recuperarea rapidă a documentelor relevante. De asemenea, sistemul asigură securitatea documentelor, protejându-le împotriva accesului neautorizat și asigurând că acestea sunt disponibile numai pentru utilizatorii autorizați.

Scenariu 2: Digitizarea automată a minutelor ședințelor de lucru Primăria introduce un sistem de digitizare automată a minutelor ședințelor de lucru. Aceasta implică utilizarea unor instrumente software specializate pentru a transforma automat transcrierile audio ale ședințelor de lucru în documente scrise. Sistemul automatizează procesul de transcriere, eliminând nevoia de a angaja personal specializat în transcrierea manuală a înregistrărilor audio. Acest lucru reduce timpul și costurile necesare pentru a pregăti minutele ședințelor de lucru, permițând primăriei să aloce mai mult timp și resurse pentru alte activități importante.

Scenariu 3: Digitizarea documentelor fizice primite la registratură Primăria implementează un sistem de digitizare a documentelor fizice primite la registratură. Acest sistem implică scanarea documentelor primite și încărcarea acestora într-un sistem de gestionare a documentelor electronice. Documentele sunt clasificate și arhivate astfel încât să poată fi ușor identificate și recuperate atunci când este necesar. Utilizând un sistem electronic, primăria poate gestiona documentele primită în mod mai eficient și poate reduce timpul și costurile asociate manipulării și depozitării documentelor fizice.

Scenariu 4: Utilizarea instrumentelor software pentru reducerea efortului necesar în introducerea datelor în MS Office sau alte aplicații Primăria începe să utilizeze instrumente software pentru a reduce timpul și efortul necesare pentru a introduce manual date în MS Office sau alte aplicații. Aceste instrumente includ tehnologii precum recunoașterea vocală sau instrumente pentru citirea codurilor de bare și a documentelor. Prin utilizarea acestor tehnologii, primăria poate accelera procesul de introducere a datelor și reduce riscul de erori umane. Aceasta conduce la o mai mare eficiență și precizie în procesele de gestionare a datelor, permițând primăriei să se concentreze mai mult asupra activităților de planificare și de administrare. În plus, primăria poate utiliza instrumente software pentru a automatiza procesele repetabile, cum ar fi prelucrarea facturilor și a altor documente financiare. Aceste instrumente asigură o mai mare precizie și rapiditate în prelucrarea datelor, reducând timpul și costurile necesare pentru procesarea documentelor financiare. De asemenea, primăria poate implementa instrumente software pentru a automatiza procesele de planificare și de raportare. Acest lucru permite primăriei să colecteze și să analizeze date mai rapid și mai eficient, permițând administratorilor să ia decizii mai bine informate.

În concluzie, digitizarea din primărie poate aduce multiple beneficii, cum ar fi creșterea eficienței, reducerea costurilor și îmbunătățirea calității serviciilor oferite cetățenilor. Implementarea unor instrumente software moderne poate ajuta la automatizarea proceselor, facilitând munca și reducând riscul de erori umane.

Descrierea unor situații de digitalizare în primărie

Mai jos introducem o listă posibilă de proiecte de digitalizare în primărie:

1. Implementarea unui sistem de gestionare a documentelor electronice
2. Crearea unei platforme online pentru a furniza servicii și informații cetățenilor
3. Implementarea unui sistem de plată online pentru serviciile oferite de primărie
4. Crearea unui portal de transparență pentru publicarea informațiilor privind cheltuielile și bugetul primăriei
5. Implementarea unui sistem de comunicare online cu cetățenii, pentru a primi feedback și pentru a primi solicitări de servicii
6. Implementarea unui sistem de monitorizare a serviciilor și proceselor primăriei, pentru a îmbunătăți eficiența și calitatea serviciilor oferite
7. Implementarea unui sistem de raportare automată, pentru a furniza informații relevante către consilierii locali și administrația primăriei
8. Implementarea unui sistem de evaluare a performanțelor și a satisfacției clienților, pentru a identifica problemele și a îmbunătăți serviciile
9. Crearea unei baze de date digitale cu informații despre proprietățile și clădirile din oraș
10. Implementarea unui sistem de monitorizare a calității aerului și a nivelului de zgomot în oraș
11. Crearea unei platforme de voluntariat și implicare în proiecte comunitare
12. Implementarea unui sistem de obținere a autorizațiilor pentru organizarea de evenimente în spațiul public
13. Crearea unei baze de date digitale cu informații despre planurile urbanistice și zonele protejate
14. Implementarea unui sistem de înregistrare și transfer al dreptului de proprietate asupra unui imobil
15. Implementarea unui sistem de obținere a certificatelor de urbanism și de atestare a conformității construcțiilor
16. Crearea unei platforme online pentru înregistrarea căsătoriilor, nașterilor sau deceselor
17. Implementarea unui sistem de obținere a certificatelor de rezidență sau de domiciliu
18. Implementarea unui sistem de înregistrare și modificare a datelor privind starea civilă
19. Implementarea unui sistem de obținere a autorizațiilor pentru desfășurarea de activități economice specifice (terase, taximetrie, etc.)
20. Implementarea unui sistem de înregistrare și gestionare a contractelor de închiriere pentru locuințele sociale

21. Implementarea unui sistem de obținere a autorizațiilor de mediu și a rapoartelor privind impactul asupra mediului
22. Implementarea unui sistem de înregistrare și gestionare a solicitărilor privind serviciile de salubritate
23. Crearea unor programe de educație și informare în domeniul protecției mediului
24. Implementarea unui sistem de înregistrare și gestionare a solicitărilor de intervenție a serviciilor de urgență
25. Implementarea unui sistem de depunere a petițiilor și propunerilor de inițiative cetățenești
26. Crearea unor programe de formare profesională sau cursuri de dezvoltare personală organizate de primărie
27. Implementarea unui sistem de înregistrare și gestionare a cererilor de vot prin corespondență sau schimbarea secției de votare
28. Crearea unor programe de prevenire și sănătate publică
29. Implementarea unui sistem de solicitare a ajutorului pentru victimele violenței domestice sau alte situații de risc
30. Implementarea unui sistem de înregistrare și gestionare a solicitărilor pentru serviciile de asistență socială și consigliere
31. Crearea unor programe de sprijin pentru antreprenorii locali și dezvoltarea afacerilor
32. Implementarea unui sistem de înregistrare și gestionare a sesizărilor privind nerespectarea normelor de conviețuire și siguranță publică
33. Crearea unor programe culturale, sportive și recreative organizate de primărie
34. Implementarea unui sistem de înregistrare și gestionare a cererilor de acces la locuințe
35. Implementarea unui sistem de înregistrare și gestionare a solicitărilor privind transportul în comun și serviciile de mobilitate
36. Implementarea unui sistem de raportare și gestionare a sesizărilor privind degradarea patrimoniului cultural și istoric
37. Crearea unor proiecte de parteneriat public-privat pentru dezvoltarea locală
38. Implementarea unui sistem de înregistrare și gestionare a solicitărilor de intervenție pentru îmbunătățirea spațiilor verzi și amenajarea parcurilor
39. Implementarea unui sistem de solicitare și obținere a informațiilor despre oportunitățile de finanțare și granturi disponibile pentru proiecte locale
40. Implementarea unui sistem de verificare a aprobărilor de construcții într-o zonă a orașului de către orice cetățean pentru a limita frauda
41. Implementarea unui sistem de înregistrare a copilului la școală sau la grădiniță.

Scenariu 1: Platforma de management integrat a proiectelor de investiții: O astfel de platformă ar trebui să permită primăriei să gestioneze proiectele de investiții într-un mod eficient și transparent. Aceasta poate fi folosită pentru a monitoriza și a evalua proiectele de investiții, precum și pentru a urmări progresul și cheltuielile proiectelor. Platforma ar putea fi conectată cu alte sisteme interne pentru a asigura o utilizare ușoară și o colaborare între echipele din primărie. De exemplu, primăria ar putea utiliza platforma pentru a planifica și a gestiona proiectele de infrastructură rutieră, de reabilitare a clădirilor istorice, sau pentru a implementa proiecte de dezvoltare urbană.

Scenariu 2: Platforma de management intern al documentelor: Aceasta este o platformă centralizată care poate fi utilizată pentru a gestiona documentele interne ale primăriei. Platforma ar trebui să permită încărcarea și stocarea documentelor, precum și posibilitatea de a căuta și de a accesa rapid informațiile. De asemenea, platforma poate fi utilizată pentru a crea fluxuri de lucru, care pot fi utilizate pentru a direcționa documentele către persoanele responsabile sau pentru a semna documentele digital. Aceasta poate îmbunătăți eficiența și transparența proceselor administrative, permițând echipei să lucreze în mod mai eficient și să furnizeze mai rapid servicii de înaltă calitate cetățenilor.

Scenariu 3: Platforma pentru achiziții publice: Aceasta este o platformă dedicată achizițiilor publice și poate fi utilizată pentru a centraliza și a gestiona procesul de achiziții din primărie. Platforma

poate permite încărcarea și publicarea de anunțuri de licitație, precum și crearea de formulare de ofertă și managementul licitațiilor. De asemenea, platforma poate furniza o modalitate simplă pentru furnizorii de servicii și bunuri să participe la procesul de licitație și să depună oferte. Utilizarea unei astfel de platforme poate reduce costurile administrative, îmbunătăți eficiența procesului de achiziție și crește transparența în ceea ce privește cheltuielile publice.

Descrierea unor situații de transformare digitală în primărie

Proiectele de transformare digitală sunt prezentate deja în prima partea a acestui material. În continuare prezentăm o descriere a câtorva dintre aceste proiecte posibile.

Scenariu 1: Operarea in cloud a tuturor aplicațiilor si aplicarea conceptului de instituție "paperless", flexibilizarea muncii și telemuncii: Transformarea digitală a primăriei poate implica operarea în cloud a tuturor aplicațiilor și serviciilor interne, eliminând nevoia de a avea echipamente hardware costisitoare și făcând posibilă munca remote. De asemenea, instituirea conceptului de instituție "paperless" poate reduce costurile și timpul alocat în mod tradițional pentru documentarea fizică, cu impact direct asupra mediului. Angajații primăriei ar putea accesa documentele și aplicațiile de oriunde, oricând, ceea ce ar permite flexibilitate și productivitate crescută, precum și creșterea satisfacției angajaților.

Într-un scenariu în care primăria ar adopta cloud computing și conceptul de instituție "paperless", angajații ar avea acces la informații și aplicații de oriunde și oricând, fără a fi legați de un birou fizic. De asemenea, ar putea beneficia de o varietate de instrumente și tehnologii digitale pentru a-și îndeplini sarcinile de zi cu zi. Aceasta ar însemna că ar fi posibil să se îmbunătățească eficiența și productivitatea prin reducerea timpului și a costurilor asociate cu utilizarea documentelor fizice și hardware-ului tradițional.

Pentru a realiza acest scenariu, primăria ar trebui să adopte un sistem de cloud computing care să permită accesul la informații și aplicații de oriunde și oricând. Angajații ar avea nevoie de un dispozitiv cu acces la internet și o conexiune sigură pentru a putea accesa informațiile și aplicațiile necesare. De asemenea, ar trebui să se dezvolte o soluție pentru stocarea, gestionarea și accesul la documentele digitale.

În ceea ce privește fluxul de lucru, angajații ar putea accesa documentele și aplicațiile necesare de pe orice dispozitiv conectat la internet, folosind credențialele lor de autentificare. Acestea ar putea fi integrate cu un sistem de autentificare unică, care ar permite utilizatorilor să acceseze toate aplicațiile și documentele dintr-un singur loc. De asemenea, ar putea fi dezvoltată o platformă de colaborare, care să permită angajaților să lucreze împreună la documente și proiecte.

În cazul instituirii conceptului de instituție "paperless", angajații ar trebui să înceteze să folosească documente fizice și să se bazeze exclusiv pe documente digitale. Documentele ar trebui să fie stocate într-un sistem de gestionare a documentelor digitale și să fie disponibile pentru toți utilizatorii autorizați. Pentru a facilita schimbul de documente între angajați și alte entități, ar putea fi dezvoltată o platformă de schimb electronic de documente.

În ceea ce privește procesele, toate procesele de afaceri ar trebui să fie reevaluate și adaptate la mediul digital. De exemplu, procesul de aprobare a cererilor sau de procesare a plăților ar putea fi automatizat și gestionat digital, eliminând necesitatea de a folosi documente fizice și proceduri manuale. Ar trebui să fie dezvoltate soluții pentru a permite utilizatorilor să semneze electronic documente și formulare, astfel încât procesul de semnare să poată fi gestionat digital.

Adoptarea unui sistem de cloud computing și a conceptului de instituție "paperless" ar implica o serie de schimbări semnificative în modul în care angajații și utilizatorii ar interacționa cu tehnologia și ar realiza activitățile de zi cu zi. Ar fi nevoie de formare și instruire pentru a asigura

că toți utilizatorii sunt capabili să utilizeze noile tehnologii și să se adapteze la noul mod de lucru. De asemenea, ar trebui să se pună accent pe securitatea datelor și protecția informațiilor, pentru a asigura confidențialitatea și integritatea datelor.

Scenariu 2: Utilizarea asistenților virtuali si platformelor online mobile de relații, cu funcții de trasabilitate si semnături digitale pentru asigurarea serviciilor către cetățean 24/7: Primăria ar putea implementa asistenți virtuali și platforme mobile de relații cu cetățenii, care ar putea fi disponibile 24/7. Aceste platforme ar putea furniza asistență și informații în timp real, prin intermediul unor chatbot-uri sau asistenți virtuali. În plus, ar putea fi implementate semnături digitale și mecanisme de urmărire pentru asigurarea securității datelor și a unei experiențe bune a utilizatorilor.

Implementarea asistenților virtuali și a platformelor online mobile ar implica o schimbare semnificativă în modul în care cetățenii interacționează cu primăria. Pentru a se asigura că aceste tehnologii sunt utilizate eficient, ar trebui să existe o strategie clară de comunicare și instruire a utilizatorilor.

În ceea ce privește fluxul de lucru, cetățenii ar putea accesa platformele online prin intermediul site-ului web al primăriei sau prin intermediul unei aplicații mobile. Chatbot-urile și asistenții virtuali ar putea fi utilizați pentru a furniza asistență în timp real, inclusiv pentru a răspunde la întrebări frecvente, a oferi informații despre serviciile disponibile și pentru a ghida utilizatorii prin procesul de obținere a unui serviciu.

Pentru a utiliza semnături digitale și mecanisme de urmărire, cetățenii ar trebui să își creeze un cont pe platforma online și să se autentifice utilizând datele personale și parole. După aceea, ar putea utiliza platforma pentru a solicita servicii, pentru a depune documente și pentru a semna documente digitale.

În ceea ce privește procesul intern de lucru, angajații din primărie ar putea utiliza aceleași platforme și tehnologii pentru a gestiona și procesa cererile cetățenilor. Ar putea utiliza asistenți virtuali și chatbot-uri pentru a răspunde rapid la cererile de asistență și pentru a ghida cetățenii prin procesul de obținere a serviciilor. De asemenea, ar putea utiliza semnături digitale și mecanisme de urmărire pentru a asigura securitatea și eficiența procesului de gestionare a documentelor și a serviciilor.

Implementarea asistenților virtuali și a platformelor online mobile poate fi o soluție eficientă pentru a îmbunătăți comunicarea cu cetățenii și a reduce timpul și costurile alocate serviciilor. Cu toate acestea, este important să se planifice cu atenție implementarea și să se asigure o instruire adecvată a utilizatorilor, pentru a se asigura că tehnologiile sunt utilizate eficient și în mod corespunzător.

Specificațiile pentru un caiet de sarcini referitor la acest proiect ar putea include următoarele:

1. Funcții și caracteristici ale platformei online: Aceasta ar trebui să permită utilizatorilor să acceseze informații relevante, să solicite servicii, să depună documente și să semneze digital documente, inclusiv cu funcții de trasabilitate și verificare. Platforma ar trebui să ofere o experiență facilă și intuitivă pentru utilizatori și să fie optimizată pentru a fi accesată de pe dispozitive mobile. O listă cu funcțiile și caracteristicile pe care ar trebui să le ofere platforma online este mai jos:

    - Acces la informații relevante: Platforma ar trebui să permită utilizatorilor să găsească informații relevante despre serviciile disponibile, procedurile de aplicare, documentele necesare și alte informații utile.

- Solicitare de servicii: Utilizatorii ar trebui să poată solicita servicii prin intermediul platformei, precum eliberarea de documente, înregistrarea de evenimente, sesizarea unor probleme și altele.
- Depunere de documente: Platforma ar trebui să permită utilizatorilor să depună documentele necesare pentru a solicita serviciile, precum copii de acte de identitate, certificări, declarații și altele.
- Semnare digitală: Platforma ar trebui să permită utilizatorilor să semneze digital documente, precum cereri, declarații sau acorduri, cu ajutorul semnăturilor digitale, și să ofere funcții de trasabilitate și verificare.
- Experiență facilă și intuitivă: Platforma ar trebui să ofere o experiență facilă și intuitivă pentru utilizatori, cu un design atractiv și ușor de utilizat. Aceasta ar trebui să fie optimizată pentru a fi accesată de pe dispozitive mobile, precum telefoane mobile sau tablete.
- Securitate și confidențialitate: Platforma ar trebui să ofere o securitate adecvată pentru datele personale și documentele depuse, prin implementarea unor măsuri de securitate precum criptarea datelor și autentificarea utilizatorilor.
- Funcții de urmărire: Platforma ar trebui să ofere funcții de urmărire pentru utilizatori, astfel încât aceștia să poată vedea stadiul cererilor și documentelor depuse, și să poată primi notificări în timp real.
- Integrare cu alte sisteme: Platforma ar trebui să poată fi integrată cu alte sisteme și aplicații utilizate de primărie, precum sistemele de gestiune a documentelor sau cele de planificare a bugetului.

2. Chatbot-uri și asistenți virtuali: Platforma ar trebui să ofere suport pentru chatbot-uri și asistenți virtuali, care ar putea fi utilizați pentru a oferi asistență în timp real, a ghida utilizatorii prin procesul de obținere a serviciilor și a răspunde la întrebări frecvente. Funcțiile pentru chatbot-uri și asistenți virtuali ar putea include:

    - Răspunsuri automate la întrebări frecvente: chatbot-ul sau asistentul virtual ar trebui să poată oferi răspunsuri automate la întrebări frecvente legate de serviciile primăriei și să furnizeze informații relevante despre acestea.
    - Ghidarea utilizatorilor prin procesul de obținere a serviciilor: chatbot-ul sau asistentul virtual ar trebui să poată ghida utilizatorii prin procesul de obținere a serviciilor și să le ofere instrucțiuni detaliate despre ceea ce trebuie să facă pentru a solicita un serviciu.
    - Integrare cu alte servicii: chatbot-ul sau asistentul virtual ar trebui să poată fi integrat cu alte servicii, cum ar fi sistemul de programare online, pentru a permite utilizatorilor să programeze întâlniri și să primească notificări despre stadiul cererii lor.
    - Identificarea utilizatorilor: chatbot-ul sau asistentul virtual ar trebui să poată identifica utilizatorii și să le ofere recomandări personalizate, bazate pe informațiile existente în baza de date a primăriei.
    - Funcții de interacțiune: chatbot-ul sau asistentul virtual ar trebui să poată interacționa cu utilizatorii prin intermediul textului, vocii sau imaginilor și să ofere opțiuni de răspuns în funcție de preferințele utilizatorilor.
    - Înregistrarea și monitorizarea interacțiunilor: chatbot-ul sau asistentul virtual ar trebui să poată înregistra și monitoriza interacțiunile cu utilizatorii, pentru a permite primăriei să îmbunătățească experiența utilizatorilor și să identifice posibile probleme în procesul de furnizare a serviciilor.

3. Autentificare și securitate: Platforma ar trebui să utilizeze metode de autentificare puternice, inclusiv autentificare cu doi factori și criptare pentru a proteja datele personale ale utilizatorilor. De asemenea, ar trebui să aibă implementate măsuri de securitate adecvate pentru a preveni accesul neautorizat la informații și pentru a proteja împotriva amenințărilor cibernetice.
4. Integrare cu sistemele existente: Platforma ar trebui să fie capabilă să se integreze cu sistemele existente din primărie, inclusiv cu bazele de date și cu alte aplicații de gestionare a serviciilor.

5. Urmărire și raportare: Platforma ar trebui să ofere funcții de urmărire și raportare, pentru a permite primăriei să urmărească și să analizeze modul în care cetățenii utilizează serviciile și să îmbunătățească experiența utilizatorilor.
6. Instruire și suport: Primăria ar trebui să ofere instruire adecvată și suport pentru utilizatorii platformei, inclusiv pentru utilizarea chatbot-urilor, semnarea digitală a documentelor și pentru depunerea documentelor online.
7. Standarde și reglementări: Platforma ar trebui să respecte standardele și reglementările privind protecția datelor personale și să fie în conformitate cu legislația aplicabilă.

Scenariu 3: Aplicarea conceptului "once-only" in relația cu cetățeanul: Conceptul "once-only" presupune ca datele personale ale cetățenilor să fie colectate o singură dată și să fie accesate de către toate autoritățile și instituțiile publice. În acest fel, cetățenii nu ar mai fi nevoiți să furnizeze aceleași informații de mai multe ori. Implementarea acestui concept ar putea reduce timpul necesar pentru a furniza servicii cetățenilor și ar putea îmbunătăți experiența acestora cu autoritățile publice.

Implementarea conceptului "once-only" în relația cu cetățeanul ar presupune o schimbare fundamentală în modul în care primăria colectează și gestionează datele personale ale cetățenilor. Fluxul de lucru ar fi următorul:

1. Colectarea datelor personale: Primăria ar trebui să colecteze datele personale ale cetățenilor o singură dată, la primul contact. Aceste date ar trebui să fie furnizate prin intermediul unor formulare online sau în format fizic, iar cetățenii ar trebui să fie informați cu privire la scopul colectării acestora.
2. Centralizarea datelor: După ce datele au fost colectate, acestea ar trebui să fie centralizate într-o bază de date centrală, unde ar putea fi accesate de către toate departamentele primăriei.
3. Validarea datelor: Înainte de a utiliza datele pentru a furniza servicii cetățenilor, primăria ar trebui să valideze informațiile colectate și să confirme că sunt corecte și complete.
4. Accesul la date: După ce datele au fost colectate și validate, acestea ar putea fi accesate de către toți angajații primăriei care au nevoie de acestea pentru a furniza servicii cetățenilor. În plus, cetățenii ar putea accesa propriile lor date prin intermediul unui portal online securizat.
5. Actualizarea datelor: Dacă cetățenii furnizează informații suplimentare sau se schimbă informațiile existente, acestea ar trebui să fie actualizate în baza de date centrală și să fie disponibile pentru toți angajații primăriei care au nevoie de acestea.
6. Securitatea datelor: Primăria ar trebui să ia măsuri adecvate pentru a asigura securitatea datelor personale ale cetățenilor și a preveni orice încălcare a securității datelor.

Implementarea conceptului "once-only" ar putea aduce numeroase beneficii, inclusiv reducerea timpului necesar pentru a furniza servicii cetățenilor, creșterea eficienței și îmbunătățirea experienței cetățenilor cu primăria.

Mai jos este o listă de specificații pentru un caiet de sarcini aferent proiectului de implementare a conceptului "once-only":

1. Platformă centralizată de colectare a datelor personale: Primăria ar trebui să implementeze o platformă centralizată pentru colectarea datelor personale ale cetățenilor. Aceasta ar trebui să permită cetățenilor să furnizeze datele personale o singură dată și să le poată actualiza ulterior, dacă este necesar.
2. Sisteme de validare și verificare a datelor: Primăria ar trebui să implementeze sisteme de validare și verificare a datelor, astfel încât să se asigure că datele colectate sunt corecte și complete. De asemenea, aceste sisteme ar trebui să permită detectarea și corectarea erorilor.
3. Portal online pentru cetățeni: Primăria ar trebui să ofere un portal online securizat prin intermediul căruia cetățenii să poată accesa propriile lor date personale și să le poată actualiza ulterior, dacă este necesar.

4. Securitatea datelor: Primăria ar trebui să ia măsuri adecvate pentru a asigura securitatea datelor personale ale cetățenilor. Aceste măsuri ar trebui să includă criptarea datelor, autentificarea și autorizarea adecvată a utilizatorilor, precum și monitorizarea și auditarea accesului la date.
5. Integrare cu alte sisteme ale primăriei: Platforma de colectare a datelor ar trebui să fie integrată cu alte sisteme ale primăriei, astfel încât datele să poată fi accesate și utilizate de către toate departamentele care furnizează servicii cetățenilor.
6. Instruirea angajaților: Angajații primăriei ar trebui să fie instruiți cu privire la utilizarea platformei de colectare a datelor și la conceptul "once-only". De asemenea, ar trebui să li se ofere suport și asistență în cazul unor probleme sau întrebări. Implementarea conceptului "once-only" ar necesita instruirea angajaților primăriei cu privire la noul flux de lucru și la buna utilizare a bazei de date centralizată. De asemenea, ar putea fi necesară instruirea cetățenilor cu privire la modul de utilizare a portalului online pentru accesul la datele personale.
7. Respectarea reglementărilor privind protecția datelor personale: Primăria ar trebui să respecte reglementările și standardele privind protecția datelor personale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR) din UE și să ia măsuri adecvate pentru a preveni orice încălcare a acestora.
8. Integrarea cu alte instituții: Primăria ar putea coopera cu alte instituții publice pentru a implementa conceptul "once-only". Aceasta ar permite o colectare și distribuire mai eficientă a datelor personale ale cetățenilor între instituții și ar îmbunătăți experiența acestora cu sectorul public în ansamblu.
9. Monitorizarea și evaluarea: Primăria ar trebui să implementeze un sistem de monitorizare și evaluare pentru a evalua eficacitatea și impactul conceptului "once-only". Acest lucru ar trebui să implice evaluarea modului în care conceptul a îmbunătățit experiența cetățenilor și a redus timpul și costurile necesare pentru a furniza servicii, precum și evaluarea modului în care a fost respectată reglementarea privind protecția datelor.

Scenariu 4: Colectare, management, analiza volume mari de date si informații cu IA, IoT, sisteme expert pentru optimizare alocare si distribuție bugetară: Primăria ar putea folosi tehnologii precum IA, IoT și sisteme expert pentru a gestiona datele și informațiile în timp real. Aceste tehnologii ar putea fi utilizate pentru a identifica probleme, a optimiza alocarea și distribuția bugetului și a îmbunătăți eficiența serviciilor.

Pentru a colecta datele, primăria ar putea utiliza senzori IoT (Internet of Things) și alte dispozitive de colectare a datelor, cum ar fi camere de supraveghere și alte echipamente inteligente. Aceste date ar fi apoi prelucrate și analizate cu ajutorul tehnologiilor IA (Inteligența Artificială) și a sistemelor expert.

Procesul de colectare și analiză a datelor ar putea fi integrat cu procesul de bugetare și planificare a serviciilor, astfel încât să se asigure o distribuție eficientă a resurselor. În plus, ar putea fi implementate sisteme de monitorizare și raportare automată pentru a permite autorităților să își adapteze planurile și să ia decizii informate în timp real.

Pentru a asigura securitatea și protecția datelor personale, primăria ar putea utiliza tehnologii de criptare și alte măsuri de securitate, precum și să respecte standardele și reglementările privind protecția datelor personale.

Angajații din primărie ar putea fi instruiți și echipați cu abilitățile necesare pentru a utiliza aceste tehnologii și a putea lua decizii informate pe baza datelor analizate. De asemenea, ar putea fi implementate instrumente de vizualizare a datelor pentru a permite autorităților să înțeleagă mai bine informațiile și să ia decizii mai bune.

Specificațiile pentru un caiet de sarcini pentru proiectul de colectare, management si analiza a volumelor mari de date cu IA, IoT si sisteme expert ar putea include:

1. Colectarea datelor: trebuie identificate sursele de date, inclusiv senzori IoT, dispozitive de monitorizare si alte echipamente inteligente, precum si metodele de colectare a datelor de la aceste surse.
2. Pre-procesarea datelor: se va defini cum se vor prelucra si prelucra datele colectate inainte de a fi analizate. Aceasta poate include curatarea datelor, transformarea datelor si integrarea datelor din surse multiple.
3. Analiza datelor: se va descrie cum se vor folosi tehnologiile IA si sistemele expert pentru a identifica modele si tendinte in datele colectate, precum si pentru a furniza recomandari si sugestii pentru optimizarea alocarii si distributiei bugetului.
4. Integrarea cu procesul de bugetare: se va defini cum se vor integra datele si recomandarile obtinute prin analiza datelor cu procesul de bugetare si planificare a serviciilor. Acest lucru poate include dezvoltarea de modele de alocare a resurselor si planuri de implementare.
5. Monitorizarea si raportarea: se va defini cum se vor monitoriza si raporta datele colectate si analizate, astfel incat sa se poata lua decizii in timp real si sa se adapteze planurile si alocarea resurselor in functie de situatii.
6. Securitatea datelor: se va descrie cum se vor proteja datele colectate, inclusiv masurile de securitate pentru a preveni accesul neautorizat si utilizarea datelor personale.
7. Training-ul angajatilor: se va descrie cum se vor instrui si pregati angajatii pentru a utiliza tehnologiile de colectare si analiza a datelor si pentru a lua decizii informate pe baza acestora.
8. Vizualizarea datelor: se va defini cum se vor vizualiza datele analizate, astfel incat autoritatile sa poata intelege mai bine informatiile si sa ia decizii mai bune. Acest lucru poate include crearea de rapoarte si dashboard-uri personalizate.
9. Reglementari privind datele personale: se va descrie cum se vor respecta reglementarile si standardele privind protejarea datelor personale, cum ar fi Regulamentul General privind Protectia Datelor (GDPR). Aceasta poate include adoptarea de politici de confidentialitate, acorduri de confidentialitate si contracte cu terti.

Scenariu 5: Adopție aplicații digitale sub forma SaaS: Primăria ar putea utiliza servicii de software ca serviciu (SaaS) pentru a economisi costuri și a permite accesul facil la aplicații digitale. Aceasta ar reduce nevoia de a investi în hardware și ar permite actualizări și întreținere mai eficiente.

Utilizarea aplicațiilor digitale sub forma SaaS ar permite angajaților din primărie și altor utilizatori să acceseze și să folosească aceste aplicații de oriunde, oricând, folosind doar o conexiune la internet și un dispozitiv mobil sau un calculator. În plus, utilizarea SaaS ar putea reduce timpul și costurile necesare pentru implementarea de noi aplicații, deoarece acestea ar fi deja dezvoltate și disponibile pe piață. Procesul de utilizare a unei aplicații SaaS ar implica în general crearea unui cont sau a unui profil de utilizator, accesarea aplicației prin intermediul unui browser web sau al unei aplicații mobile, efectuarea sarcinilor specifice și salvarea datelor într-un mediu securizat și centralizat. Angajații din primărie ar putea beneficia de capacitățile de colaborare și comunicare îmbunătățite oferite de unele aplicații SaaS, precum și de caracteristicile de automatizare și analiză a datelor.

SaaS (Software as a Service) oferă primăriei o serie de avantaje, printre care:

1. Economisirea costurilor: în loc să cumpere software și să investească în hardware costisitor, primăria poate plăti o sumă lunară sau anuală pentru a utiliza aplicațiile digitale de care are nevoie.
2. Actualizări constante: SaaS oferă actualizări constante ale aplicațiilor, astfel încât primăria nu trebuie să se ocupe de întreținerea software-ului.
3. Accesibilitate: deoarece aplicațiile sunt disponibile online, primăria și angajații săi pot accesa aplicațiile de oriunde și oricând, cu ajutorul unei conexiuni la internet.
4. Scalabilitate: primăria poate alege să utilizeze doar aplicațiile de care are nevoie și să le extindă sau să le restrângă în funcție de necesități, fără a fi nevoie să investească în hardware suplimentar.

5. Flexibilitate: SaaS permite primăriei să testeze aplicații noi sau să le schimbe în funcție de nevoile sale, fără a fi nevoie să investească timp și resurse în dezvoltarea propriilor aplicații.

Caietul de sarcini pentru proiectul de adopție a aplicațiilor digitale sub forma SaaS ar putea include următoarele specificații:

1. Lista de aplicații SaaS necesare pentru a răspunde nevoilor primăriei, precum aplicații de colaborare, analiză a datelor, automatizare și gestionare a proiectelor.
2. Cerințele hardware și software pentru a utiliza aplicațiile SaaS, precum specificațiile minime ale sistemelor și browserelor necesare.
3. Proceduri de securitate pentru protejarea datelor și informațiilor confidențiale, precum autentificare cu doi factori și criptare a datelor.
4. Proceduri de backup și de recuperare a datelor în caz de pierdere sau corupție.
5. Cerințele de suport și de întreținere pentru aplicațiile SaaS, precum nivelul de suport oferit de furnizorii de aplicații și procedurile pentru a raporta probleme sau erori.
6. Cerințe de raportare și de analiză a utilizării aplicațiilor SaaS, precum numărul de utilizatori și de sesiuni, timpul mediu de utilizare și evaluarea satisfacției utilizatorilor.
7. Acordul de nivel de serviciu (SLA) cu furnizorii de aplicații SaaS, care să definească nivelul de disponibilitate și de performanță garantat, precum și procedurile de remediere a problemelor.
8. Planul de implementare, care să includă etapele de testare, de formare a angajaților și de migrație a datelor și a utilizatorilor către aplicațiile SaaS.
9. Planul de buget și de cheltuieli, care să includă costurile de licențiere, de suport și de întreținere a aplicațiilor SaaS, precum și costurile de formare a angajaților și de migrare a datelor.

Observații

Este adevărat că investiția în digitalizare și transformare digitală implică costuri și eforturi semnificative, inclusiv pentru dezvoltarea și implementarea de soluții digitale, achiziționarea și întreținerea infrastructurii, formarea și instruirea personalului, precum și suportul și mentenanța operațională. În acest context, pentru a putea aloca resurse financiare suficiente pentru a susține operațional aceste proiecte, ar fi necesar să se stabilească un buget dedicat pentru dezvoltarea și implementarea proiectelor de digitalizare și transformare digitală, precum și pentru susținerea acestora pe termen lung.

Este important ca acest buget să fie planificat în mod realist, ținând cont de costurile operaționale, cum ar fi formarea și instruirea personalului, mentenanța și suportul, precum și actualizarea și modernizarea soluțiilor digitale pe măsură ce tehnologia evoluează.

Este dificil să oferim date cantitative specifice pentru alocarea de bugete pentru digitalizarea primăriei, deoarece acestea variază în funcție de multe factori, precum dimensiunea și complexitatea proiectelor, gradul de transformare digitală dorit, resursele financiare și umane disponibile și alte nevoi specifice. Totuși, pentru a oferi un punct de referință, următoarele sunt câteva estimări:

- Potrivit unui raport al Deloitte, în general, autoritățile publice ar trebui să aibă un buget de cel puțin 5% din cheltuielile lor anuale pentru investiții în IT și transformare digitală.
- În 2018, o analiză a Consiliului Europei a arătat că autoritățile publice din Europa de Est alocă, în medie, între 1,5% și 3% din bugetul total pe proiecte IT și digitale.
- Un studiu realizat de Gartner arată că, în medie, organizațiile publice din întreaga lume alocă aproximativ 3,8% din veniturile lor la cheltuieli IT, inclusiv investiții în digitalizare și transformare digitală.

În general, se recomandă alocarea între 5 și 10% din bugetul total al primăriei pentru dezvoltarea și implementarea proiectelor de digitalizare și transformare digitală, însă această alocare poate

varia în funcție de dimensiunea și complexitatea proiectelor, precum și de resursele financiare și umane disponibile.

În afară de bugetul alocat, există și alte aspecte importante pe care o primărie trebuie să le ia în considerare atunci când abordează transformarea digitală. Acestea includ:

1. Planificare strategică: Primăria trebuie să elaboreze o strategie clară de transformare digitală care să identifice obiectivele și prioritățile specifice, să stabilească un plan de acțiune detaliat și să evalueze periodic progresul. Aceasta trebuie să implice atât conducerea, cât și personalul din toate departamentele.
2. Managementul schimbărilor: Transformarea digitală implică schimbări semnificative în modul în care funcționează o primărie și cum interacționează cu cetățenii săi. Este important să se dezvolte un plan de management al schimbărilor, care să includă formarea și instruirea personalului, comunicarea și implicarea cetățenilor și a altor părți interesate.
3. Cooperare cu alte primării: Primăria poate beneficia de cooperarea cu alte primării care sunt angajate în procesul de transformare digitală și de învățare de la cele mai bune practici și soluții dezvoltate de alții.
4. Protecția datelor cu caracter personal: O primărie trebuie să ia măsuri pentru a proteja datele cu caracter personal colectate de la cetățeni și pentru a se conforma cu reglementările în domeniu, cum ar fi GDPR.
5. Evaluare a performanței și a impactului: Pentru a asigura că transformarea digitală este eficientă și își atinge obiectivele, este important să se evalueze periodic performanța și impactul soluțiilor digitale implementate, inclusiv prin colectarea și analizarea datelor relevante.
6. Inovație continuă: Transformarea digitală este un proces continuu, iar primăria trebuie să fie pregătită să adopte și să integreze noi tehnologii și soluții digitale pentru a se adapta la schimbările și nevoile în continuă evoluție ale cetățenilor și ale comunității în ansamblu.

FISA DE PROIECT FANION

Titlu

Sistem de management al digitalizării în Primăria Bistrița

Coordonator din partea consultantului

Stelian Brad

Necesitatea și urgența digitalizării activităților în cadrul Primăriei Bistrita

Digitalizarea instituțiilor din administrația publică este o necesitate din foarte multe puncte de vedere, dintre care amintim:

- Integrarea la nivel de fluxuri informaționale cu alte instituții publice la nivel local, regional și central pentru posibilitatea de a efectua analize pertinente și în timp util asupra alocării și distribuției bugetare pe cele mai urgente politici publice
- Respectarea cetățeanului și mediului privat – ca principali contribuitori la bugetul public – prin furnizarea unor servicii de bună calitate în timpul cel mai scurt posibil și cu efort minim de timp și de altă natură din partea beneficiarului
- Optimizarea proceselor interne și ușurarea muncii efectuate de către angajați
- Creșterea productivității muncii angajaților
- Reducerea riscurilor privind siguranța datelor și informațiilor
- Creșterea capacității de a înțelege ce se întâmplă și cum se întâmplă în interiorul instituției
- Crearea condițiilor de dezvoltare a unor servicii noi către cetățeni și alte părți interesate, imposibil de lansat în absența digitalizării
- Creșterea capacității de răspuns cu analize și rapoarte la solicitări neprevăzute venite dinspre instituțiile centrale
- Creșterea capacității de fundamentare a unor strategii corecte de dezvoltare durabilă multisectoriale la nivel de oraș
- Reducerea birocrației
- Creșterea capacității de conformare la reglementări și tendințe naționale și europene

Abordarea la nivel de sistem

Pentru atingerea acestor obiective, nu este suficientă doar elaborarea unei strategii de digitalizare, deoarece aceasta trebuie adoptată și executată, pe de o parte, iar pe de altă parte nu rezolvă integral problema digitalizării instituționale. Digitalizarea este un proces pe termen mediu, care cuprinde mai multe aspecte, în care sistemul informatic este un element suport. Problema în sine trebuie abordată procesual și la nivel sistemic. Pentru aceasta, o recomandare clară este aceea de a pune în practică pe viitor un sistem de management al sistemului informatic și politicii de digitalizare instituțională.

- Digitalizarea trebuie văzută ca fiind utilizarea tehnologiei digitale pentru a schimba modelul de operare în cadrul Primăriei Bistrita, creând linii noi de activitate aducătoare de valoare adăugată pentru societate și oportunități de servicii noi pentru cetățeni și alte terțe părți interesate
- Digitalizarea interconectează sistemul de livrare a serviciilor către societate cu procesele interne, cu angajații, partenerii si cu cetățenii
- Digitalizarea conduce la dezvoltarea unei instituții publice județene profund conectate la lanțul național al valorii ecosistemului public, creând premize favorabile pentru dezvoltarea unei infrastructuri sociale performante, care să își aducă contribuția la factorul total al productivității țării

Digitalizarea extinsă este necesară și trebuie să conducă la integrarea activităților din Primăria Bistrita cu cele ale structurilor subordinate, să facă munca mai inteligentă si comensurabilă în fluxul complicat care definește întregul sistem de servicii al Primăriei Bistrita. Din acest punct de vedere, implementarea trebuie făcută de la nivel strategic, trebuie să acopere toate procesele interne și de la interfața cu alte instituții și cu beneficiarii finali, trebuie condusă de managementul de nivel C și trebuie să producă o schimbare la nivelul culturii din instituție. Se propune în acest sens luarea în considerare a unui model propus de către Cluj IT și denumit „Casa IT-ului", prezentat în figura de mai jos, prin care se creează cadrul necesar punerii în practică a unei strategii de digitalizare.

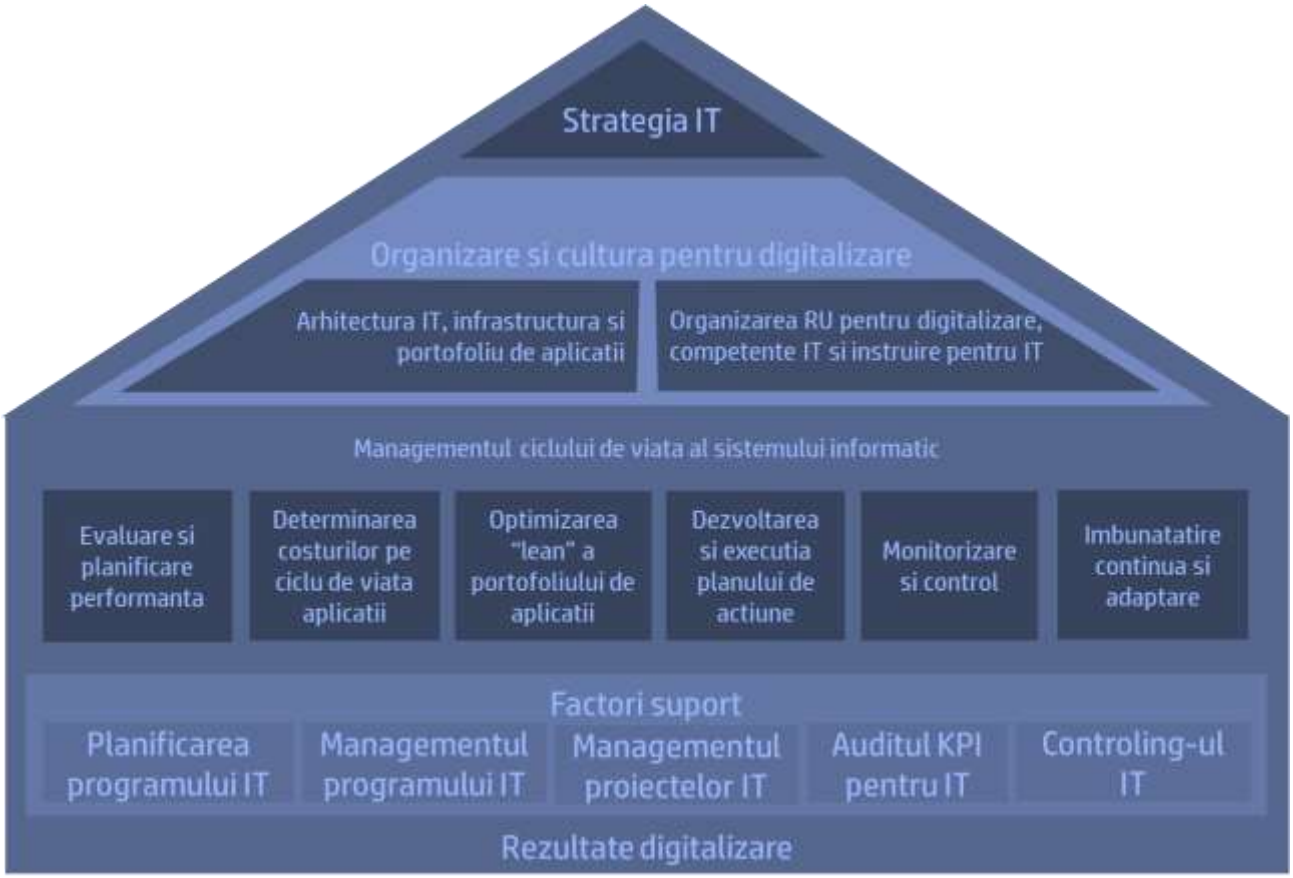


Figura: Cadrul de implementare a unei strategii de digitalizare în Primăria Bistrita

„Casa IT" vede digitalizarea pe mai multe straturi de intervenție, toate însă fiind interconectate. În acest sens, trebuie identificați, susținuți și dezvoltați factorii suport, formați din acțiuni specifice de informatizare, pe baza cărora se abordează sistemul informatic într-o formulă orientată pe ciclu de viață. Pe această fundație trebuie construită cultura organizațională orientată pe derularea digitalizată a activităților și prin intermediul unei organizări interne adecvate acestui scop. Toate la un loc trebuie să subscrie unei strategii integrate de informatizare și digitalizare. Prin intermediul unui mecanism intern de audit se evaluează periodic rezultatele în procesul de digitalizare și se intervine cu măsuri de îmbunătățire continuă.

Recomandări pe grupe de intervenție

Strategia de informatizare

Managementul de top are rolul de a stabili o viziune asupra digitalizării, care să reflecte, de asemenea, ce anume dorește organizația sa obțină în termeni de digitalizare. Această viziune ar trebui:

— să seteze o direcție și să formuleze o provocare care să inspire persoanele să se angajeze și să lucreze pentru atingerea acestui scop;

- să fie suficient de ambițioasă, fără a fi constrânsă de capabilitățile curente ale organizației

- să ofere o țintă în raport cu care să se poată măsura progresul.

Această viziunea ar putea fi dezvoltată prin intermediul unei strategii de digitalizare ce reprezintă planul general pentru a o obține efectiv. Această strategie ar trebui să ia în considerare rezultatele analizei contextului extern și intern, respectiv nevoile și așteptările identificate ale părților externe

și interne interesate. Strategia ar trebui dezvoltată în urma consultării acestor părți interesate și ar trebui să le fie comunicată. Strategia de digitalizare trebuie să definească:

- capacitățile și resursele de digitalizare ale organizației
- ce anume înseamnă procesul de digitalizare pentru organizație și pentru fiecare zonă sau unitate; a se defini criteriul care să diferențieze digitalizarea de activitatea zilnică tradițională/curentă
- tipurile de digitalizare pe care organizația trebuie să se concentreze
- nivelurile de noutate pe care organizația trebuie să se concentreze
- politica privind resursele umane care să permită digitalizarea
- politica privind colaborarea, inclusiv soluții de interacțiune din afara organizației și colaborări cu terțe părți.

Viziunea asupra digitalizării, strategia și politicile trebuie să fie disponibile ca informație documentată, să fie măsurate și comunicate în interiorul organizației și disponibile părților interesate.

Lansarea proiectelor de digitalizare într-un mediu național și internațional constant schimbător reprezintă o decizie strategică care solicită mobilizarea de cunoștințe și informații de înaltă valoare.

Managementul digitalizării necesită suportul unui proces de management adecvat la nivel strategic în vederea pregătirii unor decizii strategice în termenii organizării anticipării, poziționării, influenței, know-how-ului, libertății de utilizare și protecției bunurilor informaționale și intelectuale.

Rolul cheie al digitalizării strategice este acela de a oferi informații și cunoștințe privind sprijinul decizional. Acestea conferă organizației posibilitatea de analiză a valorii: înțelegerea nevoilor prezente și viitoare ale beneficiarului, cunoașterea evoluției în alte instituții publice, înțelegerea constrângerilor, oportunităților și riscurilor, identificarea noilor puncte de livrare, parteneriatelor, serviciilor și proceselor noi, schimbărilor tehnologice și reglementate, dezvoltării noilor standarde, finanțelor, etc.

Procesul de digitalizare strategică este bazat pe colectarea, procesarea, analiza și producerea informației și cunoștințelor care contribuie în mod notabil la diferitele stadii de luare a deciziilor în contextul managementului procesului de digitalizare: decizii privind proiectele care trebuie lansate, privind elaborarea proiectului, privind fezabilitatea proiectului, privind dezvoltarea aplicațiilor de uz intern, privind rezultatele care trebuie protejate, privind libertatea de utilizare, constrângerile etice și reglementare, totul în contextul Framework-ului referitor la strategiile mai largi ale organizației.

Ca o consecință, managementul strategic al organizației poate fi definit și implementat sub îndrumarea și autoritatea managementului de vârf.

Principalele domenii ale managementului digitalizării strategice sunt următoarele:

— implicarea managementului de top în vederea dirijării și monitorizării procesului de management al digitalizării

— definirea nevoilor și utilizărilor, strategiilor de digitalizare și luare a deciziilor, de către managementul de vârf

— integrarea în cultura organizației a interacțiunilor și partajării informației/cunoștințelor între angajați

— identificarea resurselor necesare și disponibile (umane, informaționale și de hardware)

— implementarea mijloacelor adecvate - precum indicatorii de performanță - pentru a asigura faptul că performanța este suficientă pentru ca monitorizările periodice și acțiunile corective efective să poată fi inițiate.

Organizarea și cultura pentru digitalizare

Managementul superior ar trebui să favorizeze o cultură care să sprijine digitalizarea. Cultura de digitalizare trebuie înțeleasă ca o mentalitate și fiecare persoană din cadrul organizației este responsabilă pentru contribuția la creșterea acesteia.

O cultură care sprijină digitalizarea poate fi promovată de către managementul superior prin:

— Suportul de training: alocați timp pentru stimularea dezvoltării abilităților digitale ale angajaților

— Crearea unui mediu de lucru pozitiv și constructiv care să încurajeze utilizarea uneltelor IT. Dezvoltarea unor sisteme de recunoaștere și/sau sisteme stimulatoare pentru adoptarea digitalizării. Învățarea membrilor organizației cum să-și împărtășească și promoveze experiența proprie.

— Comunicare: susțineți schimbul deschis și sincer de idei și soluții între angajați, în relație cu digitalizarea și adoptarea practicilor digitale.

— Încurajarea deschiderii și colaborării: cooperarea dintre diferiți actori interni și externi este esențială pentru digitalizare. O organizație digitală prietenoasă ce încurajează colaborările construiește respectul reciproc și furnizează mijloace de comunicare.

— Conștientizarea conflictelor: un anumit nivel de conflict încurajează dezbaterile și creativitatea, fiind esențial în procesul de digitalizare. Ar trebui gestionat în mod activ ca o potențială sursă de îmbunătățire .

— Toleranța la erori: Organizația trebuie să accepte faptul că procesul de digitalizare vine cu niște provocări și, de asemenea, cu riscuri. O organizație favorabilă procesului de digitalizare se concentrează pe aspectul de învățare din eșecuri, fiind precaută în ceea ce privește sancționările negative.

Arhitectura IT, infrastructura IT și portofoliul de aplicații

Instituția trebuie să ruleze un proiect specific pentru evaluarea periodică a arhitecturii sistemului informatic și infrastructurii IT pentru a-și atinge viziunea de digitalizare și strategia aferentă.

În baza concluziilor din procesul de evaluare se întreprind activități pentru actualizarea sistemului informatic și implementarea celei mai adecvate soluții tehnic-economice.

Instituția trebuie să monitorizeze portofoliul de aplicații din perspectivă funcțională și de atingere a obiectivelor strategice. În funcție de situație, instituția trebuie să întreprindă acțiuni pentru actualizarea portofoliului de aplicații.

Organizarea resursei umane pentru digitalizare, competențele IT ale angajaților și instruirea pentru utilizarea sistemelor informatice

Managementul de top trebuie să demonstreze angajament și atitudine de conducere în ceea ce privește digitalizarea prin:

— Asigurarea faptului că viziunea de digitalizare, strategia, politicile și obiectivele sunt stabilite și sunt compatibile cu direcția strategică a organizației;

— Promovarea unei culturi care sprijină procesul de digitalizare;

— Asigurarea integrării procesului de digitalizare în procesele de livrare a serviciilor organizației;

— Asigurarea faptului că resursele (umane și financiare) necesare pentru procesul de digitalizare sunt disponibile;

— Comunicarea importanței, prin intermediul organizației, a managementului efectiv al procesului de digitalizare;

— Asigurarea faptului că procesul de digitalizare conduce la beneficiile dorite;

— Îndrumarea și susținerea personalului pentru a contribui la eficacitatea procesului de digitalizare ;

— Promovarea îmbucătirii continue a digitalizării;

— Susținerea altor roluri relevante de management în ceea ce privește capacitatea lor de a contribui la procesul de digitalizare.

Managementul de vârf trebuie să asigure faptul că responsabilitățile și autoritatea pentru rolurile relevante în ceea ce privește procesul de digitalizare sunt asignate și comunicate în interiorul organizației.

Managementul de vârf trebuie să asigneze responsabilitatea și autoritatea pentru:

- asigurarea faptului că procesul de digitalizare se conformează recomandărilor Specificațiilor Tehnice

— raportarea performanțelor digitalizării către management de vârf.

Sistemul de management al sistemului de informatizare ar trebui să încorporeze o abordare strategică a resurselor umane. Politica resurselor umane trebuie:

— să promoveze învățarea în scopul dobândirii deprinderilor aferente digitalizării;

— să implementeze o proiectare a sarcinilor care să permită utilizarea instrumentelor digitale;

— să încurajeze interacțiunea deschisă, încrederea, diversitatea și toleranța;

— să furnizeze proceduri pentru contractele angajaților care să asigure stimulente adecvate în vederea adoptării digitalizării;

— să încurajeze participarea și reprezentarea în procesul de digitalizare a persoanelor din cadrul organizației, atunci când acest lucru este adecvat;

- să permită persoanelor accesul la informația relevantă de management.

Managementul ciclului de viață al sistemului informatic

Realizarea de sisteme informatice complexe se materializează într-o multitudine de aplicații digitale. Ciclul de viață al unui sistem informatic este constituit din următoarele etape:
— elaborarea temei de realizare;
— proiectarea ansamblului;
— proiectarea în detaliu;
— elaborarea de programe;
— implementare si testare;
— punere în funcțiune, experimentare și acceptare sistem;
— exploatare și întreținere.

Elaborarea temei de realizare a sistemelor informatice are drept obiective:
— identificarea cerințelor și restricțiilor globale pentru realizarea sistemului;
— delimitarea ariei de aplicabilitate;
— justificarea necesității, oportunității și fezabilității modelului funcțional global al noului sistem adoptat în comparație cu alte soluții;
— stabilirea cadrului tehnologic de realizare și de control al calității.

În cazul sistemelor complexe analiza efectuată în vederea elaborării temei de realizare a sistemelor informatice se efectuează în două etape: o analiză preliminară care identifică și definește aria de întindere a sistemului informatic ce urmează a fi analizat și o analiză detaliată în care se realizează cunoașterea detaliată a funcționării sistemului și a particularităților sale.

În cadrul analizei preliminarii se urmărește atingerea următoarelor obiective:
— raționalizarea sistemului informatic, urmărindu-se preponderent îmbunătățirea componentelor sale;
— creșterea calității informațiilor care circulă în sistem, a vârstei și acurateței acestora prin dezvoltarea în cadrul sistemului a unor subsisteme informatice.

În cadrul analizei detaliate se parcurg etapele:
— analiza documentelor din sistem;
— analiza fluxurilor informaționale;
— evidențierea cerințelor decizionale;
— evaluarea critică a sistemului informațional.

Prin analiză se descompune întregul în elementele lui componente și se studiază fiecare dintre acestea. Prin analiză se evidențiază factorii principali și secundari ai întregului precum și cauzele și condițiile care au acționat, le-au generat sau influențat, în sensul realizării întregului, indiferent de forma de manifestare a acestora. Drumul parcurs de analiză este invers drumului parcurs de fenomen: analiza pornește de la rezultat către elementele componente și factori. Analiza poate fi completată prin sinteză. Cu ajutorul acesteia sunt adunate la un loc toate elementele constitutive, punându-se accent pe dobândirea imaginii integrale ale fenomenului studiat. Prin completarea analizei cu sinteza, cu realizarea de raționamente și cu apelarea la abstractizări se ajunge la diagnoză.

Diagnoza reprezintă capacitatea de discernământ, de cunoaștere a tuturor formelor de manifestare a unui subiect sau fenomen în scopul influențării drumului pe care îl va parcurge acesta.

Diagnosticarea sistemului informatic în vederea identificării punctelor sale forte și slabe se poate realiza prin tehnica SWOT. Când se utilizează tehnica SWOT pentru diagnosticarea sistemelor informatice se caută răspunsul la întrebările:
— care sunt avantajele sistemului informatic existent, abordat prin prisma interacțiunilor sale cu sistemele decizional și organizatoric?

— ce caracteristici favorabile prezintă sistemul informațional, în ceea ce privește modul de structurare a datelor, informațiilor și cunoștințelor, precum și în organizarea fluxurilor și circuitelor informaționale?
— care este gradul de manifestare a deficiențelor generale și specifice ale sistemului informațional?
— care sunt avantajele și dezavantajele care rezultă dintr-o analiză comparativă cu organizațiile concurente?
— care sunt schimbările externe care au un efect benefic asupra sistemului de management al organizației și care nu au efect benefic?
— care este gradul de satisfacere a cerințelor formulate de factorii de decizie din organizație?

Rezultatul activităților din aceasta etapă se materializează sub forma temei de realizare a sistemului informatic. Această temă va cuprinde baze de elaborare a temei de proiectare, cerințele și restricțiile globale pentru realizarea sistemului informatic, precum și o justificare a necesităților și oportunităților realizării acestui sistem. Obiectivul fundamental al proiectării îl reprezintă definirea conceptului general și detaliat al noului sistem și a componentelor sale informatice.

Obiectivele principale ale proiectării de ansamblu sunt:
— specificarea cerințelor și restricțiilor pentru proiectarea noului sistem;
— elaborarea modelului de ansamblu a noului sistem informatic;
— stabilirea grafului de ordonare a exploatării componentelor funcționale și a cerințelor privind asigurarea informațională;
— estimarea necesarului de testare pentru realizarea și punerea în funcțiune a noului sistem și a eficienței economice;
— planificarea realizării și punerii în funcțiune a noului sistem;
— planificarea testării.

Întocmirea unui proiect de ansamblu presupune existența unor date de intrare, rezultate din tema de realizare, ca și opțiunea pentru aplicarea anumitor metode și tehnici de realizare. Proiectarea de ansamblu se finalizează printr-un proiect de ansamblu.

Obiectivele principale ale proiectării de detaliu sunt:
— analiza și specificarea cerințelor de detaliu;
— elaborarea modelului de detaliu (integral sau pe părți componente) - proiectarea arhitecturii componentei funcționale;
— stabilirea soluțiilor tehnice de realizare;
— planificarea realizării și punerii în funcțiune a componentelor funcționale;
— planificarea testării.

Proiectarea de detaliu se finalizează prin:
— proiectul de detaliu al componentei funcționale;
— specificația de testare;
— raportul de evaluare al etapei;
— planul de punere în funcțiune.

Realizarea proiectării presupune parcurgerea mai multor etape:
— prezentarea soluțiilor de perfecționare a sistemului informatic:
    - soluții care vizează perfecționarea componentelor informaționale (circuitele, fluxurile și procedurile informaționale);
    - soluții care prevăd trecerea la prelucrarea automată pentru anumite activități din cadrul noului sistem;
— identificarea subsistemelor informatice definite în faza precedentă, cărora le corespund costuri antecalculate supradimensionate;
— prezentarea logică a sistemului informatic:

- prezentarea situațiilor informaționale furnizate de noul sistem și destinațiile acestora;
- definirea conceptului și a structurii generale a bazei de date asociate sistemului;
- elaborarea schemei logice de sistem pentru redarea sub formă grafică a succesiunilor procedurilor automate, a tipurilor de erori semnalate de noul sistem și modul de eliminare a acestora, precum și evidențierea interfețelor dintre sistemul informațional și subsistemele sale informatice.

— proiectarea detaliată a sistemelor informatice:
  - prezentarea analitică a conținutului rapoartelor finale, prin precizarea algoritmilor;
  - descrierea modului de lucru al fiecărei proceduri automate din schema de sistem cu precizarea intrărilor, a ieșirilor și cu descrierea algoritmilor folosiți în aceste proceduri;
  - evidențierea schemelor logice de program din care să rezulte variabilele de stare corespunzătoare fiecărui program;
  - redarea modelelor economic-matematice folosite în procedurile automate într-o manieră clară care să permită înțelegerea metodelor de rezolvare folosite;
  - cuantificarea impactului implementării noului sistem asupra componentelor sistemului de management și a factorului uman din cadrul său;
  - validarea modului de lucru al procedurilor automate prin testarea funcționării acestora cu date care au caracteristici asemănătoare cu cele reale;
— elaborarea unui program de măsuri privind implementarea sistemului.

În cadrul programelor de măsuri se includ responsabilitățile ce revin factorilor de decizie și personalului de execuție în procesul de implementare, cu precizarea termenelor de finalizare a fiecărei acțiuni și a persoanelor care răspund de realizarea ei.

În cadrul elaborării de programe, principalele obiective sunt:
— proiectarea, realizarea și testarea programelor;
— elaborarea documentației de întreținere (programe și date);
— pregătirea testării.

Rezultatele etapei de elaborare programe sunt materializate în:
— specificația de realizare a programelor;
— specificația de testare;
— raport de testare si listinguri martor;
— documentația de întreținere;
— raportul de evaluare a etapei.

Prin procesul de implementare se înțelege, de regulă, ansamblul activităților desfășurate și a măsurilor organizatorice luate care asigură înlocuirea vechiului sistem cu cel proiectat. În perioada de implementare este absolut obligatoriu să nu se neglijeze aspecte legate de pregătirea personalului utilizator. Neglijarea aspectului pregătirii utilizatorilor duce întotdeauna la o eficiență scăzută a noului sistem, dacă nu chiar la compromiterea întregii lucrări.

Testarea infrastructurii hard și soft se face pe baza unor scenarii stabilite de comun acord între furnizor și beneficiar.

Punerea în funcțiune / experimentarea și acceptarea sistemului constă, în principal, din următoarele activități:
— acțiuni pregătitoare punerii în funcțiune:
  - instruire personal;
  - măsuri organizatorice;
  - măsuri tehnice;
— punerea în funcțiune propriu zisă;
— test de acceptanță / recepție, recepție sistem;

— actualizarea documentației / componentelor funcționale.

Se vor elabora următoarele documente:
— documentele de utilizare exploatare;
— documentația de întreținere;
— biblioteci sau fișiere cu componente software.

Exploatarea și întreținerea corectă a sistemului informatic are în vedere:
— funcționarea de durata a sistemului fără incidente, cu disponibilitate maximă;
— respectarea parametrilor proiectați;
— întreținerea sistemului;
— control, probe și verificări;
— actualizarea documentației.

Evaluarea și planificarea performanței sistemului informatic

Instituția trebuie să pună la punct un model – bazat pe criterii detaliate și ponderate – a performanței sistemului informatic. Pe baza acestui model se elaborează un audit al performanței. Rezultatele obținute sunt analizate în raport cu valori țintă. Decalajele sunt analizate și în funcție de impactul acestora se fundamentează un plan de îmbunătățire a sistemului informatic, cu stabilirea țintelor de natură tehnică și a termenelor de implementare.

Se elaborează un plan de acțiune, cu proiecte concrete și se caută soluții de finanțare a planului de acțiune.

Determinarea costurilor pe ciclu de viață al aplicațiilor utilizate

Pentru fiecare aplicație utilizată de către instituție se menține un document de monitorizare a costurilor și economiilor generate prin utilizarea aplicației, precum și efectele multiplicatoare generate (cuantificate tot în unități monetare).

Optimizarea pentru maximizarea valorii către cetățeni și alte părți interesate a portofoliului de aplicații

Organizația trebuie să scaneze și să analizeze în mod regulat mediul extern, pentru a identifica provocările prezente și viitoare. Organizația trebuie să analizeze în mod regulat capabilitățile sale curente și viitoare privind managementul procesului de digitalizare.

Organizația trebuie să determine părțile interesate care sunt relevante în procesul de digitalizare și să identifice nevoile acestora, așteptările și cerințele lor. Părțile interesate sunt divizate în cele externe organizației, respective în cele din interiorul ei (e.g. angajați, management de vârf, departamente).

Părțile interesate trebuie implicate și consultate pentru a-și identifica nevoile și așteptările, care pot fi explicite sau implicite. În particular, este important pentru organizație să înțeleagă nevoile cetățenilor, precum și ale contributoriilor la bugetul public și, de asemenea, nevoile lor încă neîntâlnite și nearticulate.

Dezvoltarea și execuția planului de acțiune

În conformitate cu viziunea și strategia sa asupra digitalizării și cu obiectivele corespondente, organizația trebuie să definească un proces detaliat de digitalizare, acoperind toți pașii relevanți, de la obținerea unei înțelegeri asupra unei probleme la o oportunitate de lansare reușită. Procesul de digitalizare este foarte dependent de asemenea aspecte, de tipul organizației și de structura internă a acesteia, existând astfel căi de rezolvare multiple.

Monitorizarea și controlul planului de acțiune

Echipa executivă a planului de acțiune va monitoriza progresul in timp real utilizând platforme software specializate pentru managementul agil al proiectelor de informatizare. O detaliere la nivelul fiecărui proiect se va face în momentul punerii în practică a proiectului, caz în care se va respecta următoarea procedură de lucru:

- Pentru fiecare proiect se numește un responsabil din rândul membrilor echipei de monitorizare, care va coordona buna derulare a acestuia.
- Pentru a asigura finalizarea cu succes a proiectului, se va pune în aplicare următoarea metodologie:

Pas 1: Definirea clară a obiectivelor
Pas 2: Dezvoltarea cadrului de lucru
Pas 3: Pentru fiecare proiect se va identifica dacă:
-toate cerințele referitoare la performante, costuri, timp și scop sunt îndeplinite
-toate riscurile identificate sunt în marja de acceptabilitate
-toate consecințele sunt acceptabile
Pas 4: Daca toți factorii de la pasul 3 sunt în regulă, se va dezvolta planul de implementare, incluzând evaluarea duratei de timp și evaluarea riscului
Pas 5: Evaluarea planului de implementare cu membrii echipei
Pas 6: Daca pasul 5 este in regula se va elabora „lista de sarcini"
Pas 7: Se va executa planul
Pas 8: Se va verifica periodic progresul în raport cu ce a fost planificat
Pas 9: Dacă progresul nu este acceptabil se vor aplica metode de minimizare tehnică a riscului
Pas 10: Când toate sarcinile sunt finalizate, se va derula auditul final al proiectului
Pas 11: Se vor trage concluzii și trasa sarcini pentru viitor

Îmbunătățirea continuă și adaptarea sistemului de management pentru digitalizare instituțională

Organizația trebuie să îmbunătățească în mod continuu gradul de potrivire, eficacitatea sistemului informatic, prin utilizarea viziunii și strategiei de digitalizare, a obiectivelor și planificării, facilității de digitalizare / factorilor de conducere, evaluarea performanței și revizuirea managementului superior.

Organizația trebuie să identifice deviațiile și să stabilească acțiuni corective în vederea eliminării cauzelor deviațiilor identificate, sau să stabilească acțiuni în vederea îmbunătățirii eficienței și a rezultatelor sistemului de informatizare și a sistemului de management aflat în relație cu acesta.

Trebuie definite, de asemenea, o foaie de parcurs cu metrici pentru a elimina slăbiciunile identificate, precum și pentru a întări în continuare punctele tari ale sistemului de informatizare și ale sistemului de management aflat în relație cu acesta. Implementarea măsurilor de îmbunătățire trebuie monitorizată cu privire la programul definit, la îndeplinirea task-urilor definite, respectiv la impactul așteptat de pe urma măsurilor privind sistemul de informatizare, respectiv sistemul de gestionare aferent.

Pentru a stimula învățarea și îmbunătățirea continua în cadrul organizației, măsurile privind îmbunătățirea și succesul trebuie comunicate în cadrul organizației și, pe cât posibil, părților externe interesate.

Îmbunătățirea continuă și adaptarea sistemului informatic

Organizația trebuie să stabilească indicatorii, metodele de monitorizare și criteriile de evaluare, cel puțin pentru:

— strategia de digitalizare;

— implementarea factorilor de declanșare a digitalizării / a factorilor de conducere ;

— procesul de digitalizare și rezultatele sale.

Evaluarea trebuie efectuată în mod regulat pentru a asigura o înțelegere aprofundată a diferitelor dimensiuni ale managementului digitalizării și îmbunătățirea continuă a performanțelor sistemului de management pentru informatizare. Frecvența sistemului de management pentru evaluarea informatizării depinde de dinamica mediului în care operează organizația, precum și de ambiția organizației în ceea ce privește îmbunătățirea performanțelor managementului digitalizării.

Pe lângă alte metode de evaluare, trebuie efectuată o verificare internă la intervale definite pentru a verifica performanța sistemului de management al informatizării implementat în cadrul organizației.

Managementul de vârf trebuie să revizuiască sistemul de management al informatizării organizației pentru a se asigura că este adecvată și eficient în continuare.

Această revizuire realizată de către conducere trebuie să includă:

— statusul acțiunilor, în conformitate cu reviziile precedente ale managementului superior;

— modificări în contextul intern și extern, relevante pentru sistemul de management al informatizării;

— informarea asupra performanței sistemului de management al informatizării ;

— oportunități pentru îmbunătățire continuă.

Rezultatele analizei de top management trebuie să includă decizii legate de oportunitățile de îmbunătățire continuă și orice necesitate de modificare a sistemului de management al informatizării.

Organizația trebuie să păstreze informațiile documentate ca dovadă a rezultatelor analizelor conducerii.

Rezultatele recenziilor trebuie comunicate în cadrul organizației pentru a contribui la îmbunătățirea performanței și a evita greșelile repetate și duplicarea inutilă a muncii.

Identificarea, susținerea și dezvoltarea factorilor suport ai digitalizării instituționale

Organizația trebuie să definească două responsabilități principale în contextul digitalizării:

— responsabilitățile pentru proiectele specifice de digitalizare;

— responsabilitățile pentru managementul general al digitalizării.

În funcție de mărimea și structura organizației, responsabilitățile de gestionare a digitalizării pot fi atribuite unei unități structurate, unei echipe sau unei singure persoane din cadrul organizației (chiar și în regim part-time, dacă este cazul).

Responsabilitățile generale de management al digitalizării trebuie să includă :

— asigurarea unei gestionări eficiente a digitalizării, conform recomandărilor din această specificație tehnică

— dezvoltarea planificării operaționale;

— inițierea și conducerea procesului de digitalizare;

— atribuirea pentru fiecare proiect a responsabilităților proiectului de digitalizare și, dacă este necesar, se poate include subcontractarea unor experți externi pentru anumite sarcini sau proiecte în care este identificat un decalaj în expertiza internă;

— coordonare în cadrul proiectului de digitalizare;

— raportarea către conducerea de vârf a progresului și performanței .

Responsabilitățile în legătură cu procesul de digitalizare trebuie atribuite, privind fiecare proiect, unei echipe sau unei persoane din cadrul organizației pe baza aptitudinilor și capabilităților acesteia.

Responsabilitățile privind proiectul de digitalizare, trebuie să include cel puțin:

— realizarea proiectului de digitalizare asignat și a obiectivelor acestuia ;

— utilizarea uneltelor de inovare necesare în proiect ;

— raportarea, către managementul superior, a progresului în cadrul proiectului.

Organizația trebuie să determine și să furnizeze resursele necesare pentru stabilirea, implementarea, mentenanța, și îmbunătățirea continua a procesului de digitalizare (e.g. resurse umane, echipamente, facilități și bugete).

Organizația trebuie:

— să determine competențele necesare ale persoanelor care lucrează în cadrul unor activități de digitalizare;

— să se asigure că aceste persoane sunt competente pe baza educației, formării și experienței adecvate;

— după caz, să ia măsuri pentru a dobândi competența necesară și pentru a evalua eficacitatea acțiunilor întreprinse;

— să îmbunătățească continuu abilitățile și capacitățile necesare pentru îmbunătățirea performanței digitalizării.

Acțiunile aplicabile pot include, de exemplu: furnizarea de instruire, îndrumarea angajaților curenți, sau angajarea sau contractarea de persoane și / sau organizații competente.

Persoanele care lucrează sub controlul organizației trebuie să fie conștiente și motivate în legătură cu importanța digitalizării pentru organizație, cu viziunea și strategia de digitalizare și cu importanța contribuției acestora la eficacitatea sistemului de management al informatizării, inclusiv a beneficiilor unei performanțe digitale îmbunătățite. O cultură puternică de digitalizare poate oferi acest lucru.

Organizația trebuie să stabilească comunicări interne și externe relevante pentru sistemul de management al informatizării, ținând seama de aspecte cum ar fi: obiectul comunicării (ce trebuie comunicat), momentul, părțile între care are loc comunicarea, furnizarea canalelor de comunicare și feedbackul dorit.

Sistemul de management al informatizării organizației trebuie să includă informații documentate, determinate de organizație ca fiind necesare pentru eficacitatea sistemului de management al

informatizării și dovezile privind performanța acestuia, derivate din aplicarea prezentei specificații tehnice.

Documentația trebuie creată, identificată, distribuită, actualizată, stocată, controlată și protejată, după caz.

Planificarea programului de digitalizare instituțională

Atunci când planifică digitalizarea, organizația trebuie să ia în considerare problemele externe și interne, nevoile și așteptările, respectiv viziunea și strategia de digitalizare și să determine riscurile și oportunitățile care trebuie abordate pentru:

— asigurarea faptului că digitalizarea poate duce la atingerea rezultatelor propuse;

— prevenirea, sau reducea, efectelor nedorite;

— obținerea unui proces de optimizare continuă.

Organizația trebuie să planifice acțiuni pentru a aborda aceste riscuri și oportunități, respectiv să stabilească cum să integreze și să pună în aplicare acțiunile în procesele sale de digitalizare și să evalueze eficacitatea acestor acțiuni.

În toate activitățile de digitalizare, riscul și incertitudinea ar trebui luate în considerare. Organizația trebuie să stabilească obiective de digitalizare privind funcții și niveluri relevante. Obiectivele de digitalizare trebuie să fie consistente cu viziunea și strategia de digitalizare comunicată, măsurabilă sau practicabilă, monitorizată și actualizată în mod corespunzător. Organizația trebuie să rețină informație documentată asupra obiectivelor de digitalizare. Atunci când se planifică realizarea obiectivelor sale de digitalizare, organizația trebuie să determine activitățile, resursele, responsabilitățile și reperele factorilor de declanșare a digitalizării / factorilor de conducere și procesul de management al digitalizării și să stabilească indicatorii de monitorizare a succesului pe termen scurt și lung al digitalizării.

Managementul programului de digitalizare instituțională

Organizația trebuie să definească o politică de colaborare internă și externă. Colaborarea în cadrul organizației ar trebui promovată astfel încât ideile și cunoștințele despre digitalizare să poată fi partajate între diferite persoane, grupuri și unități, prin:

— diseminarea provocărilor și a stimulilor pentru idei și rezolvarea problemelor (provenite de la angajați, informații strategice etc.);

— încurajarea persoanelor și grupurilor (cu o diversitate de perspectivă) să colaboreze pentru a dezvolta idei și a împărtăși cunoștințe.

Colaborarea cu organizațiile externe poate ajuta la identificarea ideilor, a nevoilor clienților, a cunoștințelor și a partenerilor, pentru a ajuta atât la rezolvarea problemelor, cât și la exploatarea ideilor. Oportunitățile pot fi identificate prin:

— ascultarea activă și adoptarea ideilor de la cetățeni, furnizori și alte părți;

— reunirea rețelelor de transfer de cunoștințe, organisme profesionale;

— colaborarea cu Clusterul Cluj IT, sau punerea în funcțiune a inițiativelor acestui Cluster, care să contribuie la dezvoltarea digitalizării.

Managementul proiectelor de informatizare

Este recomandată dezvoltarea proceselor de digitalizare prin adoptarea unei metodologii adecvate: de exemplu, un proces "phase-gate" sau un proces de gândire digitalizat, sau combinația acestora. Primul beneficiu al unui proces phase-gate este disciplina pe care acesta o impune în elaborarea unui plan detaliat al proiectului, având obiective clare și livrabile rezultate de pe urma acestuia.

In cadrul fiecărei faze, este util a se pune la punct cel puțin următoarele detalii:

— obiectivele și rezultatele așteptate ale fazei;

— task-uri de realizat;

— resurse (umane, budgetare și facilități) de îndeplinit;

— etapele necesare, inclusiv datele de începere și de finalizare;

— revizii formale pentru a marca evoluția de la o fază a proiectului la alta, sau pentru a finaliza proiectul și a capta învățarea pentru proiecte viitoare;

— strategii de atenuare a riscurilor;

— instrumente și tehnici care ar putea facilita digitalizarea.

Atunci când se ajunge la o situație cu mai multe proiecte, organizația trebuie să stabilească o gestionare integrată a portofoliului de proiecte, ținând cont de aspecte precum:

— potrivire cu priorități în funcție de viziunea, strategia și obiectivele digitalizării;

— echilibru al proiectelor pe termen scurt / lung, proiecte cu risc ridicat / risc scăzut etc .;

— monitorizarea globală a progresului proiectelor luând în considerare noi elemente provenind din informațiile strategice, în special impactul evoluției contextului intern sau extern asupra proiectului în curs;

— optimizarea resurselor partajate.

Conform strategiei de digitalizare a organizației, rezultatele proiectului de digitalizare trebuie să fie protejate și exploatate în mod adecvat.

Auditul performanței în direcția digitalizării

Rezultatele procesului de digitalizare pentru organizație sunt atât financiare, cât și nefinanciare. Organizația ar trebui să precizeze de câte ori, în raport cu ce anume și de către cine ar trebui să fie evaluate rezultatele. Organizația trebuie să definească indicatori pentru evaluarea rezultatelor digitalizării. Indicatorii financiari privind aceste rezultate pot include:

— productivitatea internă;

— economii de cost pentru organizație și clienți;

— creșterea marjei de funcționare;

— rentabilitatea investițiilor în digitalizare.

Indicatorii non-financiari pot include:

— numărul de proiecte de digitalizare;

— satisfacția cetățenilor;

— eficiența proceselor;

— reputația;

— impactul asupra numărului de angajați ca rezultat al digitalizării;

Evaluarea rezultatelor față de acești indicatori trebuie să ofere feedback asupra succesului și eșecului, respectiv asupra învățării pentru îmbunătățirea în continuare a procesului de management al digitalizării.

„Controllingul" financiar-contabil al sistemului informatic

O acțiune importantă în controlul și optimizarea costurilor referitoare la sistemul informatic o reprezintă planificarea costurilor care se realizează prin procesul de bugetare. Analiza cost-volum-beneficiu (economii interne) (CVB) este un instrument important în planificare. Prin intermediul acesteia, instituția va analiza cum evoluează beneficiile (economiile interne) în diverse scenarii de acțiune și va analiza scenariul cel mai benefic. Pentru controlul costurilor cu sistemul informatic, monitorizarea costurilor pe centre de responsabilitate este un instrument important.

Pentru maximizarea economiilor trebuie să identifice care sunt segmentele de activitate care adaugă valoare reală pentru beneficiari și cele care aduc mai puțină valoare pentru beneficiarii finali sau chiar pierderi pentru societate în general.

Atunci când instituția își planifică niște obiective generale (o economie internă de X RON) acestea sunt desfășurate în cascadă ca responsabilitate către diverse compartimente. Astfel bugetul general pentru sistemul informatic se va detalia la nivel de centre de responsabilitate.

Ulterior rezultatele reale vor fi monitorizate prin intermediul rapoartelor pe centre de responsabilitate. Această informație este foarte importantă pentru luarea deciziilor corecte de îmbunătățire. De asemenea, această monitorizare permite măsurarea și recompensarea performanței în instituție în funcție de rezultate.

Evaluarea rezultatelor digitalizării la nivelul satisfacției angajaților și beneficiarilor

Instituția trebuie să identifice periodic efectele digitalizării asupra angajaților, cetățenilor și altor părți interesate. În acest sens, instituția trebuie să asigure resurse necesare sondării acestor actori. Rezultatele trebuie aduse la cunoștința factorilor de decizie și apoi propuse măsuri de îmbunătățire.

FISA DE PROIECT FANION

Titlu

Consolidarea securității cibernetice în Primăria Bistrița

Coordonator din partea consultantului

Stelian Brad

Rezumat

Titlul proiectului: Consolidarea securitatii cibernetice in Primaria Bistrita

Scopul acestui proiect este de a consolida securitatea cibernetica in Primaria Bistrita prin imbunatatirea capacitatiilor de detectare, prevenire si raspuns la incidente cibernetice.

Se urmareste analiza avansata a informatiilor privind amenintarile persistente, testarea Cyberrange, raportarea managementului riscului de securitate cibernetica, monitorizarea vulnerabilitatii securitatii cibernetice, inteligenta cibernetica a amprentei digitale, raspuns la incident, aviz Pentest, evaluarea securitatii tehnice, precum si organizarea de training-uri in securitate cibernetica pentru angajatii Primariei Bistrita si cetatenii din comunitate.

Beneficiarii acestui proiect sunt reprezentati de angajatii si cetatenii din comunitatea locala, care vor beneficia de o infrastructura mai sigura si mai rezistenta la atacuri cibernetice.

Context si justificare: Primaria Bistrita are nevoie de consolidarea securitatii cibernetice pentru a asigura protectia informatiilor confidentiale si a datelor personale ale cetatenilor, precum si a sistemelor si infrastructurii IT. Amenintarile cibernetice sunt in continua crestere si pot avea consecinte grave pentru Primarie si comunitatea locala. Acest proiect se justifica prin necesitatea de a raspunde la aceste amenintari si de a asigura o infrastructura sigura si protejata impotriva atacurilor cibernetice.

Obiectivele pe termen lung si scurt ale proiectului sunt:
- Sa imbunatateasca capacitatea de detectare si prevenire a amenintarilor cibernetice prin analiza avansata a informatiilor privind amenintarile persistente, testarea Cyberrange, raportarea managementului riscului de securitate cibernetica si monitorizarea vulnerabilitatii securitatii cibernetice.
- Sa consolideze capacitatea de raspuns la incidente cibernetice prin organizarea de training-uri in securitate cibernetica si prin evaluarea vulnerabilitatii din punct de vedere al resurselor umane, tehnologiei si politicii de securitate.
- Sa creasca nivelul de securitate cibernetica prin evaluarea securitatii tehnice, investitii in tehnologie pentru monitorizarea dispozitivelor mobile si a sistemului si infrastructurii IT, precum si prin organizarea de training-uri in securitate cibernetica pentru angajatii Primariei Bistrita si cetatenii din comunitate.

Rezultatele asteptate ale proiectului includ:
- infrastructura mai sigura si mai rezistenta la atacurile cibernetice
- mai buna capacitate de detectare si prevenire a amenintarilor cibernetice
- mai buna capacitate de raspuns la incidente cibernetice
- angajatii Primariei Bistrita si cetatenii din comunitatea locala vor fi mai bine informati si pregatiti pentru a face fata amenintarilor cibernetice
- reducerea riscului de pierdere a datelor personale si informatiilor confidentiale ale cetatenilor
- cresterea increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale

Proiectul va fi implementat in 18 luni.

Activitatile principale ale proiectului:
- Analiza avansata a informatiilor privind amenintarile persistente
- Testarea Cyberrange
- Raportarea managementului riscului de securitate cibernetica
- Monitorizarea vulnerabilitatii securitatii cibernetice
- Inteligenta cibernetica a amprentei digitale

- Raspuns la incident
- Aviz Pentest
- Evaluarea securitatii tehnice
- Formare profesionala - Apărător Cyber Security
- Formare profesionala - Clădiri inteligente și securitatea clădirilor
- Formare profesionala - Securitate cibernetică pentru toată lumea
- Formare profesionala - Specializare in securitate cibernetica pentru sectorul public
- Evaluarea vulnerabilității din punct de vedere al resurselor umane
- Evaluarea vulnerabilității din punct de vedere al tehnologiei
- Evaluarea vulnerabilității din punct de vedere al politicii de securitate
- Investiții în tehnologie pentru monitorizarea dispozitivelor mobile din perspectiva securității cibernetice
- Investiții în tehnologie pentru monitorizarea sistemului și infrastructurii IT din perspectiva securității cibernetice
- Implementarea de solutii de securitate a datelor pentru a asigura protectia datelor cu caracter personal si confidential ale cetatenilor
- Dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica
- Auditul de securitate cibernetica pentru toate aplicatiile si sistemele IT utilizate de Primaria Bistrita
- Implementarea de solutii de securitate a retelelor si a infrastructurii IT, inclusiv firewall-uri, sisteme de detectare a intrusilor si sisteme de autentificare multi-factor
- Testarea exhaustiva a angajatilor pe GDPR si securitate cibernetica si sensibilizarea angajatilor Primariei Bistrita privind amenintarile cibernetice si metodele de prevenire a acestora.

Responsabilitati:
Echipa de proiect va fi formata din specialisti in securitate cibernetica si IT, care vor fi responsabili de implementarea activitatilor proiectului. Primaria Bistrita va fi responsabila de supervizarea si coordonarea proiectului, asigurand o buna comunicare intre membrii echipei de proiect.

Termene:
Implementarea proiectului va avea o durata de 18 luni, dupa cum urmeaza:

1. Analiza avansata a informatiilor privind amenintarile persistente - 2 luni
2. Testarea Cyberrange - 1 luna
3. Raportarea managementului riscului de securitate cibernetica - 2 luni
4. Monitorizarea vulnerabilitatii securitatii cibernetice - 3 luni
5. Inteligenta cibernetica a amprentei digitale - 3 luni
6. Raspuns la incident - 2 luni
7. Aviz Pentest - 1 luna
8. Evaluarea securitatii tehnice - 2 luni
9. Formare profesionala - Apărător Cyber Security - 1 luna
10. Formare profesionala - Clădiri inteligente și securitatea clădirilor - 1 luna
11. Formare profesionala - Securitate cibernetică pentru toată lumea - 1 luna
12. Formare profesionala - Specializare in securitate cibernetica pentru sectorul public - 1 luna
13. Evaluarea vulnerabilității din punct de vedere al resurselor umane - 2 luni
14. Evaluarea vulnerabilității din punct de vedere al tehnologiei - 2 luni
15. Evaluarea vulnerabilității din punct de vedere al politicii de securitate - 2 luni
16. Investiții în tehnologie pentru monitorizarea dispozitivelor mobile din perspectiva securității cibernetice - 5 luni
17. Investiții în tehnologie pentru monitorizarea sistemului și infrastructurii IT din perspectiva securității cibernetice - 5 luni

18. Implementarea de solutii de securitate a datelor pentru a asigura protectia datelor cu caracter personal si confidential ale cetatenilor: 3-6 luni, in functie de complexitatea si volumul de date gestionate.
19. Dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica: 2-3 luni, in functie de complexitatea procedurilor si de numarul de angajati implicati.
20. Auditul de securitate cibernetica pentru toate aplicatiile si sistemele IT utilizate de Primaria Bistrita: 2-3 luni, in functie de numarul si complexitatea aplicatiilor si a sistemelor IT.
21. Implementarea de solutii de securitate a retelelor si a infrastructurii IT, inclusiv firewall-uri, sisteme de detectare a intrusilor si sisteme de autentificare multi-factor: 4-6 luni, in functie de dimensiunea si complexitatea retelei si a infrastructurii IT.
22. Testarea exhaustiva a angajatilor pe GDPR si securitate cibernetica si sensibilizarea angajatilor Primariei Bistrita privind amenintarile cibernetice si metodele de prevenire a acestora: 1-2 luni, in functie de numarul de angajati implicati si de complexitatea informatiilor transmise.

Buget:
Bugetul total al proiectului poate varia in functie de specificul si dimensiunea acestuia, precum si de resursele disponibile. In general, costurile pentru un astfel de proiect pot include:

- Costuri pentru echipamente si solutii de securitate cibernetica (firewall-uri, sisteme de detectare a intrusilor, autentificare multi-factor etc.)
- Costuri pentru training si formare a angajatilor
- Costuri pentru servicii de consultanta in domeniul securitatii cibernetice
- Costuri pentru evaluarea si auditul de securitate cibernetica
- Costuri pentru achizitionarea si implementarea de solutii de securitate a datelor cu caracter personal si confidential ale cetatenilor
- Costuri pentru dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica
- Costuri pentru investitii in tehnologie pentru monitorizarea dispozitivelor mobile si a infrastructurii IT din perspectiva securitatii cibernetice

In functie de specificul si dimensiunea proiectului, bugetul total poate varia intre 250.000 si 500.000 de euro. Este important sa se realizeze o estimare detaliata a costurilor si sa se aloce resursele corespunzator pentru a asigura succesul proiectului si implementarea masurilor de securitate cibernetica necesare pentru protejarea datelor si a infrastructurii IT impotriva atacurilor cibernetice.

Sustenabilitatea proiectului va fi asigurata prin:
- Continuarea investitiilor in tehnologie si formarea angajatilor in domeniul securitatii cibernetice, pentru a asigura o infrastructura sigura si protejata impotriva atacurilor cibernetice pe termen lung.
- Asigurarea unei bune coordonari si comunicari intre membrii echipei de proiect si angajatii Primariei Bistrita, pentru a mentine nivelul ridicat de securitate cibernetica.
- Sensibilizarea si educarea cetatenilor in ceea ce priveste securitatea cibernetica si nevoia de a proteja datele lor personale si confidentiale.

Impactul social, economic si de mediu al proiectului va fi pozitiv si se va manifesta prin:
- Cresterea nivelului de securitate cibernetica in Primaria Bistrita, asigurand protectia informatiilor personale si confidentiale ale cetatenilor si a infrastructurii IT.
- Cresterea increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale.
- Reducerea riscului de pierdere a datelor personale si informatiilor confidentiale ale cetatenilor.
- Reducerea costurilor si a timpului alocat pentru remedierea unui incident cibernetic.

- Contribuirea la dezvoltarea economica si sociala a comunitatii locale prin cresterea increderii cetatenilor in Primaria Bistrita si prin asigurarea protectiei informatiilor confidentiale si a infrastructurii IT.
- Reducerea impactului asupra mediului prin cresterea eficientei si a sigurantei sistemelor IT, reducand astfel consumul de energie si emisiile de gaze cu efect de sera.

Anexe:
Nu sunt necesare anexe la aceasta fisa de proiect.

Context si justificare

In contextul digitalizarii accelerate a serviciilor publice si a cresterei numarului de amenintari cibernetice, Primaria Bistrita a recunoscut nevoia de a consolida securitatea cibernetica in cadrul institutiei si a comunitatii locale. Acest proiect are ca scop protejarea datelor si infrastructurii IT impotriva atacurilor cibernetice, asigurand siguranta si confidentialitatea informatiilor gestionate de Primarie si a datelor cu caracter personal ale cetatenilor.

Amenintarile cibernetice sunt o realitate din ce in ce mai mare, iar in Romania acestea au inregistrat o crestere semnificativa in ultimii ani. Potrivit studiului realizat de Bitdefender in 2020, Romania se afla in topul celor mai afectate tari din Europa de Est, cu o crestere a atacurilor cibernetice cu 140% in 2019 fata de anul anterior. In plus, studiul Kaspersky Lab arata ca in 2020, aproape jumatate dintre companiile din Romania au fost afectate de cel putin un atac cibernetic.

Acest trend se poate observa si la nivelul autoritatilor publice din Romania, unde incidentele de securitate cibernetica au devenit o preocupare tot mai mare. Potrivit unui studiu realizat de SRI, in 2020, peste 50 de autoritati publice din Romania au fost afectate de atacuri cibernetice, iar acest numar este in crestere constanta.

In acest context, Primaria Bistrita a recunoscut nevoia de a lua masuri pentru consolidarea securitatii cibernetice in cadrul institutiei si a comunitatii locale. Obiectivul principal al acestui proiect este de a asigura protectia datelor si infrastructurii IT impotriva atacurilor cibernetice, prin implementarea unor solutii de securitate cibernetica si prin cresterea gradului de constientizare si formare a angajatilor cu privire la amenintarile cibernetice si la modalitatile de prevenire a acestora.

De asemenea, un alt factor care a contribuit la necesitatea consolidarii securitatii cibernetice in Primaria Bistrita este cresterea digitalizarii serviciilor publice. In ultimii ani, Primaria Bistrita a facut eforturi semnificative pentru a oferi cetatenilor servicii publice digitale, cum ar fi plata taxelor si impozitelor online sau accesarea de informatii despre serviciile publice prin intermediul portalului oficial al institutiei. Aceste servicii digitale genereaza o cantitate mare de date cu caracter personal si confidential, ceea ce face necesara implementarea unor solutii de securitate cibernetica eficiente pentru a asigura protectia datelor impotriva atacurilor cibernetice.

Consolidarea securitatii cibernetice in Primaria Bistrita este o necesitate nu numai pentru a proteja datele si infrastructura IT impotriva amenintarilor cibernetice actuale, ci si pentru a se asigura ca institutia este pregatita pentru viitoarele initiative guvernamentale de digitalizare. Legea interoperabilitatii prevede ca toate autoritatile publice trebuie sa utilizeze sisteme informatice interoperabile, astfel incat sa fie posibila schimbul de date si informatii intre diferitele institutii publice.

Implementarea legii interoperabilitatii va implica utilizarea unui cloud guvernamental comun, care va permite accesul la date si informatii de la nivel national, inclusiv din alte autoritati publice. Acest lucru va face Primaria Bistrita vulnerabila la atacuri cibernetice si va face si mai importanta consolidarea securitatii cibernetice in aceasta institutie. Sistemele informatice trebuie sa fie sigure si protejate impotriva atacurilor cibernetice, pentru a asigura confidentialitatea si integritatea datelor stocate.

De asemenea, consolidarea securitatii cibernetice in Primaria Bistrita este importanta si pentru implementarea unei arhive electronice, care va stoca toate documentele si informatiile oficiale ale institutiei. Aceasta arhiva va fi accesibila online si va permite cetatenilor sa acceseze si sa obtina documente oficiale fara a fi necesara deplasarea la Primaria Bistrita. Aceasta solutie va imbunatati transparenta institutiei si va reduce timpul si costurile de administrare a documentelor.

Prin consolidarea securitatii cibernetice in Primaria Bistrita, se va asigura protectia datelor si infrastructurii IT impotriva atacurilor cibernetice. In ziua de azi, riscurile de securitate cibernetica sunt din ce in ce mai frecvente si mai sofisticate, astfel incat institutiile publice sunt vulnerabile la atacuri cibernetice care pot avea consecinte devastatoare. Protectia datelor si infrastructurii IT este, prin urmare, o preocupare majora pentru institutiile publice, inclusiv pentru Primaria Bistrita.

De asemenea, consolidarea securitatii cibernetice va permite Primariei Bistrita sa ofere servicii publice digitale mai sigure si mai eficiente. In ultimii ani, exista o crestere semnificativa a cererii pentru servicii publice digitale, iar Primaria Bistrita nu face exceptie. Cresterea cererii pentru servicii publice digitale, cum ar fi plata taxelor si impozitelor online, inregistrarea actelor de stare civila sau solicitarea de autorizatii online, implica o crestere a cantitatii de date si informatii care trebuie sa fie stocate si protejate impotriva amenintarilor cibernetice. Consolidarea securitatii cibernetice va asigura ca aceste servicii publice digitale sunt mai sigure si mai eficiente, iar cetatenii vor avea mai multa incredere in capacitatea Primariei Bistrita de a le oferi aceste servicii.

Un alt beneficiu important al consolidarii securitatii cibernetice in Primaria Bistrita este cresterea increderii cetatenilor in institutie. Datele cu caracter personal ale cetatenilor sunt stocate si utilizate de catre Primaria Bistrita in mai multe scopuri, cum ar fi administrarea taxelor si impozitelor sau eliberarea de autorizatii. Consolidarea securitatii cibernetice va asigura ca aceste date sunt protejate impotriva atacurilor cibernetice si ca confidentialitatea si integritatea acestora sunt mentinute. Acest lucru va spori increderea cetatenilor in Primaria Bistrita si va demonstra angajamentul institutiei fata de protejarea datelor personale si sensibile ale cetatenilor.

Consolidarea securitatii cibernetice in Primaria Bistrita este esentiala din perspectiva Regulamentului General privind Protectia Datelor (GDPR), care reglementeaza colectarea, prelucrarea si stocarea datelor cu caracter personal ale cetatenilor din Uniunea Europeana. GDPR este o legislatie cruciala in domeniul protectiei datelor personale, care are scopul de a proteja drepturile si libertatile cetatenilor UE in ceea ce priveste prelucrarea datelor cu caracter personal si de a asigura un nivel adecvat de protectie a acestor date.

Consolidarea securitatii cibernetice va permite Primariei Bistrita sa protejeze datele cu caracter personal ale cetatenilor si sa asigure ca acestea sunt prelucrate si stocate in conformitate cu regulile GDPR. Primaria Bistrita colecteaza, stocheaza si prelucreaza date cu caracter personal ale cetatenilor in cadrul unor procese administrative, precum inregistrarea actelor de stare civila, plata taxelor si impozitelor sau eliberarea de autorizatii. In cazul in care aceste date sunt compromise, prin intermediul unui atac cibernetic sau prin alte mijloace, institutia ar putea fi considerata responsabila pentru nerespectarea regulilor GDPR.

In plus, consolidarea securitatii cibernetice va ajuta la identificarea si gestionarea incidentelor de securitate cibernetica care ar putea afecta datele cu caracter personal ale cetatenilor. Regulamentul GDPR prevede ca institutiile publice si companiile trebuie sa raporteze incidentele de securitate cibernetica care afecteaza datele cu caracter personal in termen de 72 de ore. Consolidarea securitatii cibernetice va asigura ca Primaria Bistrita este pregatita sa gestioneze astfel de incidente, sa le raporteze si sa ia masurile necesare pentru a minimiza impactul asupra datelor cu caracter personal ale cetatenilor.

In plus, consolidarea securitatii cibernetice poate avea beneficii semnificative pentru Primaria Bistrita, prin reducerea costurilor si a riscurilor asociate cu nerespectarea regulilor GDPR. GDPR prevede amenzi semnificative pentru institutiile publice si companiile care nu respecta regulile privind protectia datelor cu caracter personal. Consolidarea securitatii cibernetice va ajuta la reducerea riscurilor de nerespectare a regulilor GDPR si la evitarea amenzilor si costurilor asociate.

Implementarea acestui proiect va avea un impact pozitiv semnificativ asupra mediului economic si social local, prin cresterea nivelului de securitate cibernetica in Primaria Bistrita. In timpul ultimelor decenii, dezvoltarea tehnologiei a determinat o crestere semnificativa a dependentei societatii de tehnologie si a resurselor informatice. Acest fapt a creat un cadru favorabil pentru infractiunile cibernetice si a crescut nevoia de securitate cibernetica in toate sectoarele economice si sociale.

Prin cresterea nivelului de securitate cibernetica, Primaria Bistrita poate preveni pierderea de date si informatii confidentiale, care ar putea afecta afacerile si economia locala. Daca informatiile si datele cu caracter personal ale cetatenilor sunt compromise, aceasta poate avea un impact negativ asupra reputatiei Primariei Bistrita, precum si asupra economiei locale, prin pierderea de incredere a cetatenilor si a intreprinderilor in serviciile publice. De asemenea, pierderea de informatii si date poate afecta capacitatea Primariei Bistrita de a lua decizii strategice importante si de a furniza servicii publice de calitate.

Prin formarea si cresterea gradului de constientizare a angajatilor cu privire la amenintarile cibernetice, se poate preveni frauda si alte tipuri de infractiuni cibernetice, care ar putea afecta economia locala si comunitatea. Angajatii care sunt educati si constienti de amenintarile cibernetice sunt mai capabili sa recunoasca si sa previna aceste amenintari si sa protejeze datele si informatiile confidențiale. In plus, formarea angajatilor poate contribui la imbunatatirea eficientei si productivitatii Primariei Bistrita, prin cresterea gradului de constientizare a angajatilor in ceea ce priveste utilizarea responsabila a tehnologiei.

Pe de alta parte, infractiunile cibernetice pot afecta si comunitatea locala, prin compromiterea datelor personale si financiare ale cetatenilor si intreprinderilor din zona. De exemplu, infractorii cibernetici pot accesa si utiliza datele cu caracter personal ale cetatenilor, precum numele, adresa, numarul de telefon sau de card de credit, pentru a comite fraude sau alte infractiuni. Prin consolidarea securitatii cibernetice in Primaria Bistrita, se poate preveni acest tip de infractiuni si se poate proteja comunitatea impotriva acestora.

Mai adaugam aici si alte motive care sustin acest proiect. Un motiv suplimentar este legat de faptul ca securitatea cibernetica este una dintre cele mai importante probleme cu care se confrunta societatea moderna. Infractiunile cibernetice sunt in continua crestere, cu costuri financiare si sociale semnificative, atat pentru indivizi, cat si pentru intreprinderi si organizatii guvernamentale. In plus, vulnerabilitatile cibernetice pot avea consecinte grave, cum ar fi pierderea datelor si informatiilor cu caracter personal, frauda, furtul de identitate sau atacuri asupra infrastructurii critice, precum retelele de electricitate, apa si transport. Al doilea motiv suplimemtar este legat de faptul ca Primaria Bistrita are o responsabilitate speciala in ceea ce priveste securitatea cibernetica, deoarece detine informatii si date cu caracter personal sensibile si confidentiale ale cetatenilor. Aceste date pot include informatii medicale, date bancare, informatii privind impozitele si taxele, informatii privind contractele de munca, informatii privind transportul public si multe altele. Prin consolidarea securitatii cibernetice in Primaria Bistrita, se poate proteja aceste date si se poate asigura confidentialitatea si integritatea lor. Al treilea motiv suplimentar este legat de faptul ca Primaria Bistrita poate deveni un lider in adoptia bunelor practice de securitate cibernetica, nu doar in zona locala, ci si la nivel national. Implementarea acestui proiect poate servi ca un model si un exemplu pentru alte institutii publice din Romania si poate contribui la cresterea imaginii la nivel national.

In ceea ce priveste finantarea acestui proiect, se poate lua in considerare obtinerea de fonduri europene sau guvernamentale pentru securitate cibernetica. De asemenea, Primaria Bistrita poate aloca un buget special pentru implementarea acestui proiect si poate colabora cu companii specializate in securitate cibernetica pentru a identifica cele mai eficiente solutii si strategii.

Obiective si rezultate

Obiectivele pe termen lung si scurt ale proiectului sunt:

- Sa imbunatateasca capacitatea de detectare si prevenire a amenintarilor cibernetice prin analiza avansata a informatiilor privind amenintarile persistente, testarea Cyberrange, raportarea managementului riscului de securitate cibernetica si monitorizarea vulnerabilitatii securitatii cibernetice.

Pentru a atinge acest obiectiv, proiectul urmareste sa imbunatateasca capacitatea de detectare si prevenire a amenintarilor cibernetice prin analiza avansata a informatiilor privind amenintarile persistente. Acest lucru presupune utilizarea unor instrumente avansate de analiza si monitorizare a amenintarilor cibernetice, care sa permita identificarea si evaluarea riscurilor de securitate cibernetica. Prin utilizarea acestor instrumente, Primaria Bistrita poate sa detecteze si sa previna amenintarile cibernetice inainte ca acestea sa aiba un impact asupra sistemelor si aplicatiilor IT.

De asemenea, proiectul urmareste sa consolideze securitatea cibernetica prin testarea Cyberrange, care este o metoda avansata de testare a securitatii cibernetice. Aceasta presupune crearea unui mediu de testare controlat, in care se pot testa si evalua scenarii de atac cibernetic si vulnerabilitati. In acest fel, se poate identifica si remedia punctele slabe ale sistemelor si aplicatiilor IT, astfel incat sa se poata preveni atacurile cibernetice si sa se protejeze datele si informatiile cu caracter personal ale cetatenilor.

Pe langa acestea, proiectul vizeaza si imbunatatirea capacitatii de raportare si management al riscului de securitate cibernetica. Aceasta inseamna dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica, astfel incat sa se poata raspunde rapid si eficient la incidentele de securitate cibernetica. De asemenea, se va realiza o monitorizare continua a vulnerabilitatilor si a riscurilor de securitate cibernetica, astfel incat sa se poata interveni rapid in cazul unor probleme.

- Sa consolideze capacitatea de raspuns la incidente cibernetice prin organizarea de training-uri in securitate cibernetica si prin evaluarea vulnerabilitatii din punct de vedere al resurselor umane, tehnologiei si politicii de securitate.

Prin organizarea de training-uri in securitate cibernetica, obiectivul este de a imbunatati competentele si capacitatea de raspuns a personalului implicat in gestionarea incidentelor de securitate cibernetica, inclusiv a echipei de securitate cibernetica, a specialistilor IT, a responsabililor de protectie a datelor si a altor angajati care lucreaza cu date sensibile. Training-urile vor acoperi subiecte precum detectarea si prevenirea amenintarilor cibernetice, evaluarea riscurilor de securitate cibernetica si tehnici de raspuns la incidente. Acest lucru va asigura ca Primaria Bistrita are personalul pregatit sa gestioneze incidentele de securitate cibernetica si sa protejeze datele cu caracter personal ale cetatenilor.

In plus, prin evaluarea vulnerabilitatii din punct de vedere al resurselor umane, tehnologiei si politicii de securitate, obiectivul este de a identifica eventualele vulnerabilitati din cadrul organizatiei si de a dezvolta solutii pentru a le remedia. Evaluarea va identifica eventualele lacune in politica de securitate a organizatiei, precum si posibilele probleme tehnice si de resurse umane care pot conduce la vulnerabilitati de securitate cibernetica. Pe baza acestor evaluari, se vor dezvolta planuri de actiune pentru a imbunatati procesele, politica si tehnologia utilizate de Primaria Bistrita.

- Sa creasca nivelul de securitate cibernetica prin evaluarea securitatii tehnice, investitii in tehnologie pentru monitorizarea dispozitivelor mobile si a sistemului si infrastructurii IT, precum si prin organizarea de training-uri in securitate cibernetica pentru angajatii Primariei Bistrita si cetatenii din comunitate.

Evaluarea securității tehnice va oferi o imagine de ansamblu asupra vulnerabilităților și problemelor de securitate existente în infrastructura IT a Primăriei Bistrița, ceea ce va permite implementarea unor soluții de securitate adecvate și îmbunătățirea securității în general.

Investițiile în tehnologie pentru monitorizarea dispozitivelor mobile și a sistemului și infrastructurii IT vor consolida și mai mult securitatea IT a Primăriei Bistrița. Aceste investiții vor permite identificarea și remedierea rapidă a eventualelor amenințări sau vulnerabilități, reducând astfel riscul de atacuri cibernetice și de pierdere a datelor sensibile.

Organizarea de training-uri în securitate cibernetică pentru angajații Primăriei Bistrița și cetățenii din comunitate este un alt obiectiv important. Aceste training-uri vor ajuta la creșterea gradului de conștientizare a angajaților cu privire la amenințările cibernetice și la dezvoltarea de competențe și cunoștințe necesare pentru a preveni și a gestiona astfel de amenințări. De asemenea, training-urile pentru cetățeni vor contribui la creșterea gradului de conștientizare și la educarea acestora cu privire la măsurile de securitate cibernetică.

Prin evaluarea vulnerabilității din punct de vedere al resurselor umane, tehnologiei și politicii de securitate, Primăria Bistrița va identifica și aborda problemele specifice de securitate cibernetică din aceste domenii, îmbunătățind astfel capacitatea de gestionare a amenințărilor cibernetice și creșterea nivelului de securitate cibernetică în general.

Rezultatele asteptate ale proiectului includ:

- infrastructura mai sigura si mai rezistenta la atacurile cibernetice

Acest lucru va fi realizat prin implementarea unor solutii de securitate pentru retele, dispozitive mobile si sisteme IT, inclusiv firewall-uri, sisteme de detectare a intrusilor si autentificare multi-factor, precum și prin monitorizarea constanta a dispozitivelor mobile și a sistemului și infrastructurii IT.

Metricile și valorile țintă asociate cu acest rezultat ar putea include următoarele:

  - Nivelul de securitate al rețelelor și a infrastructurii IT înainte și după implementarea soluțiilor de securitate, măsurat cu ajutorul unui sistem de monitorizare. Valoarea țintă ar putea fi de creștere a nivelului de securitate cu cel puțin 50% față de nivelul inițial.
  - Nivelul de conștientizare al angajaților privind amenințările cibernetice, măsurat prin intermediul unor sesiuni de instruire. Valoarea țintă ar putea fi de creștere a nivelului de conștientizare cu cel puțin 75% față de nivelul inițial.

- capacitate mai buna de detectare si prevenire a amenintarilor cibernetice

Acest lucru se va realiza prin implementarea de soluții de securitate cibernetică și prin organizarea de training-uri în domeniul securității cibernetice pentru angajații Primăriei Bistrița și cetățenii din comunitate.

Pentru a măsura succesul acestui rezultat, următoarele metrici și valori țintă pot fi utilizate:

  - Timpul de detectare a incidentelor de securitate cibernetică: timpul necesar pentru a detecta o amenințare cibernetică trebuie să fie redus la maximum 24 de ore.
  - Numărul de incidente de securitate cibernetică raportate: numărul de incidente de securitate cibernetică raportate ar trebui să scadă cu minimum 50% după implementarea soluțiilor de securitate cibernetică și organizarea de training-uri în securitatea cibernetică.
  - Nivelul de conștientizare a angajaților cu privire la amenințările cibernetice: nivelul de conștientizare a angajaților în privința amenințărilor cibernetice ar trebui să crească cu minimum 30% după organizarea de training-uri în securitatea cibernetică.

- Numărul de atacuri cibernetice evitate: numărul de atacuri cibernetice evitate ar trebui să crească cu minimum 50% după implementarea soluțiilor de securitate cibernetică și organizarea de training-uri în securitatea cibernetică.
- Nivelul de securitate cibernetică al infrastructurii IT: nivelul de securitate cibernetică al infrastructurii IT ar trebui să fie măsurat prin intermediul unui audit de securitate cibernetică și trebuie să respecte cele mai bune practici din domeniu.

- capacitate mai buna de raspuns la incidente cibernetice

Rezultatul "capacitate mai bună de răspuns la incidente cibernetice" se referă la îmbunătățirea capacitatății Primăriei Bistrița de a reacționa prompt și eficient în cazul unui incident cibernetic, precum o breșă de securitate sau un atac cibernetic. Aceasta va fi realizată prin organizarea de training-uri în securitate cibernetică pentru angajați, precum și prin evaluarea vulnerabilității din punct de vedere al resurselor umane, tehnologiei și politicii de securitate.

Pentru a măsura succesul acestui rezultat, vor fi adăugate următoarele metrici și valori țintă:

1. Timpul de răspuns la incidente cibernetice: Acesta se referă la intervalul de timp dintre momentul în care a fost identificat un incident cibernetic și momentul în care acesta este gestionat și rezolvat complet. Valoarea țintă este de maximum 24 de ore, pentru a asigura un răspuns prompt și eficient.
2. Gradul de conformitate cu protocoalele de gestionare a incidentelor: Acesta măsoară nivelul de respectare a procedurilor și protocoalelor de gestionare a incidentelor de securitate cibernetică. Valoarea țintă este de minimum 95%, pentru a asigura că toți angajații Primăriei Bistrița cunosc și respectă protocoalele de gestionare a incidentelor.
3. Gradul de îmbunătățire a capacității de răspuns la incidente: Acesta se referă la procentul de îmbunătățire a capacității de răspuns la incidente cibernetice, în comparație cu situația anterioară implementării proiectului. Valoarea țintă este de minimum 50%, pentru a asigura o îmbunătățire semnificativă a capacității de răspuns la incidente cibernetice.

- angajatii Primariei Bistrita si cetatenii din comunitatea locala vor fi mai bine informati si pregatiti pentru a face fata amenintarilor cibernetice

Rezultatul consta in imbunatatirea nivelului de constientizare a angajatilor Primariei Bistrita si cetatenilor din comunitatea locala cu privire la amenintarile cibernetice si modalitatile de prevenire a acestora. Acest lucru se va realiza prin organizarea de training-uri in securitate cibernetica, care vor acoperi o gama larga de subiecte, inclusiv principiile de securitate cibernetica, amenintarile cibernetice comune, masuri de prevenire si detectare a incidentelor cibernetice, gestionarea incidentelor cibernetice si proceduri de raportare a incidentelor.

Metricile si valorile tinta care vor fi monitorizate includ:

- Numarul de angajati ai Primariei Bistrita si cetateni din comunitatea locala care vor participa la training-urile organizate in cadrul proiectului. Valoarea tinta va fi de cel putin 80% din totalul angajatilor Primariei Bistrita si a cetatenilor din comunitatea locala.
- Gradul de satisfactie al participantilor la training-urile in securitate cibernetica, care va fi evaluat printr-un sondaj de feedback. Valoarea tinta va fi de cel putin 90% din participantii la training-uri care vor evalua training-urile ca fiind utile si informative.
- Cresterea gradului de constientizare a angajatilor si cetatenilor cu privire la amenintarile cibernetice, care va fi evaluata prin intermediul unui sondaj inainte si dupa participarea la training-uri. Valoarea tinta va fi o crestere cu cel putin 30% a cunostintelor si intelegerii participantilor cu privire la amenintarile cibernetice si masurile de prevenire a acestora.

- reducerea riscului de pierdere a datelor personale si informatiilor confidentiale ale cetatenilor

Primaria Bistrita va trebui reducă riscul de pierdere a datelor personale și a informațiilor confidentiale ale cetățenilor, ceea ce va contribui la creșterea încrederii cetățenilor în Primarie și la îmbunătățirea relației cu comunitatea. De asemenea, reducerea riscului de pierdere a datelor și a informațiilor poate avea un impact pozitiv asupra economiei locale prin protejarea afacerilor locale de posibilele pierderi financiare cauzate de furtul de identitate sau alte infracțiuni cibernetice.

Pentru a măsura succesul acestui rezultat, pot fi folosite următoarele metrici și valori țintă:

1. Numărul de incidente de securitate cibernetică raportate de cetățeni sau descoperite intern - Valoarea țintă: Reducerea numărului de incidente cu cel puțin 50% în următorii 2 ani.
2. Timpul mediu de detectare a incidentelor cibernetice - Valoarea țintă: Reducerea timpului de detectare cu cel puțin 30% în următorii 2 ani.
3. Numărul de date personale sau informații confidentiale pierdute sau compromise - Valoarea țintă: Reducerea numărului de incidente cu cel puțin 50% în următorii 2 ani.
4. Nivelul de satisfacție a cetățenilor cu privire la securitatea datelor lor personale și confidentiale - Valoarea țintă: Creșterea nivelului de satisfacție cu cel puțin 20% în următorii 2 ani, măsurat prin sondaje de opinie sau feedback-ul cetățenilor.

- cresterea increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale

Rezultatul trebuie sa fie o crestere semnificativa a increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale. Prin implementarea masurilor de securitate cibernetica, Primaria Bistrita va putea sa protejeze atat datele si infrastructura IT proprii, cat si datele cu caracter personal ale cetatenilor si sa ofere servicii publice digitale mai sigure si mai eficiente. Astfel, cetatenii vor avea mai multa incredere in Primaria Bistrita si in capacitatea acesteia de a proteja informatiile lor personale si confidentiale. De asemenea, prin organizarea de training-uri in securitate cibernetica pentru angajatii Primariei Bistrita si cetatenii din comunitate, acestia vor fi mai bine informati si pregatiti pentru a face fata amenintarilor cibernetice.

Pentru a măsura rezultatul de creștere a încrederii cetățenilor în capacitatea Primăriei Bistrița de a proteja informațiile lor personale și confidentiale, pot fi urmărite următoarele metrici și valori țintă:

- Numărul de plângeri privind încălcarea securității cibernetice înregistrate de Primăria Bistrița de la cetățeni, comparativ cu perioadele anterioare și cu media la nivel național. Valoarea țintă ar putea fi o reducere cu cel puțin 20% a numărului de plângeri înregistrate în ultimul an.
- Numărul de cetățeni care utilizează serviciile publice digitale oferite de Primăria Bistrița, comparativ cu perioadele anterioare și cu media la nivel național. Valoarea țintă ar putea fi o creștere cu cel puțin 10% a numărului de utilizatori înregistrat în ultimul an.
- Gradul de satisfacție a cetățenilor cu privire la nivelul de securitate cibernetică oferit de Primăria Bistrița. Acest lucru poate fi evaluat prin intermediul unor sondaje de opinie și feedback-ul primit de la cetățeni cu privire la nivelul de securitate și protecție a datelor personale și confidentiale. Valoarea țintă ar putea fi o creștere a gradului de satisfacție cu cel puțin 15% în ultimul an.
- Numărul de parteneriate sau acorduri de colaborare încheiate de Primăria Bistrița cu organizații sau companii specializate în securitate cibernetică, în scopul consolidării capacității de protecție și prevenire a amenințărilor cibernetice. Valoarea țintă ar putea fi încheierea a cel puțin două astfel de parteneriate în ultimul an.

- Numărul de evenimente de formare și sensibilizare în securitate cibernetică organizate de Primăria Bistrița pentru cetățeni și angajați, comparativ cu perioadele anterioare și cu media la nivel național. Valoarea țintă ar putea fi organizarea a cel puțin trei astfel de evenimente în ultimul an.

Alte metrici ale acestui rezultat ar putea fi:

- Numarul de cetateni care se simt mai increzatori in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale, masurat prin intermediul unui sondaj de opinie.
- Numarul de cereri de acces la date cu caracter personal, care indica nivelul de incredere al cetatenilor in capacitatea Primariei Bistrita de a proteja datele lor personale.
- Nivelul de satisfactie al cetatenilor in legatura cu serviciile publice digitale oferite de Primaria Bistrita, masurat prin intermediul unui sondaj de opinie.
- Numarul de incidente de securitate cibernetica raportate de catre cetateni, care indica nivelul de incredere al acestora in capacitatea Primariei Bistrita de a gestiona si solutiona astfel de probleme.

Planul de implementare

Implementarea proiectului de face pe o serie de pachete de lucru, dupa cum urmeaza:

WP1: Evaluare vulnerabilitate si decalaje in sistemul de securitate cibernetica

- Auditul de securitate cibernetica pentru toate aplicatiile si sistemele IT utilizate de Primaria Bistrita

Auditul de securitate cibernetică constă într-un proces sistematic de evaluare a măsurilor de securitate și a vulnerabilităților unui sistem sau aplicație IT, cu scopul de a identifica eventualele probleme și a recomanda soluții pentru îmbunătățirea securității. În cazul Primăriei Bistrița, auditul de securitate cibernetică va fi efectuat pentru toate aplicațiile și sistemele IT utilizate, pentru a identifica și evalua vulnerabilitățile acestora. Acest proces va implica utilizarea unor instrumente de securitate cibernetică precum scanere de vulnerabilități, sisteme de detectare a intruziunilor, teste de penetrare și alte tehnologii pentru a identifica și evalua nivelul de securitate al aplicațiilor și sistemelor IT utilizate. Evaluarea va fi urmată de recomandări pentru remedierea problemelor identificate și îmbunătățirea nivelului de securitate cibernetică al Primăriei Bistrița.

Planul de implementare pentru activitatea de audit de securitate cibernetică constă în următoarele etape:

1. Identificarea tuturor aplicațiilor și sistemelor IT utilizate de Primăria Bistrița: Pentru a se asigura că auditul este cuprinzător, este important să se identifice toate aplicațiile și sistemele IT utilizate de Primăria Bistrița. Acest lucru poate fi realizat prin intermediul unui chestionar completat de către departamentele respective, pentru a identifica toate aplicațiile și sistemele IT folosite.
2. Evaluarea riscurilor de securitate cibernetică: După identificarea aplicațiilor și sistemelor IT, următorul pas este evaluarea riscurilor de securitate cibernetică. Acest proces constă în analizarea fiecărui sistem și aplicație în parte, pentru a identifica eventualele vulnerabilități sau amenințări de securitate cibernetică. În acest proces sunt luate în considerare amenințările potențiale, probabilitatea lor de apariție și impactul lor potențial asupra organizației.
3. Realizarea auditului de securitate cibernetică: După evaluarea riscurilor de securitate cibernetică, urmează realizarea auditului de securitate cibernetică în sine. Acesta implică analiza sistematică și exhaustivă a tuturor aspectelor de securitate cibernetică ale aplicațiilor și sistemelor IT identificate. Auditul va evalua vulnerabilitățile și măsurile de securitate existente, precum și politica și procedurile de securitate cibernetică.
4. Identificarea măsurilor de îmbunătățire: În urma realizării auditului, se vor identifica eventualele probleme sau deficiențe în sistemul de securitate cibernetică. Aceste probleme pot fi de exemplu, vulnerabilități ale sistemului, politici de securitate cibernetică insuficiente sau o lipsă de formare și conștientizare a angajaților în ceea ce privește amenințările cibernetice. Se vor identifica măsurile de îmbunătățire necesare pentru a remedia aceste probleme.

- Evaluarea securitatii tehnice

Evaluarea securitatii tehnice este o activitate complexa ce consta in identificarea si evaluarea vulnerabilitatilor si riscurilor asociate infrastructurii IT a Primariei Bistrita. Aceasta activitate poate implica scanarea si testarea retelelor, sistemelor si aplicatiilor pentru a identifica potentiale probleme de securitate, cum ar fi porturi deschise, configurari incorecte sau vulnerabilitati cunoscute. De asemenea, evaluarea securitatii tehnice poate include si evaluarea si actualizarea politicilor de securitate existente, precum si implementarea unor noi politici si proceduri de securitate pentru a preveni si a gestiona incidentele de securitate cibernetica. Prin evaluarea si

imbunatatirea securitatii tehnice, Primaria Bistrita poate reduce riscurile de pierdere a datelor si de a fi afectata de atacurile cibernetice, asigurand protectia datelor cu caracter personal si confidential ale cetatenilor si a propriilor sale sisteme si aplicatii IT.

Planul de implementare pentru evaluarea securitatii tehnice va implica urmatorii pasi:

1. Identificarea si selectarea specialistilor in securitate cibernetica - Pentru a asigura o evaluare obiectiva si precisa a securitatii tehnice, este necesara identificarea si selectarea unor specialisti in securitate cibernetica cu experienta relevanta si cunostinte solide in domeniul evaluarii securitatii tehnice.
2. Identificarea si evaluarea resurselor IT - Specialistii in securitate cibernetica vor identifica si evalua resursele IT ale Primariei Bistrita, inclusiv retelele, sistemele si aplicatiile utilizate, precum si dispozitivele mobile si alte echipamente IT. Acest pas va ajuta la identificarea vulnerabilitatilor si la evaluarea nivelului de securitate existent.
3. Identificarea si evaluarea riscurilor de securitate cibernetica - Specialistii in securitate cibernetica vor identifica si evalua riscurile de securitate cibernetica asociate cu resursele IT ale Primariei Bistrita. Acest pas va ajuta la identificarea potentialelor amenintari si vulnerabilitati si la evaluarea nivelului de risc existent.
4. Analiza si evaluarea masurilor de securitate existente - Specialistii in securitate cibernetica vor analiza si evalua masurile de securitate existente ale Primariei Bistrita, inclusiv politici, proceduri, tehnologii si alte masuri de securitate implementate. Acest pas va ajuta la identificarea lacunelor de securitate si la evaluarea eficacitatii masurilor de securitate existente.
5. Dezvoltarea de recomandari si planuri de imbunatatire a securitatii tehnice - Pe baza evaluarii resurselor IT, a identificarii riscurilor de securitate cibernetica si a analizei masurilor de securitate existente, specialistii in securitate cibernetica vor dezvolta recomandari si planuri pentru imbunatatirea securitatii tehnice a Primariei Bistrita. Acest pas va include identificarea prioritatilor, stabilirea de obiective clare si definirea unui plan de actiune detaliat.

- Evaluarea vulnerabilității din punct de vedere al resurselor umane

Evaluarea vulnerabilității din punct de vedere al resurselor umane constă în identificarea și analizarea posibilelor vulnerabilități ale organizației cauzate de comportamentul angajaților sau de lipsa de cunoștințe în materie de securitate cibernetică. Această evaluare implică o serie de activități, cum ar fi analiza politicilor și procedurilor de securitate, interviuri cu angajații, identificarea practicilor bune și a practicilor care trebuie îmbunătățite, precum și analiza datelor de securitate cibernetică relevante, cum ar fi atacurile prin phishing sau alte tipuri de atacuri cu ajutorul angajatilor. În urma evaluării vulnerabilităților din punct de vedere al resurselor umane, se pot dezvolta planuri de formare și conștientizare a angajaților cu privire la amenințările cibernetice și măsurile de prevenire a acestora, precum și dezvoltarea de politici și proceduri mai clare pentru a preveni astfel de amenințări. Acest lucru poate contribui semnificativ la creșterea nivelului de securitate cibernetică a organizației și la protejarea datelor și a infrastructurii IT de potențialele amenințări cibernetice.

Planul de implementare pentru evaluarea vulnerabilității din punct de vedere al resurselor umane include următoarele etape:

1. Identificarea tuturor angajaților care au acces la sistemele și datele critice ale Primăriei Bistrița și care ar putea fi considerați ca potențiali factori de risc pentru securitatea cibernetică.
2. Evaluarea nivelului de conștientizare și cunoaștere a acestor angajați în ceea ce privește practicile bune de securitate cibernetică, prin intermediul unor interviuri și/sau chestionare.

3. Analiza datelor colectate și identificarea punctelor slabe în cunoașterea și aplicarea politicilor și procedurilor de securitate cibernetică, inclusiv prin compararea rezultatelor cu standardele de securitate cibernetică relevante.
4. Propunerea de soluții pentru a îmbunătăți nivelul de conștientizare și cunoaștere a angajaților în ceea ce privește securitatea cibernetică, inclusiv prin organizarea de training-uri, sesiuni de sensibilizare și/sau materiale educaționale.

- Evaluarea vulnerabilității din punct de vedere al tehnologiei

Evaluarea vulnerabilității din punct de vedere al tehnologiei este un proces complex de analiză și evaluare a sistemelor și infrastructurii IT pentru a identifica vulnerabilitățile și deficiențele de securitate cibernetică. Aceasta implică utilizarea unor instrumente specializate de scanare a rețelei și a sistemelor, identificarea punctelor slabe în ceea ce privește configurarea, patch-urile de securitate, și verificarea securității aplicațiilor. De asemenea, evaluarea tehnică a vulnerabilității poate include și testarea de penetrare, în care specialiștii în securitate informatică încearcă să pătrundă în sistem pentru a identifica și exploata vulnerabilitățile. Rezultatele evaluării tehnice a vulnerabilității pot fi utilizate pentru a identifica și remediate problemele de securitate, în scopul protejării infrastructurii IT și a datelor sensibile de atacurile cibernetice.

Planul de implementare pentru evaluarea vulnerabilității din punct de vedere al tehnologiei va fi următorul:

1. Identificarea tuturor tehnologiilor utilizate de Primăria Bistrița în procesul de gestionare a datelor și informațiilor cetățenilor.
2. Identificarea punctelor vulnerabile și a riscurilor de securitate în ceea ce privește tehnologiile utilizate.
3. Crearea unui plan de acțiune pentru îmbunătățirea securității tehnologice, care să includă soluții specifice pentru fiecare punct vulnerabil identificat.

- Evaluarea vulnerabilității din punct de vedere al politicii de securitate

Evaluarea vulnerabilității din punct de vedere al politicii de securitate reprezintă un proces de analiză și evaluare a politicilor, procedurilor și regulilor existente în ceea ce privește securitatea informației și a datelor în cadrul organizației. Această evaluare implică o analiză detaliată a politicilor de securitate și a proceselor existente, cu scopul de a identifica punctele slabe și vulnerabilitățile sistemului. Evaluarea politicii de securitate include, de asemenea, revizuirea politicilor de securitate existente și a planurilor de continuitate a afacerii pentru a asigura o securitate corespunzătoare în caz de incidente de securitate cibernetică. Această evaluare are ca scop îmbunătățirea securității sistemelor și a datelor organizației prin identificarea și remedierea vulnerabilităților în politica de securitate și planurile de continuitate a afacerii. În cadrul acestei evaluări, se pot utiliza diferite metode, precum chestionare, interviuri cu personalul, analiza documentelor și revizuirea sistemelor existente.

Planul de implementare pentru activitatea "Evaluarea vulnerabilității din punct de vedere al politicii de securitate" constă în următorii pași:

1. Identificarea politicilor și procedurilor de securitate cibernetică existente: Echipa de evaluare va analiza documentele existente referitoare la politici și proceduri de securitate cibernetică pentru a determina care sunt cele deja existente și care ar putea fi îmbunătățite.
2. Definirea obiectivelor și scopurilor: Echipa de evaluare va defini obiectivele și scopurile pentru evaluarea vulnerabilității din punct de vedere al politicii de securitate cibernetică. Aceste obiective ar putea include îmbunătățirea politicilor și procedurilor de securitate cibernetică, creșterea gradului de conștientizare a personalului cu privire la riscurile de securitate cibernetică, creșterea securității rețelelor și a sistemelor de informații etc.

3. Identificarea vulnerabilităților: Echipa de evaluare va identifica vulnerabilitățile în politicile și procedurile de securitate cibernetică. Acestea ar putea include probleme de securitate la nivel de autentificare, autorizare, criptare, gestionare a parolelor, gestionare a patch-urilor etc.
4. Evaluarea nivelului de conformitate: Echipa de evaluare va evalua nivelul de conformitate al politicilor și procedurilor de securitate cibernetică cu standardele și reglementările relevante, cum ar fi GDPR, NIST, ISO etc.
5. Identificarea soluțiilor și planificarea remedierii: Echipa de evaluare va identifica soluțiile pentru remedierea vulnerabilităților identificate și va planifica implementarea acestora. Acestea ar putea include revizuirea și actualizarea politicilor și procedurilor, îmbunătățirea sistemelor de autentificare și autorizare, implementarea unui sistem de gestionare a parolelor, implementarea unui sistem de gestionare a patch-urilor etc.

- Testarea exhaustiva pe GDPR si securitate cibernetica a angajatilor si sensibilizarea angajatilor Primariei Bistrita privind amenintarile cibernetice si metodele de prevenire a acestora

Testarea exhaustiva pe GDPR si securitate cibernetica a angajatilor se refera la evaluarea nivelului de constientizare si pregatire a angajatilor cu privire la GDPR si securitatea cibernetica, prin testarea si evaluarea cunostintelor lor teoretice si practice in acest domeniu. Aceasta poate include, de exemplu, teste de securitate cibernetica, simularea de atacuri cibernetice, exercitii de securitate a datelor si exercitii de raspuns la incidente cibernetice. Scopul acestei activitati este de a identifica si remedia lacunele de securitate cibernetica din organizatie si de a asigura ca angajatii sunt constienti de riscurile cibernetice si de masurile de precautie necesare pentru a le preveni. Sensibilizarea angajatilor cu privire la amenintarile cibernetice si metodele de prevenire a acestora poate include, de asemenea, formare si instruire in securitatea cibernetica, seminarii si prezentari si materiale de informare.

Planul de implementare pentru testarea exhaustivă a angajaților pe GDPR și securitatea cibernetică și sensibilizarea acestora cu privire la amenințările cibernetice și metodele de prevenire a acestora ar putea include următoarele activități:

1. Definirea obiectivelor și a scopului testării exhaustive a angajaților și a campaniei de sensibilizare. Obiectivele ar trebui să includă evaluarea nivelului de conștientizare a angajaților cu privire la GDPR și securitatea cibernetică și identificarea lacunelor și punctelor slabe în cunoștințele lor. Scopul ar trebui să fie creșterea nivelului de conștientizare a angajaților și îmbunătățirea securității cibernetice a Primăriei Bistrița.
2. Identificarea categoriilor de angajați care ar trebui să fie testați, cum ar fi angajații cu acces la datele personale ale cetățenilor, departamentele cu cele mai mari riscuri de securitate cibernetică și angajații din departamentele cheie.
3. Selecționarea unei platforme de testare adecvate pentru evaluarea angajaților în funcție de nivelul lor de cunoștințe despre GDPR și securitatea cibernetică, cum ar fi simulările de atacuri sau phishing.
4. Realizarea testului exhaustiv pentru angajați, care ar trebui să includă diverse scenarii de atac și probleme de securitate, precum phishing, ransomware sau exploatarea vulnerabilităților de securitate.
5. Analiza și evaluarea rezultatelor testului exhaustiv pentru a identifica lacunele și punctele slabe din cunoștințele și comportamentul angajaților legate de GDPR și securitatea cibernetică.
6. Dezvoltarea unui plan de acțiune pentru remedierea lacunelor identificate în cadrul testului exhaustiv și pentru a crește nivelul de conștientizare a angajaților cu privire la GDPR și securitatea cibernetică.
7. Realizarea unei campanii de sensibilizare pentru angajați cu privire la amenințările cibernetice și metodele de prevenire a acestora, inclusiv sesiuni de instruire, seminarii și comunicare constantă prin intermediul canalelor interne de comunicare.

8. Realizarea unui test de evaluare repetat la un interval regulat pentru a verifica îmbunătățirile în nivelul de conștienizare și pentru a identifica eventualele lacune și puncte slabe restante.

WP2: Analiza practicilor de securitate cibernetica

- Analiza avansata a informatiilor privind amenintarile persistente

Analiza avansată a informațiilor privind amenințările persistente este o activitate de securitate cibernetică care constă în colectarea și analiza continuă a datelor din diverse surse pentru a identifica amenințările cibernetice care sunt în desfășurare sau care pot fi iminente. Aceasta include analiza datelor de trafic de rețea, loguri de sistem, evenimente de securitate și alte surse relevante. Scopul acestei activități este de a identifica modele și comportamente suspecte care ar putea indica o posibilă amenințare cibernetică, pentru a putea lua măsuri preventive sau reactiva rapid în cazul unui incident. Analiza avansată a informatiilor privind amenintarile persistente implică utilizarea de tehnologii precum inteligența artificială, machine learning și analiza comportamentului pentru a identifica amenințările cibernetice avansate și pentru a asigura o protecție eficientă împotriva acestora.

Planul de implementare pentru activitatea de analiza avansata a informatiilor privind amenintarile persistente ar putea include urmatoarele etape:

1. Identificarea si colectarea datelor relevante pentru analiza amenintarilor cibernetice, inclusiv date despre sistemele IT, retele si aplicatii utilizate de Primaria Bistrita si furnizorii sai.
2. Evaluarea si clasificarea datelor colectate in functie de nivelul de risc si importanta pentru infrastructura IT si operatiunile Primariei Bistrita.
3. Utilizarea unor instrumente avansate de analiza a datelor pentru identificarea tiparelor si a semnelor de amenintari cibernetice, precum si pentru detectarea si raportarea incidentelor de securitate.
4. Implementarea unor masuri de securitate proactiva pentru a preveni, detecta si raspunde la amenintarile cibernetice identificate, inclusiv prin actualizarea sistemelor de securitate, aplicarea de patch-uri de securitate si instruirea angajatilor cu privire la bunele practici de securitate.

- Testarea Cyberrange

Testarea Cyberrange se referă la o metodă de testare a capacității de apărare împotriva atacurilor cibernetice și de evaluare a capacității de răspuns la aceste atacuri. Aceasta implică crearea unui mediu simulat de rețea pentru a imita condițiile reale de atac și pentru a permite experților în securitate cibernetică să testeze și să evalueze reacția și eficacitatea sistemelor de securitate ale unei organizații. Testarea Cyberrange poate implica simularea diferitelor scenarii de atac, inclusiv atacuri asupra infrastructurii IT și a rețelelor, phishing și alte metode de atac cibernetic, permițând astfel specialiștilor în securitate cibernetică să identifice punctele slabe ale sistemelor de securitate și să le remedieze înainte ca acestea să fie exploatate de atacatori.

Planul de implementare pentru activitatea de testare a Cyberrange constă în următoarele etape:

1. Identificarea obiectivelor de testare - identificarea sistemelor, rețelelor și infrastructurilor IT care vor fi supuse testării în mediul Cyberrange.
2. Proiectarea scenariilor de testare - definirea scenariilor de testare și a diferitelor situații în care acestea vor fi aplicate, precum și a obiectivelor specifice pentru fiecare scenariu.
3. Implementarea mediului de testare - configurarea mediului Cyberrange și a sistemelor de testare în conformitate cu scenariile de testare.

4. Testarea propriu-zisă - efectuarea testelor utilizând scenariile de testare și evaluarea rezultatelor.
5. Raportarea rezultatelor - documentarea rezultatelor testelor și prezentarea acestora echipei de management pentru a putea fi luate decizii referitoare la îmbunătățirea securității cibernetice.

- Raportarea managementului riscului de securitate cibernetica

Raportarea managementului riscului de securitate cibernetica reprezinta un proces important de evaluare si monitorizare a riscurilor de securitate cibernetica la nivelul Primariei Bistrita. Aceasta activitate implica identificarea, evaluarea si gestionarea riscurilor asociate cu datele si infrastructura IT a Primariei, cu scopul de a minimiza impactul negativ al incidentelor cibernetice. Pentru a realiza aceasta activitate, se va realiza o analiza detaliata a riscurilor de securitate cibernetica, se vor identifica vulnerabilitatile, se vor stabili prioritatile de actiune si se vor dezvolta planuri de mitigare a riscurilor. De asemenea, se va implementa un sistem de raportare periodica a riscurilor de securitate cibernetica, astfel incat managementul sa poata lua decizii mai informate si sa poata adopta masuri de prevenire a incidentelor cibernetice.

Planul de implementare pentru activitatea de Raportarea managementului riscului de securitate cibernetica ar putea include urmatoarele etape:

1. Identificarea riscurilor: In aceasta etapa, se va efectua o analiza a riscurilor asociate cu activitatile desfasurate de Primaria Bistrita, inclusiv riscurile de securitate cibernetica. Acest lucru poate fi realizat prin examinarea sistemelor, aplicatiilor si infrastructurii IT utilizate de catre Primaria Bistrita.
2. Evaluarea riscurilor: In aceasta etapa, se va efectua o evaluare a riscurilor identificate in etapa anterioara, pentru a stabili impactul si probabilitatea fiecarui risc. Aceasta etapa va ajuta la determinarea prioritatii de actiune pentru fiecare risc.
3. Identificarea si evaluarea controalelor existente: In aceasta etapa, se vor identifica controalele de securitate cibernetica deja existente si se va evalua eficacitatea lor in prevenirea si detectarea riscurilor identificate.
4. Identificarea si evaluarea controalelor suplimentare: In aceasta etapa, se vor identifica si evalua controalele de securitate cibernetica suplimentare care ar putea fi implementate pentru a reduce riscurile identificate.
5. Elaborarea unui plan de gestionare a riscurilor: In aceasta etapa, se va elabora un plan de gestionare a riscurilor, care va include o lista de actiuni recomandate si prioritizate pentru imbunatatirea securitatii cibernetice.

- Monitorizarea vulnerabilitatii securitatii cibernetice

Monitorizarea vulnerabilității securității cibernetice se referă la procesul de urmărire și identificare a potențialelor amenințări cibernetice care ar putea afecta securitatea și integritatea datelor și sistemelor de la Primaria Bistrita. Această activitate poate implica utilizarea de instrumente automate de monitorizare a rețelelor, scanarea periodică a sistemelor și a aplicațiilor pentru a detecta vulnerabilități și probleme de securitate, precum și analiza activității și evenimentelor de securitate în timp real pentru a identifica eventualele atacuri sau incercari de intruziune. Monitorizarea vulnerabilității securității cibernetice poate ajuta la identificarea rapidă a problemelor de securitate și la implementarea măsurilor de remediere pentru a reduce riscul de atacuri cibernetice. De asemenea, poate ajuta la îmbunătățirea capacității Primariei Bistrita de a răspunde rapid și eficient la incidentele de securitate cibernetică, precum și la îmbunătățirea planurilor de continuitate a afacerii și a planurilor de recuperare a dezastrelor.

Planul de implementare pentru activitatea de monitorizare a vulnerabilitatii securitatii cibernetice include urmatoarele etape:

1. Identificarea sistemelor si aplicatiilor critice care necesita monitorizare.
2. Selectarea unei solutii de monitorizare adecvate pentru acestea, inclusiv firewall-uri, sisteme de detectare a intrusilor si sisteme de autentificare multi-factor.
3. Implementarea solutiei si configurarea acesteia pentru a monitoriza activitatea in timp real si pentru a detecta orice incidente de securitate cibernetica.
4. Setarea unor alerte automatizate pentru incidentele critice, precum si asignarea unui responsabil pentru a gestiona fiecare incident.
5. Actualizarea constanta a solutiei de monitorizare si a alertelor, pentru a asigura ca acestea raman eficiente impotriva noilor amenintari cibernetice.
6. Efectuarea de rapoarte periodice si analize ale datelor de monitorizare pentru a identifica tendinte si modele de activitate suspecta, si pentru a lua masuri de imbunatatire a securitatii cibernetice.

- Inteligenta cibernetica a amprentei digitale

Inteligenta cibernetica a amprentei digitale se refera la procesul de colectare, analizare si interpretare a datelor legate de activitatea online a unui utilizator sau a unei organizatii. Aceasta analiza permite identificarea modelelor si comportamentelor neobisnuite, care ar putea indica o posibila incalcare a securitatii cibernetice sau a regulilor de confidentialitate. Inteligenta cibernetica a amprentei digitale utilizeaza algoritmi avansati de analiza a datelor, precum si tehnologii de inteligenta artificiala si de invatare automata. Aceasta abordare poate ajuta la identificarea rapidă a vulnerabilitatilor de securitate cibernetica si la identificarea amenintarilor si riscurilor de securitate mai devreme decat ar fi posibil prin alte metode. In ceea ce priveste implementarea acestui proces, poate implica utilizarea de tehnologii de securitate cibernetica avansate, cum ar fi solutii de monitorizare a retelelor, de detectare a intrusilor si de analiza a log-urilor. De asemenea, poate fi necesar ca organizația să instituie proceduri și politici stricte de securitate cibernetica, pentru a minimiza riscurile de incalcare a securitatii si confidentialitatii datelor.

Planul de implementare pentru activitatea de Inteligenta cibernetica a amprentei digitale ar putea include urmatoarele etape:

1. Identificarea datelor relevante: Prima etapă ar fi identificarea datelor relevante care trebuie colectate pentru a genera o amprentă digitală a dispozitivelor și rețelelor utilizate de Primaria Bistrita. Aceasta poate include informații despre sistemul de operare, aplicațiile instalate, setările de securitate, adrese IP și multe altele.
2. Colectarea și analiza datelor: După identificarea datelor relevante, acestea trebuie colectate și analizate pentru a genera o imagine completă a amprentei digitale a dispozitivelor și rețelelor. Acest lucru poate fi realizat cu ajutorul instrumentelor specializate de colectare și analiză a datelor, cum ar fi soluțiile de monitorizare și analiză a securității.
3. Crearea unei amprente digitale: Utilizând datele colectate și analizate, se poate crea o amprentă digitală a dispozitivelor și rețelelor utilizate de Primaria Bistrita. Aceasta poate fi o imagine completă a securității cibernetice și poate fi utilizată pentru a identifica orice amenințări potențiale sau vulnerabilități.
4. Monitorizarea și actualizarea: Pentru a menține o amprentă digitală actualizată și precisă, trebuie să se monitorizeze continuu dispozitivele și rețelele utilizate de Primaria Bistrita. Orice schimbări sau actualizări trebuie adăugate la amprenta digitală existentă.
5. Implementarea măsurilor de securitate: În funcție de informațiile identificate prin amprenta digitală, se pot implementa măsuri suplimentare de securitate pentru a proteja dispozitivele și rețelele împotriva amenințărilor cibernetice.

- Raspuns la incident

Raspunsul la incident reprezinta un proces de gestionare a situatiilor de securitate cibernetica care pot aparea. Scopul acestui proces este de a reduce la minimum impactul incidentelor de securitate asupra infrastructurii si a datelor. Procesul de raspuns la incident implica identificarea incidentului, evaluarea impactului si a riscului, stabilirea si implementarea unui plan de remediere, precum si monitorizarea si raportarea incidentului. Este important ca acest proces sa fie implementat intr-un mod coordonat si rapid, pentru a reduce timpul de inactivitate si a minimiza impactul asupra datelor si infrastructurii. Planul de raspuns la incident ar trebui sa fie testat si actualizat periodic pentru a se asigura ca acesta este eficient si adaptat la amenintarile actuale de securitate cibernetica.

Planul de implementare pentru activitatea de Raspuns la incident poate include urmatoarele etape:

1. Definirea procedurilor de raspuns la incident: Aceasta etapa include identificarea tipurilor de incidente si dezvoltarea unor proceduri clare pentru a raspunde la acestea. Procedurile pot include notificarea echipelor relevante, stabilirea unui plan de actiune si gestionarea incidentului in sine.
2. Identificarea si implementarea unor unelte si solutii de monitorizare si detectare: Aceasta etapa presupune selectarea unor unelte si solutii de monitorizare a retelelor si a sistemelor pentru detectarea incidentelor. Aceste solutii pot include firewall-uri, sisteme de detectare a intrusilor, sisteme de monitorizare a traficului de retea, etc.
3. Dezvoltarea unui plan de backup si de recuperare a datelor: Aceasta etapa implica definirea unui plan de backup si de recuperare a datelor pentru a minimiza pierderea de date in cazul unui incident.
4. Testarea planurilor de raspuns la incidente: Aceasta etapa implica testarea periodica a planurilor de raspuns la incidente pentru a asigura functionarea corecta a acestora.
5. Formarea si antrenarea angajatilor: Aceasta etapa include formarea si antrenarea angajatilor pentru a recunoaste si a gestiona incidentele de securitate cibernetica.

- Aviz Pentest

Avizul Pentest este o activitate prin care se realizeaza o evaluare a securitatii informatice a unei aplicatii sau a unei infrastructuri IT, prin testarea activa a acestora. Scopul acestei activitati este de a identifica vulnerabilitatile si potentialele amenintari din sistem, astfel incat sa poata fi luate masuri de remediere. Pentestul poate fi realizat in doua moduri: White-box, cand sunt oferite detalii complete despre infrastructura si codul sursa, si Black-box, cand se testeaza aplicatia sau sistemul fara a avea acces la detalii complete despre infrastructura. In urma Pentestului se elaboreaza un raport de evaluare a securitatii, care include si recomandari de remediere a problemelor identificate. Aceasta activitate este utila pentru a preveni atacurile cibernetice si pentru a imbunatati securitatea informatiei, inclusiv a datelor cu caracter personal.

Planul de implementare pentru activitatea "Aviz Pentest" consta in urmatoarele etape:

1. Selectarea unei companii specializate in testarea de penetrare (pentesting) pentru a efectua avizul. Alegerea companiei trebuie sa fie bazata pe experienta anterioara, reputatie si calitatea serviciilor oferite.
2. Definirea obiectivelor si a perimetrelor care vor fi testate. Se va stabili tipul de teste de penetrare care se va efectua (black-box, white-box, grey-box), precum si sistemele, aplicatiile sau retelele care vor fi evaluate.
3. Stabilirea unui acord de confidentialitate si semnarea contractului cu compania selectata. Acestea vor specifica obligatiile fiecarei parti, termenii si conditiile testului, precum si drepturile de proprietate intelectuala.

4. Efectuarea testului de penetrare de catre compania selectata, conform obiectivelor si perimetrelor definite anterior.
5. Analiza rezultatelor testului si identificarea punctelor vulnerabile. Se vor evalua si prioritiza problemele identificate in functie de impactul potential si de dificultatea remedierii acestora.
6. Prezentarea raportului de aviz Pentest. Acesta va include informatii detaliate despre vulnerabilitatile identificate, gradul de risc si recomandarile de remediere.
7. Implementarea masurilor de remediere pentru problemele identificate in cadrul testului de penetrare.
8. Reevaluarea sistemelor, aplicatiilor sau retelelor dupa remedierea problemelor identificate.

WP3: Formare profesionala in securitate cibernetica

- Formare profesionala - Apărător Cyber Security

Formarea profesională Apărător Cyber Security este o activitate de instruire a angajaților Primăriei Bistrița în vederea dezvoltării competențelor în domeniul securității cibernetice. Acest program de formare are ca scop creșterea nivelului de conștientizare și înțelegere a amenințărilor cibernetice, precum și dezvoltarea de competențe în identificarea, prevenirea și gestionarea acestor amenințări. În cadrul acestei activități, participanții vor fi familiarizați cu concepte de bază precum vulnerabilități, atacuri cibernetice, autentificare și criptare, precum și cu diferite tehnici și instrumente pentru protejarea datelor și a sistemelor informatice. De asemenea, vor fi prezentate studii de caz și scenarii practice pentru a ajuta la consolidarea competențelor și dezvoltarea abilităților necesare în domeniul securității cibernetice. Programul de formare poate fi personalizat pentru a se potrivi cu nevoile specifice ale Primăriei Bistrița și poate fi livrat într-o varietate de formate, inclusiv training-uri în clasă, sesiuni de e-learning și workshop-uri practice.

Planul de implementare pentru activitatea de formare profesionala "Apărător Cyber Security" include urmatoarele etape:

1. Identificarea nevoilor de formare a angajatilor Primariei Bistrita in ceea ce priveste cunoasterea si aplicarea principiilor si metodelor de securitate cibernetica.
2. Selectarea furnizorului de formare profesionala specializat in domeniul securitatii cibernetice, care va livra cursurile si materialele de instruire.
3. Dezvoltarea unui plan de instruire personalizat, adaptat nevoilor si nivelurilor de cunostinte ale angajatilor din diverse departamente ale Primariei Bistrita.
4. Livrarea cursurilor de formare profesionala, care vor include prezentari teoretice si studii de caz, precum si exercitii practice si teste de evaluare a cunostintelor dobandite.
5. Monitorizarea participarii si a progresului angajatilor in procesul de formare profesionala, pentru a asigura o completare eficienta a cursului si o imbunatatire a abilitatilor de securitate cibernetica.
6. Evaluarea rezultatelor formarii si a impactului acesteia asupra performantelor si eficientei angajatilor si a organizatiei in ansamblu.
7. Identificarea si implementarea de masuri suplimentare, daca este necesar, pentru a imbunatati nivelul de securitate cibernetica in organizatie.

- Formare profesionala - Clădiri inteligente și securitatea clădirilor

Formarea profesională în clădiri inteligente și securitatea clădirilor se referă la instruirea specialiștilor din domeniul construcțiilor și tehnologiei informației despre tehnologiile și metodologiile utilizate pentru a asigura securitatea clădirilor inteligente. Acest lucru implică o varietate de competențe, cum ar fi configurarea și monitorizarea sistemelor de securitate fizică și electronică, gestionarea accesului și a sistemelor de control al intrării și ieșirii, evaluarea vulnerabilităților și a riscurilor, și dezvoltarea de politici și proceduri pentru a preveni incidentele de securitate cibernetică. Formarea profesională ar trebui să acopere și aspecte cum ar fi

securitatea rețelelor de comunicații, siguranța datelor și a datelor personale, și riscurile asociate cu utilizarea dispozitivelor mobile și a internetului de lucru. Scopul final este de a asigura protecția clădirilor inteligente împotriva amenințărilor cibernetice și fizice și de a minimiza riscurile pentru proprietari, angajați și utilizatori.

Planul de implementare pentru activitatea "Formare profesionala - Clădiri inteligente și securitatea clădirilor" constă în următoarele etape:

1. Identificarea furnizorilor de formare specializați în securitatea clădirilor inteligente și selectarea celui mai potrivit în funcție de nevoile Primăriei Bistrița.
2. Stabilirea obiectivelor de învățare și a conținutului cursului, care trebuie să includă informații despre securitatea clădirilor inteligente, tehnologii de securitate și amenințările cibernetice specifice acestui domeniu.
3. Planificarea sesiunilor de formare, care trebuie să fie adaptate la nevoile specifice ale diferitelor departamente din cadrul Primăriei Bistrița și să fie programate astfel încât să nu afecteze prea mult activitatea de zi cu zi a instituției.
4. Identificarea resurselor necesare pentru susținerea programului de formare, inclusiv resurse financiare, echipamente și spații de învățare.
5. Realizarea programului de formare, asigurarea unei participări active a angajaților și evaluarea nivelului de înțelegere și aplicare a conținutului cursului.
6. Îmbunătățirea continuă a programului de formare pe baza feedback-ului angajaților și a schimbărilor în tehnologiile și amenințările de securitate în domeniul clădirilor inteligente.

- Formare profesionala - Securitate cibernetică pentru toată lumea

Formarea profesională în securitate cibernetică pentru toată lumea se referă la programele de instruire care au ca scop să ofere angajatilor din Primarie si cetățenilor o înțelegere mai profundă a securității cibernetice și a modului în care aceasta poate fi protejată. Aceste programe pot fi oferite atât în mod online, cât și în mod tradițional, și acoperă subiecte precum protecția datelor, prevenirea phishing-ului și altor amenințări cibernetice, cum să-ți protejezi dispozitivele mobile, cum să-ți creezi parole puternice și multe altele. Astfel de programe de formare pot ajuta cetățenii să devină mai conștienți de amenințările cibernetice și să ia măsuri adecvate pentru a-și proteja informațiile personale și confidentiale.

Planul de implementare pentru activitatea "Formare profesionala - Securitate cibernetică pentru toată lumea" include urmatoarele etape:

1. Identificarea necesitatilor de formare - se va realiza o analiza a angajatilor Primariei Bistrita pentru a identifica nivelul actual de cunoastere a conceptelor si practicilor de securitate cibernetica.
2. Identificarea furnizorilor de formare specializați în securitatea cibernetica și selectarea celui mai potrivit în funcție de nevoile Primăriei Bistrița.
3. Dezvoltarea de programe de formare - se vor dezvolta programe de formare personalizate pentru diferite categorii de angajati, care sa includa aspecte precum prevenirea phishing-ului, pastrarea parolelor sigure, gestionarea datelor personale si confidentialitatea informatiilor.
4. Implementarea programelor de formare - programul de formare va fi implementat prin intermediul sesiunilor de formare, webinarelor sau cursurilor online.
5. Evaluarea eficientei programului de formare - se vor efectua evaluari periodice ale programului de formare pentru a asigura ca obiectivele de invatare sunt atinse si ca angajatii sunt capabili sa aplice cunostintele dobandite in practica.
6. Actualizarea continua a programului de formare - programul de formare va fi actualizat in mod regulat pentru a reflecta noile amenintari de securitate cibernetica si pentru a oferi angajatilor cele mai recente cunostinte si competente.

- Formare profesionala - Specializare in securitate cibernetica pentru sectorul public

Specializarea în securitatea cibernetică pentru sectorul public se concentrează pe dezvoltarea abilităților și competențelor necesare pentru a proteja infrastructurile și datele sensibile ale organizațiilor din sectorul public împotriva amenințărilor cibernetice. Această formare profesională include concepte teoretice și practice referitoare la securitatea cibernetică, inclusiv metode de identificare și analiză a vulnerabilităților, tehnici de protecție și prevenire a atacurilor cibernetice, dezvoltarea politicilor de securitate cibernetică și procedurilor de gestionare a incidentelor de securitate. În plus, specializarea oferă o pregătire specială pentru cei implicați în domeniul securității cibernetice din sectorul public, cum ar fi administratorii de rețea, analiștii de securitate și managerii de securitate.

Planul de implementare pentru activitatea de formare profesională în specializarea securității cibernetice pentru sectorul public va cuprinde următoarele etape:

1. Identificarea nevoilor de formare: se va realiza o analiză a cerințelor și nevoilor de formare în domeniul securității cibernetice pentru sectorul public.
2. Proiectarea programului de formare: pe baza nevoilor identificate, se va elabora un program de formare care va include materiale didactice relevante, exerciții practice și evaluări periodice.
3. Selecția și pregătirea formatorilor: se vor selecta formatori specializați în domeniul securității cibernetice, cu experiență în sectorul public, care vor fi pregătiți pentru a preda conținutul programului.
4. Implementarea programului de formare: programul de formare va fi implementat printr-o combinație de prezentări, cursuri în clasă, ateliere practice și simulări de scenarii de securitate cibernetică.
5. Evaluarea și îmbunătățirea programului: se va efectua o evaluare a programului de formare, inclusiv a satisfacției participanților și a efectului acestuia asupra îmbunătățirii securității cibernetice în sectorul public. Pe baza rezultatelor, se vor face îmbunătățiri și ajustări la programul de formare.
6. Diseminarea rezultatelor și experiențelor: rezultatele și experiențele obținute în cadrul programului de formare vor fi diseminate în comunitatea securității cibernetice pentru a spori gradul de conștientizare și de pregătire în domeniul securității cibernetice.

<u>WP4: Consolidarea capabilitatii tehnice de securitate cibernetica</u>

- Investiții în tehnologie pentru monitorizarea dispozitivelor mobile din perspectiva securității cibernetice

Investițiile în tehnologie pentru monitorizarea dispozitivelor mobile din perspectiva securității cibernetice se referă la achiziționarea și implementarea de soluții de securitate a dispozitivelor mobile, care să permită monitorizarea și gestionarea acestora în ceea ce privește securitatea informațiilor și a datelor. Aceste soluții pot include, printre altele, instrumente de gestionare a parolelor, criptare a datelor, protecție împotriva virușilor și a malware-ului, restricționarea accesului la rețelele interne sau la anumite aplicații și servicii, dar și monitorizarea activității și a comportamentului utilizatorilor, astfel încât să poată fi identificate și prevenite potențialele amenințări cibernetice. Această investiție contribuie la îmbunătățirea securității cibernetice în cadrul Primăriei Bistrița, prin creșterea nivelului de protecție a datelor și informațiilor confidențiale ale cetățenilor, precum și a infrastructurii IT a Primăriei.

Planul de implementare pentru activitatea de investiții în tehnologie pentru monitorizarea dispozitivelor mobile din perspectiva securității cibernetice implică următorii pași:

1. Identificarea nevoilor și obiectivelor de securitate cibernetică pentru dispozitivele mobile utilizate de Primăria Bistrița.
2. Evaluarea soluțiilor tehnologice disponibile pe piață și selectarea celor mai potrivite pentru nevoile identificate.
3. Proiectarea și implementarea unei soluții de monitorizare a dispozitivelor mobile, inclusiv instalarea și configurarea de aplicații de securitate, astfel încât să se asigure că dispozitivele sunt securizate și actualizate corespunzător.
4. Testarea soluției pentru a se asigura că funcționează corespunzător și că este eficientă din punct de vedere al costurilor.
5. Implementarea unui plan de formare pentru utilizatorii dispozitivelor mobile, astfel încât să se asigure că aceștia sunt conștienți de riscurile de securitate cibernetică și că utilizează dispozitivele într-un mod sigur și responsabil.
6. Implementarea unui plan de mentenanță și actualizare pentru soluția de monitorizare a dispozitivelor mobile, astfel încât să se asigure că aceasta rămâne eficientă și actualizată în timp.

- Investiții în tehnologie pentru monitorizarea sistemului și infrastructurii IT din perspectiva securității cibernetice

Investițiile în tehnologie pentru monitorizarea sistemului și infrastructurii IT din perspectiva securității cibernetice reprezintă o activitate importantă pentru asigurarea securității datelor și a sistemelor informatice. Această activitate implică implementarea de instrumente și soluții tehnologice care permit monitorizarea și gestionarea securității sistemelor informatice și a infrastructurii IT din Primăria Bistrița. Astfel, aceste soluții pot include firewall-uri, sisteme de detectare a intrusilor, sisteme de autentificare multi-factor, soluții de criptare a datelor, soluții de backup și recuperare a datelor, precum și alte tehnologii avansate de securitate cibernetică. Aceste investiții pot ajuta la prevenirea pierderii datelor, a fraudelor cibernetice și a altor amenințări cibernetice, protejând astfel afacerile și comunitatea locală.

Planul de implementare pentru investiții în tehnologie pentru monitorizarea sistemului și infrastructurii IT din perspectiva securității cibernetice poate include următoarele etape:

1. Evaluarea infrastructurii IT existente pentru a identifica punctele vulnerabile și lacunele de securitate.
2. Identificarea soluțiilor tehnologice care pot fi implementate pentru monitorizarea sistemului și infrastructurii IT.
3. Evaluarea și selecția soluțiilor tehnologice potrivite în funcție de nevoile organizației și bugetul disponibil.
4. Implementarea soluțiilor tehnologice, inclusiv firewall-uri, sisteme de detecție a intrușilor și autentificare multi-factor.
5. Configurarea soluțiilor tehnologice pentru a se potrivi cu infrastructura IT existentă și nevoile organizației.
6. Testarea soluțiilor tehnologice pentru a se asigura că acestea sunt eficiente și că îndeplinesc obiectivele de securitate cibernetică ale organizației.
7. Implementarea unui plan de mentenanță și actualizare a soluțiilor tehnologice pentru a se asigura că acestea sunt mereu actualizate și funcționează corespunzător.
8. Training-ul personalului IT și angajaților pentru utilizarea soluțiilor tehnologice și pentru a se asigura că aceștia înțeleg importanța securității cibernetice și rolul lor în protejarea organizației.

- Implementarea de solutii de securitate a datelor pentru a asigura protectia datelor cu caracter personal si confidential ale cetatenilor

Implementarea de soluții de securitate a datelor implică utilizarea unor tehnologii și metode de protejare a datelor cu caracter personal și confidential ale cetățenilor împotriva accesului neautorizat, a pierderii, furtului sau distrugerii acestora. Aceste soluții de securitate includ criptarea datelor, autentificarea multi-factor, controlul accesului, auditarea și monitorizarea activităților cu date sensibile, precum și implementarea politicilor de securitate și procedurilor de management al datelor. Implementarea unor astfel de soluții de securitate poate asigura protecția datelor și a confidențialității acestora, oferind în același timp încredere și satisfacție cetățenilor în privința modului în care instituția respectă reglementările privind protecția datelor personale.

Planul de implementare pentru activitatea "Implementarea de solutii de securitate a datelor pentru a asigura protectia datelor cu caracter personal si confidential ale cetatenilor" poate include urmatoarele etape:

1. Identificarea datelor cu caracter personal si confidential ale cetatenilor care necesita protectie.
2. Evaluarea riscurilor de securitate cibernetica care ar putea afecta aceste date.
3. Selectarea solutiilor de securitate adecvate, cum ar fi criptarea datelor, autentificarea multi-factor si/sau monitorizarea accesului la date.
4. Implementarea solutiilor selectate.
5. Testarea si verificarea solutiilor pentru a se asigura ca ofera nivelul adecvat de protectie pentru datele cu caracter personal si confidential ale cetatenilor.
6. Formarea angajatilor Primariei Bistrita privind utilizarea solutiilor de securitate si practicile recomandate pentru protejarea datelor cu caracter personal si confidential.
7. Monitorizarea continua a solutiilor de securitate implementate si a datelor cu caracter personal si confidential pentru a detecta eventuale probleme sau vulnerabilitati si a lua masuri remediatore.
8. Actualizarea solutiilor de securitate la nivelul necesar si adaptarea acestora la evolutiile tehnologice si schimbarile legislative in materie de protectie a datelor cu caracter personal si confidential.

- Implementarea de solutii de securitate a retelelor si a infrastructurii IT, inclusiv firewall-uri, sisteme de detectare a intrusilor si sisteme de autentificare multi-factor

Implementarea de soluții de securitate a rețelelor și a infrastructurii IT presupune utilizarea unor instrumente precum firewall-uri, sisteme de detectare a intrușilor și sisteme de autentificare multi-factor pentru a asigura securitatea și protecția rețelelor și a infrastructurii IT. Aceste soluții ajută la protejarea datelor și a informațiilor confidențiale împotriva amenințărilor cibernetice, cum ar fi atacurile DDoS, furtul de date, hacking-ul și multe altele. Firewall-urile filtrează traficul de rețea înainte ca acesta să ajungă la dispozitivele și sistemul IT, iar sistemele de detectare a intrușilor identifică activitățile suspecte și previn accesul neautorizat. Sistemele de autentificare multi-factor implică utilizarea mai multor metode de autentificare, cum ar fi parola și autentificarea prin biometrie, pentru a crește securitatea rețelelor și a infrastructurii IT. Implementarea acestor soluții ajută la reducerea riscurilor cibernetice și la protejarea datelor și informațiilor confidențiale.

Planul de implementare pentru activitatea de implementare de solutii de securitate a retelelor si a infrastructurii IT va consta dintr-un set de actiuni care vor fi luate pentru a proteja si a preveni orice vulnerabilitate sau incidente de securitate cibernetica. Printre aceste actiuni se numara:

1. Auditul infrastructurii IT si a retelei pentru identificarea punctelor vulnerabile si a riscurilor de securitate cibernetica.

2. Implementarea firewall-urilor si a altor solutii de securitate, cum ar fi sistemele de detectare a intrusilor si sistemele de autentificare multi-factor, pentru a proteja reteaua si infrastructura IT impotriva atacurilor cibernetice.
3. Actualizarea si mentinerea sistemelor si a aplicatiilor cu cele mai recente patch-uri de securitate si actualizari de firmware.
4. Implementarea de politici de securitate robuste si proceduri de gestionare a incidentelor pentru a raspunde la orice incidente de securitate cibernetica.
5. Monitorizarea continua a infrastructurii IT si a retelei pentru a identifica activitati suspecte si pentru a preveni eventuale incidente de securitate cibernetica.

- Dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica

Dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica presupune definirea unui set de pasi si responsabilitati pentru a raspunde rapid la evenimente de securitate cibernetica. Acesta include stabilirea unor proceduri clare de comunicare interna si externa, evaluarea si clasificarea incidentelor, identificarea cauzelor si remedierea acestora, precum si documentarea si raportarea incidentului. Protocoalele pot fi personalizate pentru a raspunde nevoilor specifice ale Primariei Bistrita, si pot include un plan de actiune, un calendar de implementare si o lista de contacte de urgenta. O gestionare adecvata a incidentelor de securitate cibernetica poate reduce timpul de inactivitate si riscul de pierdere a datelor sau a informatiilor confidentiale.

Planul de implementare pentru activitatea "Dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica" include urmatoarele etape:

1. Identificarea si clasificarea incidentelor de securitate cibernetica, in functie de gravitatea si impactul acestora asupra activitatii Primariei Bistrita.
2. Dezvoltarea de proceduri si protocoale pentru raportarea incidentelor de securitate cibernetica, inclusiv criteriile de notificare, fluxurile de lucru si raspunsurile de urmarire.
3. Crearea unui catalog actualizat al incidentelor cibernetice si a solutiilor corespunzatoare pentru fiecare tip de incident.
4. Dezvoltarea de planuri de gestionare a incidentelor pentru situatiile de criza si pentru incidentele majore de securitate cibernetica.
5. Testarea si validarea planurilor de gestionare a incidentelor, prin organizarea de exercitii de simulare a incidentelor.
6. Formarea si instruirea personalului relevant cu privire la procedurile de gestionare a incidentelor de securitate cibernetica si implicarea acestora in exercitiile de simulare.
7. Implementarea de solutii tehnologice si de securitate cibernetica pentru monitorizarea, detectarea si raportarea incidentelor de securitate cibernetica.
8. Evaluarea continua a procedurilor de gestionare a incidentelor de securitate cibernetica si actualizarea acestora, dupa cum este necesar.

<u>Supliment</u>

Primaria Bistrita poate analiza si extinde proiectul cu fundamentarea „Planului de Interventie in Situatii Critice de Continuitate, Redresare si Rezilienta in Cazul Crizelor Generate de Reusita Atacurilor Cibernetice Majore”.

Planul de Interventie in Situatii Critice de Continuitate, Redresare si Rezilienta in Cazul Crizelor Generate de Reusita Atacurilor Cibernetice Majore trebuie sa contina specificatii clare si detaliate privind modul in care organizatia va actiona in cazul unei astfel de situatii. Printre aceste specificatii se pot numara:

1. Identificarea responsabilitatilor: Planul trebuie sa defineasca responsabilitatile fiecarei persoane si departamentului din organizatie pentru a garanta ca toate aspectele sunt acoperite.
2. Evaluarea riscurilor: Planul trebuie sa includa o evaluare detaliata a riscurilor pentru a identifica posibilele scenarii care ar putea aparea si pentru a determina nivelul de risc asociat acestora.
3. Identificarea scenariilor: Planul trebuie sa includa o lista a posibilelor scenarii care pot fi generate de un atac cibernetic major si sa defineasca procedurile pentru fiecare.
4. Implementarea unui sistem de alerta timpurie: Planul trebuie sa includa un sistem de alerta timpurie care sa permita organizatiei sa detecteze si sa reactioneze rapid in cazul unui atac.
5. Proceduri de comunicare: Planul trebuie sa includa proceduri clare de comunicare cu toate departamentele implicate si cu parti externe, cum ar fi furnizorii sau autoritatile.
6. Redundanta sistemelor si serviciilor critice: Planul trebuie sa prevada masuri pentru asigurarea redundantei sistemelor si serviciilor critice astfel incat sa se poata mentine activitatile esentiale ale organizatiei.
7. Testarea si actualizarea planului: Planul trebuie sa fie testat in mod regulat pentru a se asigura ca este actual si eficient si trebuie actualizat in functie de noile riscuri identificate sau de noile tehnologii si solutii disponibile.
8. Instruire experientiala si formare: Planul trebuie sa prevada programe de instruire experientiala si formare pentru toti angajatii implicati, astfel incat sa fie pregatiti sa actioneze in cazul unei situatii critice de continuitate, redresare si rezilienta generata de un atac cibernetic major.

Există mai multe standarde și ghiduri care pot fi considerate în elaborarea unui Plan de Intervenție în Situații Critice de Continuitate, Redresare și Reziliență în cazul crizelor generate de reușita atacurilor cibernetice majore. Unele dintre acestea sunt:

1. ISO 22301:2019 - Sisteme de management al continuității afacerii - Cerințe
2. NIST SP 800-61 Rev. 2 - Computer Security Incident Handling Guide
3. CERT Resilience Management Model (CERT-RMM)
4. ITIL Continuity Management Process
5. NIST SP 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations
6. ISO 22301 - Sistemul de management al continuității afacerii - specifică cerințele pentru planificarea, implementarea, monitorizarea și îmbunătățirea unui sistem de management al continuității afacerii.
7. BS 25999 - Managementul continuității afacerii - specifică cerințele pentru implementarea, monitorizarea și îmbunătățirea unui sistem de management al continuității afacerii.
8. ISO 27031 - Ghid pentru managementul continuității afacerii în contextul securității informațiilor - oferă orientări pentru planificarea și implementarea unui plan de continuitate a afacerii în contextul securității informațiilor.
9. ISO 22316 - Ghid pentru reziliența organizațională - oferă o orientare privind implementarea unui sistem de management al rezilienței organizaționale și abordează conceptele de conducere, planificare, implementare, evaluare și îmbunătățire continuă.
10. NIST SP 800-34 - Ghid pentru managementul continuității afacerii - furnizează orientări privind dezvoltarea, implementarea și menținerea unui program de management al continuității afacerii.

Aceste standarde și ghiduri oferă un cadru general pentru dezvoltarea unui plan de intervenție în situații critice și pentru asigurarea continuității afacerii în cazul unor atacuri cibernetice majore. Ele pot fi utilizate ca punct de plecare pentru dezvoltarea unui plan personalizat, adaptat nevoilor și specificului organizației respective.

Sustenabilitate si impact

Sectiunea de "Sustenabilitate si Impact" prezinta modul in care proiectul de securitate cibernetica implementat in Primaria Bistrita asigura o infrastructura sigura si protejata impotriva atacurilor cibernetice, impactul pozitiv asupra angajatilor, cetatenilor si comunitatii locale, precum si masurile de protectie a mediului asociate cu infrastructura de IT.

In privinta sustenabilitatii evidentiem:

1. Continuarea investitiilor in tehnologie si formarea angajatilor in domeniul securitatii cibernetice, pentru a asigura o infrastructura sigura si protejata impotriva atacurilor cibernetice pe termen lung - Prin continuarea investitiilor in tehnologie si formarea angajatilor, proiectul va fi sustenabil si securitatea cibernetica a Primariei Bistrita va fi asigurata pe termen lung. Prin aceasta actiune, se va asigura mentinerea nivelului de securitate cibernetica, evitandu-se riscurile si amenintarile potential periculoase care ar putea afecta functionalitatea si performanta sistemelor IT ale Primariei.
2. Asigurarea unei bune coordonari si comunicari intre membrii echipei de proiect si angajatii Primariei Bistrita, pentru a mentine nivelul ridicat de securitate cibernetica - O buna coordonare si comunicare intre membrii echipei de proiect si angajatii Primariei Bistrita este esentiala pentru asigurarea nivelului ridicat de securitate cibernetica si pentru a evita incidentele de securitate cibernetica. Prin aceasta actiune, se va asigura un flux continuu de informatii intre membrii echipei de proiect si angajatii Primariei Bistrita, permitandu-le sa identifice si sa remedieze rapid eventualele probleme.
3. Sensibilizarea si educarea angajatilor si cetatenilor in ceea ce priveste securitatea cibernetica si nevoia de a proteja datele lor personale si confidentiale - Sensibilizarea si educarea angajatilor si cetatenilor privind securitatea cibernetica si nevoia de a proteja datele lor personale si confidentiale este cruciala pentru a asigura sustenabilitatea si succesul proiectului. Prin aceasta actiune, angajatii si cetatenii vor fi constientizati cu privire la riscurile si amenintarile cibernetice si vor fi informati cu privire la masurile de precautie pe care trebuie sa le ia pentru a-si proteja datele personale si confidentiale.

Impactul social, economic si de mediu al proiectului va fi pozitiv si se va manifesta prin:

1. Cresterea nivelului de securitate cibernetica in Primaria Bistrita, asigurand protectia informatiilor personale si confidentiale ale cetatenilor si a infrastructurii IT - Proiectul va avea un impact pozitiv asupra securitatii cibernetice a Primariei Bistrita, prin asigurarea protectiei informatiilor personale si confidentiale ale cetatenilor si a infrastructurii IT. Prin aceasta actiune, se vor reduce riscurile si amenintarile cibernetice care ar putea afecta functionarea si performanta sistemelor IT ale Primariei Bistrita.
2. Cresterea increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale - Cresterea increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale este cruciala pentru a asigura sustenabilitatea si succesul proiectului.
3. Contribuirea la dezvoltarea economică și socială a comunității locale prin creșterea încrederii cetățenilor în Primăria Bistrița și prin asigurarea protecției informațiilor confidentiale și a infrastructurii IT - Implementarea unui plan solid de securitate cibernetică în Primăria Bistrița va consolida încrederea cetățenilor în administrația locală și în capacitatea acesteia de a proteja informațiile personale și confidentiale. În plus, un nivel ridicat de securitate cibernetică va contribui la îmbunătățirea mediului de afaceri local și va atrage investitori noi în zonă. Aceasta poate avea un impact pozitiv asupra economiei locale și poate duce la creșterea numărului de locuri de muncă și îmbunătățirea calității vieții în comunitate. Prin urmare, dezvoltarea și implementarea unui plan de securitate cibernetică eficient poate juca un rol important în dezvoltarea economică și socială a comunității locale.

4. Reducerea impactului asupra mediului prin creșterea eficienței și a siguranței sistemelor IT, reducând astfel consumul de energie și emisiile de gaze cu efect de seră - Implementarea măsurilor de securitate cibernetică poate reduce impactul asupra mediului prin creșterea eficienței și siguranței sistemelor IT, reducând astfel consumul de energie și emisiile de gaze cu efect de seră. În plus, un nivel ridicat de securitate cibernetică poate reduce riscul de defrișare a pădurilor și de poluare a râurilor și a solului prin evitarea unor practici care ar fi necesare în cazul unui incident cibernetic. Astfel, implementarea măsurilor de securitate cibernetică nu numai că protejează datele personale și infrastructura IT, ci poate avea și un impact pozitiv asupra mediului înconjurător.
5. Reducerea riscului de pierdere a datelor personale si informatiilor confidentiale ale cetatenilor este unul dintre obiectivele principale ale proiectului de securitate cibernetica. Prin implementarea solutiilor de securitate adecvate si prin formarea angajatilor in acest domeniu, riscul de pierdere sau compromitere a datelor personale si confidentiale ale cetatenilor va fi redus semnificativ. Acest lucru va asigura siguranta si increderea cetatenilor in Primaria Bistrita si va contribui la consolidarea relatiilor de incredere intre Primarie si cetateni.
6. Reducerea costurilor si a timpului alocat pentru remedierea unui incident cibernetic este un alt obiectiv important al proiectului. Implementarea solutiilor adecvate de securitate cibernetica, precum si formarea angajatilor pentru a face fata incidentelor de securitate cibernetica, va reduce timpul si costurile alocate pentru remedierea unui astfel de incident. Acest lucru va avea un impact pozitiv asupra eficientei si eficacitatii organizatiei si va ajuta la asigurarea continuitatii si redresarii rapide in cazul unui atac cibernetic major.

Pentru a asigura un nivel ridicat de securitate cibernetica, proiectul va include o serie de activitati care vor fi implementate pe o perioada 18 luni, in functie de complexitatea si volumul de date gestionate, numarul si complexitatea aplicatiilor si sistemelor IT, precum si dimensiunea si complexitatea retelei si a infrastructurii IT. Printre aceste activitati se numara: analiza avansata a informatiilor privind amenintarile persistente, testarea Cyberrange, raportarea managementului riscului de securitate cibernetica, monitorizarea vulnerabilitatii securitatii cibernetice, inteligenta cibernetica a amprentei digitale, raspuns la incident, Aviz Pentest, evaluarea securitatii tehnice, formare profesionala pentru Apărător Cyber Security, Clădiri inteligente și securitatea clădirilor, Securitate cibernetică pentru toată lumea si specializare in securitate cibernetica pentru sectorul public, evaluarea vulnerabilitatii din punct de vedere al resurselor umane, tehnologiei si politicii de securitate, investitii in tehnologie pentru monitorizarea dispozitivelor mobile si a sistemului si infrastructurii IT din perspectiva securitatii cibernetice, implementarea de solutii de securitate a datelor si dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica, auditul de securitate cibernetica pentru toate aplicatiile si sistemele IT utilizate de Primaria Bistrita, implementarea de solutii de securitate a retelelor si a infrastructurii IT, inclusiv firewall-uri, sisteme de detectare a intrusilor si sisteme de autentificare multi-factor, testarea exhaustiva a angajatilor pe GDPR si securitate cibernetica si sensibilizarea acestora privind amenintarile cibernetice si metodele de prevenire a acestora. Aceste activitati vor avea un impact pozitiv asupra securitatii cibernetice a Primariei Bistrita si vor asigura protectia informatiilor personale si confidentiale ale cetatenilor, reducerea costurilor si a timpului alocat pentru remedierea unui incident cibernetic, cresterea increderii cetatenilor in capacitatea Primariei Bistrita de a proteja informatiile lor personale si confidentiale, reducerea impactului asupra mediului prin cresterea eficientei si a sigurantei sistemelor IT, contribuirea la dezvoltarea economica si sociala a comunitatii locale si cresterea nivelului de securitate cibernetica in Primaria Bistrita.

Implementarea proiectului va avea o durata de 18 luni, dupa cum urmeaza:

1. Analiza avansata a informatiilor privind amenintarile persistente - 2 luni
2. Testarea Cyberrange - 1 luna
3. Raportarea managementului riscului de securitate cibernetica - 2 luni
4. Monitorizarea vulnerabilitatii securitatii cibernetice - 3 luni
5. Inteligenta cibernetica a amprentei digitale - 3 luni

6. Raspuns la incident - 2 luni
7. Aviz Pentest - 1 luna
8. Evaluarea securitatii tehnice - 2 luni
9. Formare profesionala - Apărător Cyber Security - 1 luna
10. Formare profesionala - Clădiri inteligente și securitatea clădirilor - 1 luna
11. Formare profesionala - Securitate cibernetică pentru toată lumea - 1 luna
12. Formare profesionala - Specializare in securitate cibernetica pentru sectorul public - 1 luna
13. Evaluarea vulnerabilității din punct de vedere al resurselor umane - 2 luni
14. Evaluarea vulnerabilității din punct de vedere al tehnologiei - 2 luni
15. Evaluarea vulnerabilității din punct de vedere al politicii de securitate - 2 luni
16. Investiții în tehnologie pentru monitorizarea dispozitivelor mobile din perspectiva securității cibernetice - 5 luni
17. Investiții în tehnologie pentru monitorizarea sistemului și infrastructurii IT din perspectiva securității cibernetice - 5 luni
18. Implementarea de solutii de securitate a datelor pentru a asigura protectia datelor cu caracter personal si confidential ale cetatenilor: 3-6 luni, in functie de complexitatea si volumul de date gestionate.
19. Dezvoltarea de proceduri si protocoale pentru gestionarea incidentelor de securitate cibernetica: 2-3 luni, in functie de complexitatea procedurilor si de numarul de angajati implicati.
20. Auditul de securitate cibernetica pentru toate aplicatiile si sistemele IT utilizate de Primaria Bistrita: 2-3 luni, in functie de numarul si complexitatea aplicatiilor si a sistemelor IT.
21. Implementarea de solutii de securitate a retelelor si a infrastructurii IT, inclusiv firewall-uri, sisteme de detectare a intrusilor si sisteme de autentificare multi-factor: 4-6 luni, in functie de dimensiunea si complexitatea retelei si a infrastructurii IT.
22. Testarea exhaustiva a angajatilor pe GDPR si securitate cibernetica si sensibilizarea angajatilor Primariei Bistrita privind amenintarile cibernetice si metodele de prevenire a acestora: 1-2 luni, in functie de numarul de angajati implicati si de complexitatea informatiilor transmise.

Daca se doreste si implementarea Planului de Interventie in Situatii Critice de Continuitate, Redresare si Rezilienta in Cazul Crizelor Generate de Reusita Atacurilor Cibernetice Majore, trebuie alocat intre 6 si 12 luni acestui sub-proiect, cu un buget intre 60.000 si 100.000 euro.

FISA DE PROIECT FANION

Titlu

Politicile interne în privința securității cibernetice

Coordonator din partea consultantului

Stelian Brad

Rezumat

Proiectul "Politicile interne in privinta securitatii cibernetice" se refera la dezvoltarea si implementarea politicii interne de securitate cibernetica la nivelul Primariei Bistrita. Acesta este un proiect deosebit de important, deoarece institutiile publice trebuie sa-si protejeze activ resursele si informatiile impotriva amenintarilor cibernetice, iar Primaria Bistrita gestioneaza o serie de informatii si date sensibile, cum ar fi datele personale ale angajatilor si cetatenilor, precum si informatii legate de operatiunile administrative. In cazul unui atac cibernetic, aceste informatii pot fi compromise, ceea ce ar putea duce la consecinte negative semnificative.

Scopul acestui proiect este de a proteja informatiile si resursele impotriva amenintarilor cibernetice, de a dezvolta o cultura a securitatii cibernetice si de a reduce riscul de atacuri cibernetice. Proiectul isi propune sa dezvolte si sa implementeze politici interne de securitate cibernetica la nivelul Primariei Bistrita, sa formeze angajatii cu privire la securitatea cibernetica si sa monitorizeze si sa evalueze performanta in domeniul securitatii cibernetice.

Obiectivele proiectului "Politicile interne in privinta securitatii cibernetice" vor ajuta la dezvoltarea unei culturi a securitatii cibernetice in cadrul institutiei si la protejarea informatiilor si resurselor impotriva amenintarilor cibernetice. Aceste obiective sunt urmatoarele:

1. Dezvoltarea unui cadru de politici interne de securitate cibernetica care sa respecte cele mai bune practici si standarde internationale in materie de securitate cibernetica.
2. Implementarea politicii interne de securitate cibernetica in cadrul tuturor departamentelor si serviciilor Primariei Bistrita.
3. Formarea angajatilor din cadrul Primariei Bistrita cu privire la securitatea cibernetica si la modul in care pot contribui la protejarea activelor si informatiilor Primariei.
4. Evaluarea si monitorizarea continua a performantei in domeniul securitatii cibernetice si raportarea de incidente de securitate cibernetica.

Rezultatele asteptate ale proiectului "Politicile interne in privinta securitatii cibernetice" includ urmatoarele:

1. O politica interna de securitate cibernetica elaborata in conformitate cu cele mai bune practici si standarde internationale.
2. Implementarea cu succes a politicii interne de securitate cibernetica in cadrul tuturor departamentelor si serviciilor Primariei Bistrita.
3. Angajatii Primariei Bistrita vor fi instruiti si pregatiti cu privire la securitatea cibernetica.
4. Evaluarea continua a performantei in domeniul securitatii cibernetice si raportarea incidentelor de securitate cibernetica vor ajuta la identificarea si abordarea prompta a oricarei probleme legate de securitatea cibernetica.

Planul de implementare al proiectului "Politicile interne in privinta securitatii cibernetice" include urmatoarele etape:

1. Dezvoltarea politicii interne de securitate cibernetica, care include identificarea celor mai bune practici si standarde internationale in materie de securitate cibernetica, elaborarea politicii si revizuirea si aprobarea acesteia de catre consiliul local.
2. Implementarea politicii interne de securitate cibernetica, inclusiv formarea tuturor angajatilor din cadrul Primariei Bistrita privind politica interna de securitate cibernetica, implementarea politicii in toate departamentele si serviciile Primariei Bistrita si monitorizarea continua a respectarii regulilor si procedurilor de securitate cibernetica.
3. Evaluarea si monitorizarea continua a performantei in domeniul securitatii cibernetice, prin implementarea unui sistem de raportare a incidentelor de securitate cibernetica, monitorizarea

continua a performantei in domeniul securitatii cibernetice si a masurilor de protectie si evaluarea regulata a politicii interne de securitate cibernetica si a procedurilor aferente.

Sustenabilitatea si impactul proiectului "Politicile interne in privinta securitatii cibernetice" trebuie sa conduca la implementarea acestei politici interne de securitate cibernetica care va asigura ca Primaria Bistrita are un cadru solid pentru a proteja informatiile si resursele sale impotriva amenintarilor cibernetice. In plus, formarea angajatilor cu privire la securitatea cibernetica va ajuta la dezvoltarea unei culturi a securitatii cibernetice in cadrul institutiei, care va contribui la reducerea riscului de atacuri cibernetice si la protejarea informatiilor si resurselor institutiei.

Proiectul va fi implementat pe o perioada de 18 luni si va implica dezvoltarea de politici si proceduri, formare, evaluare si monitorizare continua a performantei in domeniul securitatii cibernetice. Implementarea cu succes a acestui proiect va asigura ca Primaria Bistrita respecta cele mai bune practici si standarde internationale in materie de securitate cibernetica si va ajuta la protejarea informatiilor si resurselor institutiei impotriva atacurilor cibernetice.

Pentru a asigura succesul acestui proiect, este important ca Primaria Bistrita sa aloce resurse adecvate si sa aiba angajamentul necesar pentru dezvoltarea si implementarea politicii interne de securitate cibernetica. In plus, este important ca angajatii sa fie bine pregatiti si sa aiba cunostinte solide despre securitatea cibernetica, astfel incat sa poata contribui la protectia informatiilor si resurselor institutiei.

Context si justificare

Contextul actual international este marcat de o creștere rapidă a amenințărilor cibernetice. Instituțiile publice, precum Primăria Bistrița, sunt vulnerabile la aceste amenințări și trebuie să-și protejeze activ resursele și informațiile împotriva atacurilor cibernetice. Datele personale ale angajaților și ale cetățenilor, precum și informațiile legate de operațiunile administrative, sunt foarte importante și trebuie protejate de atacurile cibernetice. În cazul unui astfel de atac, aceste informații pot fi compromise, ceea ce poate duce la consecințe negative semnificative pentru instituție și pentru cetățeni. În cazul Primăriei Bistrița, atacurile cibernetice ar putea compromite informațiile și resursele instituției, inclusiv date personale ale angajaților și ale cetățenilor, informații legate de operatiunile administrative și alte informații sensibile.

Potrivit unui raport realizat de IBM, costul mediu al unui atac cibernetic pentru o instituție publică este de aproximativ 4,7 milioane de dolari. Acest cost poate include cheltuieli pentru remedierea atacului, investigații, recuperarea datelor pierdute și pierderea de venituri. În plus, un astfel de atac poate duce la pierderea încrederii cetățenilor în instituție și poate avea un impact negativ asupra reputației Primăriei Bistrița.

De asemenea, conform unui studiu realizat de Cybersecurity Ventures, până în 2025 costurile globale pentru atacurile cibernetice vor depăși 10 trilioane de dolari, iar pierderile provocate de acestea vor crește de la an la an.

În ceea ce privește amenințările cibernetice, acestea se referă la orice încercare de a obține acces neautorizat la sisteme informatice și date. Acestea pot fi sub forma de viruși, malware, atacuri prin intermediul rețelelor sociale, DDoS, phishing, ransomware și multe altele. Este important să se înțeleagă că amenințările cibernetice pot veni din diferite surse, inclusiv din interiorul instituției. De aceea, este necesară dezvoltarea unor politici interne solide de securitate cibernetică pentru a reduce riscul de atacuri cibernetice și pentru a proteja activ resursele și informațiile Primăriei Bistrița.

În ultimii ani, atacurile cibernetice împotriva instituțiilor publice au crescut semnificativ. Potrivit unui studiu realizat de Centrul European de Cercetare și Analiză a Amenințărilor Cibernetice (ENISA), numărul atacurilor cibernetice împotriva instituțiilor publice a crescut cu 14% în anul 2020 față de anul precedent. Atacurile de securitate cibernetică au continuat să crească în a doua jumătate a anului 2021 și 2022, nu numai în ceea ce privește vectorii și cifrele dar și în ceea ce privește impactul acestora. Criza Rusia-Ucraina a definit o nouă eră pentru războiul cibernetic și hacktivismul, rolul său și impactul său asupra conflictelor. Statele și alte operațiuni cibernetice se vor adapta foarte probabil la acest nou starea de fapt și să profite de noutățile și provocările aduse de acest război. Cu toate acestea, aceasta noua paradigma adusă de război are implicații pentru normele internaționale în spațiul cibernetic și, mai precis, pentru sponsorizarea atacurilor cibernetice și țintirea infrastructurii civile critice. Din cauza situatiei internaţionale volatile, ne așteptăm să observăm mai multe operațiuni cibernetice conduse de geopolitică în viitorul apropiat și mediu.

În plus, potrivit unui raport al companiei de securitate cibernetică Kaspersky, în 2020, peste 80% dintre angajații instituțiilor publice au lucrat de la distanță, ceea ce a crescut vulnerabilitatea la atacurile cibernetice. Aceste atacuri au costat, în medie, aproximativ 500.000 de dolari pentru fiecare incident.

În ceea ce privește România, un raport al Inspectoratului General al Poliției Române arată că numărul infracțiunilor cibernetice a crescut cu 25% în primele nouă luni ale anului 2020 față de aceeași perioadă a anului precedent. Un raport al DNSC arată că atacurile informatice împotriva instituțiilor sau firmelor românești au crescut exponențial de la începerea conflictului din Ucraina. Experții în domeniu sunt de părere că autoritățile române nu sunt pregătite pentru un atac masiv,

fapt confirmat și de gruparea Anonymous România. Acest lucru subliniază importanța luării unor măsuri pentru protejarea instituțiilor publice, cum ar fi Primăria Bistrița, împotriva amenințărilor cibernetice.

De asemenea, potrivit unui studiu realizat de PwC, instituțiile publice sunt mai vulnerabile la atacurile cibernetice decât companiile private, întrucât acestea sunt mai deschise publicului și au mai multe puncte de acces la informații sensibile.

Dezvoltarea conceptului de „cybercrime as a service" reprezintă o amenințare serioasă pentru instituțiile publice, inclusiv pentru Primăria Bistrița. Această practică permite persoanelor care nu au cunoștințe tehnice avansate în domeniul informatic să achiziționeze servicii de hacking și să lanseze atacuri cibernetice împotriva instituțiilor.

Această tendință a condus la o creștere a numărului de atacuri cibernetice asupra instituțiilor publice. Dezvoltarea „cybercrime as a service" poate avea implicații semnificative pentru Primăria Bistrița, inclusiv pentru resursele și informațiile sale. Prin intermediul acestei practici, hackerii pot accesa datele și informațiile sensibile ale Primăriei și le pot utiliza în scopuri ilegale, cum ar fi frauda sau șantajul. De asemenea, un atac cibernetic lansat de către un furnizor de servicii de „cybercrime as a service" poate fi mult mai dificil de detectat și de contracarat, ceea ce poate duce la pierderi semnificative de timp și resurse pentru instituție.

În plus, atacurile cibernetice lansate prin intermediul „cybercrime as a service" pot fi direcționate și asupra sistemelor critice ale Primăriei Bistrița, cum ar fi rețelele de energie electrică sau sistemele de comunicații, ceea ce poate duce la întreruperi de servicii și la pierderi semnificative de resurse.

Un studiu realizat de Recorded Future arată că serviciile de hacking ca serviciu (HaaS) sunt disponibile în prezent pe piața neagră și pot fi achiziționate de oricine dorește să lanseze un atac cibernetic. Acest studiu a constatat că, în general, costul acestor servicii variază de la câteva zeci de dolari la câteva sute de dolari pe oră.

De asemenea, potrivit unui raport realizat de Centrul European de Cercetare și Analiză a Amenințărilor Cibernetice (ENISA), instituțiile publice sunt ținte frecvente ale serviciilor de hacking ca serviciu (HaaS) și a altor tipuri de atacuri cibernetice. Acest raport constată că instituțiile publice sunt mai expuse riscului de a fi ținte ale unor astfel de atacuri decât alte sectoare, cum ar fi cel financiar sau cel industrial.

Aceste date sugerează că „cybercrime as a service" reprezintă o amenințare serioasă pentru instituțiile publice și că acestea sunt în mod frecvent țintite de către hackeri. Prin urmare, este esențial ca instituțiile publice să ia măsuri proactive pentru a se proteja împotriva acestor amenințări, inclusiv prin dezvoltarea și implementarea de politici interne solide de securitate cibernetică, formarea angajaților și implementarea unor soluții tehnice de securitate adecvate.

Primăria Bistrița este o instituție publică importantă care își desfășoară activitatea în beneficiul cetățenilor din oraș. Aceasta are o gamă largă de responsabilități, inclusiv administrarea serviciilor publice, dezvoltarea orașului și protejarea intereselor cetățenilor săi. Din acest motiv, este necesar să se dezvolte și să se implementeze politici interne solide de securitate cibernetică pentru a proteja activ resursele și informațiile Primăriei Bistrița și pentru a reduce riscul de atacuri cibernetice.

Pe lângă consecințele financiare, atacurile cibernetice pot duce la încălcarea drepturilor cetățenilor și la compromiterea datelor personale. Prin urmare, este necesară protejarea acestor informații sensibile prin implementarea unor politici interne de securitate cibernetică. În plus, există riscul

ca astfel de atacuri să afecteze și imaginea instituției, ceea ce poate duce la pierderea încrederii cetățenilor în Primăria Bistrița.

Dezvoltarea și implementarea de politici interne solide de securitate cibernetică va ajuta la protejarea activelor și informațiilor Primăriei Bistrița împotriva amenințărilor cibernetice și va contribui la creșterea încrederii cetățenilor în instituție. Aceste politici vor fi elaborate în conformitate cu cele mai bune practici și standarde internaționale în materie de securitate cibernetică și vor fi aplicate în cadrul tuturor departamentelor și serviciilor Primăriei Bistrița. De asemenea, dezvoltarea și implementarea acestor politici va ajuta la dezvoltarea unei culturi a securității cibernetice în cadrul instituției, ceea ce va contribui la reducerea riscului de atacuri cibernetice.

În plus, implementarea de politici interne solide de securitate cibernetică va asigura că Primăria Bistrița respectă cele mai bune practici și standarde internaționale în materie de securitate cibernetică. Implementarea de politici interne solide de securitate cibernetică reprezintă o necesitate crucială pentru Primăria Bistrița, în special în contextul actual al creșterii riscurilor de securitate cibernetică și al amenințărilor din ce în ce mai sofisticate. Prin implementarea unor politici interne de securitate cibernetică bine dezvoltate și bine aplicate, instituția poate reduce semnificativ riscurile și consecințele atacurilor cibernetice asupra propriilor sale sisteme și infrastructură.

Cu toate acestea, implementarea de politici interne solide de securitate cibernetică nu va afecta pozitiv numai securitatea organizației, ci poate avea și un impact semnificativ asupra reputației Primăriei Bistrița și încrederea cetățenilor în instituție. Aceasta poate fi realizată prin respectarea celor mai bune practici și standarde internaționale în materie de securitate cibernetică. Există mai multe standarde internaționale care se concentrează pe securitatea cibernetică, iar adoptarea acestor standarde poate fi foarte benefică pentru instituțiile publice precum Primăria Bistrița. Iată câteva exemple:

1. ISO 27001: Aceasta este una dintre cele mai recunoscute standarde internaționale pentru managementul securității informațiilor. ISO 27001 oferă un cadru cuprinzător pentru implementarea, monitorizarea, revizuirea și îmbunătățirea continuă a sistemelor de management al securității informațiilor. Adoptarea acestei standarde poate ajuta Primăria Bistrița să își protejeze activ informațiile, să își gestioneze riscurile și să își îndeplinească obiectivele de securitate cibernetică.
2. NIST Cybersecurity Framework: Acesta este un cadru de referință dezvoltat de Institutul Național de Standarde și Tehnologie din Statele Unite. Framework-ul se concentrează pe identificarea, protejarea, detectarea, răspunsul și recuperarea din amenințările cibernetice. Adoptarea acestui cadru poate ajuta Primăria Bistrița să își construiască o strategie de securitate cibernetică mai robustă și să își coordoneze eforturile de securitate cibernetică.
3. GDPR: Regulamentul General privind Protecția Datelor este o lege europeană care se concentrează pe protecția datelor personale ale cetățenilor europeni. Adoptarea standardelor GDPR poate ajuta Primăria Bistrița să își protejeze datele personale ale cetățenilor și să își îndeplinească obligațiile legale în materie de protecție a datelor.
4. CIS Controls: Acest cadru oferă o listă de controale de securitate cibernetică care sunt considerate cele mai eficiente pentru a proteja organizațiile împotriva amenințărilor cibernetice. Adoptarea acestor controale poate ajuta Primăria Bistrița să își îmbunătățească securitatea cibernetică și să își reducă riscurile de securitate cibernetică.
5. ENISA (Agenția Europeană pentru Securitate Cibernetică) acționează ca un centru de expertiză în domeniul securității cibernetice. ENISA are ca misiune să ajute Uniunea Europeană și statele membre să-și îmbunătățească nivelul de securitate cibernetică prin furnizarea de informații și sfaturi practice. Recomandările ENISA sunt o serie de documente și ghiduri elaborate de experții în securitate cibernetică ai agenției pentru a ajuta organizațiile să-și îmbunătățească nivelul de securitate cibernetică. Aceste recomandări acoperă o gamă largă de subiecte, de la

securitatea rețelelor și a sistemelor informatice până la gestionarea incidentelor de securitate cibernetică și securitatea datelor. Implementarea recomandărilor ENISA poate fi foarte utilă pentru instituțiile publice, cum ar fi Primăria Bistrița, în îmbunătățirea nivelului lor de securitate cibernetică. De exemplu, documentul ENISA "Ghid pentru gestionarea riscurilor de securitate cibernetică" oferă un cadru de lucru pentru evaluarea riscurilor de securitate cibernetică și luarea măsurilor adecvate pentru a le reduce. Implementarea acestui ghid poate ajuta Primăria Bistrița să identifice și să gestioneze riscurile de securitate cibernetică asociate cu activitățile sale. Un alt exemplu este documentul ENISA "Ghid pentru dezvoltarea unui plan de gestionare a incidentelor de securitate cibernetică". Implementarea acestui ghid poate ajuta Primăria Bistrița să pregătească și să răspundă în mod eficient la incidente de securitate cibernetică, reducând astfel impactul acestora asupra activităților instituției și protejând datele și resursele sale. Prin implementarea recomandărilor ENISA, Primăria Bistrița poate să ia măsuri proactive pentru a-și îmbunătăți nivelul de securitate cibernetică și să se alinieze celor mai bune practici și standard internaționale în domeniul securității cibernetice. Acest lucru poate ajuta la consolidarea credibilității instituției în ochii cetățenilor și la atragerea de noi investiții și resurse în oraș.

Respectarea standardelor internaționale în materie de securitate cibernetică poate fi văzută ca un semnal de angajament al instituției în asigurarea securității datelor și protejarea informațiilor cu caracter personal ale cetățenilor și partenerilor de afaceri. În plus, aceasta poate asigura că Primăria Bistrița este la curent cu ultimele tendințe și tehnologii în domeniul securității cibernetice și poate implementa cele mai bune soluții de securitate pentru a se proteja împotriva atacurilor cibernetice.

Creșterea credibilității instituției în ochii cetățenilor și a altor entități poate fi un factor important în atragerea de noi investiții și resurse în oraș. Companiile și investitorii caută adesea parteneri care au o politică solidă de securitate cibernetică și care își protejează în mod corespunzător datele și informațiile. Prin implementarea unei politici de securitate cibernetică, Primăria Bistrița poate obține încrederea acestor companii și investitori și poate fi văzută ca un partener de încredere în afaceri.

Dezvoltarea și implementarea unor politici interne solide de securitate cibernetică va fi o abordare proactivă pentru a reduce riscul de atacuri cibernetice și pentru a proteja activ resursele și informațiile Primăriei Bistrița. Această abordare poate contribui la economisirea costurilor necesare pentru a aborda astfel de atacuri după ce acestea au avut loc și poate ajuta la menținerea integrității informațiilor și a activelor instituției.

Obiective si rezultate

Obiectivele proiectului sunt urmatoarele:

1. Dezvoltarea unui cadru de politici interne de securitate cibernetica care sa respecte cele mai bune practici si standarde internationale in materie de securitate cibernetica.

Primul obiectiv al proiectului este de a dezvolta un cadru solid de politici interne de securitate cibernetică care să respecte cele mai bune practici și standarde internaționale în domeniu. Acest cadru de politici va include o serie de reguli, proceduri și orientări pentru protejarea activelor și informațiilor Primăriei Bistrița. Politicile vor fi adaptate la nevoile specifice ale instituției și vor fi dezvoltate în urma unei analize atente a riscurilor la care instituția este expusă. Aceste politici vor fi actualizate în mod regulat pentru a reflecta schimbările în mediul de securitate cibernetică și pentru a aborda noile amenințări.

2. Implementarea politicii interne de securitate cibernetica in cadrul tuturor departamentelor si serviciilor Primariei Bistrita.

Cel de-al doilea obiectiv al proiectului este de a implementa politica internă de securitate cibernetică în cadrul tuturor departamentelor și serviciilor Primăriei Bistrița. Aceasta va implica o serie de acțiuni, cum ar fi furnizarea de resurse și instruiri specifice pentru fiecare departament și serviciu, și verificarea aplicării politicii. Fiecare departament și serviciu va fi responsabil de asigurarea faptului că politica este implementată în mod corespunzător și că toți angajații își îndeplinesc responsabilitățile în ceea ce privește securitatea cibernetică.

3. Formarea angajatilor din cadrul Primariei Bistrita cu privire la securitatea cibernetica si la modul in care pot contribui la protejarea activelor si informatiilor Primariei.

Al treilea obiectiv al proiectului este de a forma angajații din cadrul Primăriei Bistrița cu privire la securitatea cibernetică și la modul în care pot contribui la protejarea activelor și informațiilor instituției. Aceasta va implica furnizarea de instruiri și sesiuni de formare adaptate pentru fiecare departament și serviciu, astfel încât angajații să înțeleagă riscurile cibernetice și să poată aplica practici de securitate cibernetică corespunzătoare în activitatea lor zilnică. De asemenea, aceasta va spori gradul de conștientizare a securității cibernetice în cadrul Primăriei Bistrița și va ajuta la dezvoltarea unei culturi de securitate cibernetică.

4. Evaluarea si monitorizarea continua a performantei in domeniul securitatii cibernetice si raportarea de incidente de securitate cibernetica.

Obiectivul 4 al proiectului este evaluarea și monitorizarea continuă a performanței în domeniul securității cibernetice și raportarea incidentelor de securitate cibernetică. Acest obiectiv este important deoarece, chiar și cu o politică solidă de securitate cibernetică, este posibil ca vulnerabilități să apară și să fie exploatate. Prin evaluarea și monitorizarea continuă a performanței, se poate identifica și gestiona eficient aceste vulnerabilități. Evaluarea performanței în domeniul securității cibernetice poate fi realizată prin diferite mijloace, cum ar fi audituri de securitate, testări de penetrare și analize ale vulnerabilităților. Aceste evaluări pot ajuta la identificarea eventualelor probleme de securitate și la dezvoltarea unor soluții adecvate. Monitorizarea continuă a securității cibernetice poate fi realizată prin utilizarea de instrumente de monitorizare a rețelei și a sistemelor de informații. Aceste instrumente pot ajuta la detectarea activităților suspecte sau neautorizate și la prevenirea eventualelor atacuri cibernetice. Raportarea incidentelor de securitate cibernetică este importantă pentru identificarea și gestionarea rapidă a acestora. Aceste rapoarte pot include informații despre natura incidentului, impactul asupra organizației și acțiunile luate pentru a gestiona incidentul. Raportarea incidentelor poate ajuta la prevenirea unor astfel de incidente în

viitor și la dezvoltarea unor soluții adecvate pentru a preveni sau minimiza impactul unor atacuri cibernetice viitoare.

Rezultatele asteptate ale proiectului sunt urmatoarele:

1. O politica interna de securitate cibernetica elaborata in conformitate cu cele mai bune practici si standarde internationale.
2. Implementarea cu succes a politicii interne de securitate cibernetica in cadrul tuturor departamentelor si serviciilor Primariei Bistrita.
3. Angajatii Primariei Bistrita vor fi instruiti si pregatiti cu privire la securitatea cibernetica.
4. Evaluarea continua a performantei in domeniul securitatii cibernetice si raportarea incidentelor de securitate cibernetica vor ajuta la identificarea si abordarea prompta a oricarei probleme legate de securitatea cibernetica.

Rezultatul așteptat numărul 1: Una dintre principalele rezultate ale proiectului este o politică internă de securitate cibernetică elaborată în conformitate cu cele mai bune practici și standarde internaționale. Acest lucru va include un cadru coerent de politici și proceduri care să stabilească standarde clare pentru protejarea datelor și sistemelor informatice. Un astfel de cadru va asigura că toți angajații Primăriei Bistrița înțeleg obligațiile lor cu privire la securitatea cibernetică și își îndeplinesc rolurile în acest sens. Metricile relevante pentru evaluarea acestui rezultat ar putea include nivelul de conformitate cu standardele ISO 27001 sau cu recomandările ENISA privind politica internă de securitate cibernetică, precum și numărul de politici și proceduri stabilite în cadrul cadrelor de securitate cibernetică ale Primăriei Bistrița. Valoarea țintă ar putea fi de 100% conformitate cu standardele și de cel puțin 30 politici și proceduri stabilite în cadrul cadrelor de securitate cibernetică ale Primăriei Bistrița.

Rezultatul așteptat numărul 2: Un alt rezultat cheie al proiectului este implementarea cu succes a politicii interne de securitate cibernetică în cadrul tuturor departamentelor și serviciilor Primăriei Bistrița. Acest lucru va asigura că toți angajații folosesc și respectă politica internă de securitate cibernetică și că sunt luate măsuri adecvate pentru a proteja datele și sistemele informatice ale instituției. Metricile relevante pentru evaluarea acestui rezultat ar putea include nivelul de conformitate cu politica internă de securitate cibernetică și numărul de departamente și servicii ale Primăriei Bistrița care au implementat cu succes politica internă de securitate cibernetică. Valoarea țintă ar putea fi de 100% conformitate cu politica internă de securitate cibernetică și implementarea cu succes a politicii în toate departamentele și serviciile Primăriei Bistrița.

Rezultatul așteptat numărul 3: Un alt rezultat important al proiectului este instruirea și pregătirea angajaților Primăriei Bistrița cu privire la securitatea cibernetică. Acest lucru va include o serie de programe de instruire și formare care să-i ajute pe angajați să înțeleagă riscurile asociate securității cibernetice și să-i învețe cum să evite atacurile cibernetice și să protejeze activelor și informațiilor Primăriei. Metricile relevante pentru evaluarea acestui rezultat ar putea include numărul de angajați care au participat la programele de instruire și formare din total angajați, precum și gradul de înțelegere și aplicare a conceptelor de securitate cibernetică. Un obiectiv important al instruirii și pregătirii angajaților este de a dezvolta o cultură a securității cibernetice în cadrul Primăriei Bistrița. Această cultură ar trebui să încurajeze angajații să fie proactivi în protejarea activelor și informațiilor Primăriei împotriva atacurilor cibernetice și să raporteze incidentele de securitate cibernetică în mod prompt. De asemenea, instruirea și pregătirea angajaților ar trebui să încurajeze colaborarea între departamente și servicii pentru a promova o abordare integrată a securității cibernetice în cadrul Primăriei. Metricile pentru evaluarea acestui rezultat ar putea include numărul de incidente de securitate cibernetică raportate de angajați și gradul de conștientizare a securității cibernetice în rândul angajaților, măsurat prin intermediul sondajelor sau a altor mijloace de evaluare. În plus, numărul de incidente de securitate cibernetică raportate poate fi utilizat pentru a evalua eficacitatea programelor de instruire și formare și pentru a identifica zonele care necesită îmbunătățiri.

Rezultatul așteptat numărul 4: Un alt rezultat important al proiectului este evaluarea continuă a performanței în domeniul securității cibernetice și raportarea incidentelor de securitate cibernetică. Aceasta va permite Primăriei Bistrița să identifice rapid problemele de securitate cibernetică și să le abordeze prompt, astfel încât să se minimizeze impactul acestora asupra organizației și a cetățenilor. Metricile relevante pentru evaluarea acestui rezultat ar putea include frecvența evaluărilor de securitate cibernetică, timpul necesar pentru a remedia problemele identificate, numărul de incidente raportate și timpul necesar pentru a le rezolva. De asemenea, ar putea fi monitorizat nivelul de conformitate cu standardele și regulamentele de securitate cibernetică, precum și numărul de amenințări detectate și rezolvate cu succes.

Planul de implementare

1. Dezvoltarea politicii interne de securitate cibernetica:

- Identificarea celor mai bune practici si standarde internationale in materie de securitate cibernetica
  - Definirea obiectivelor: Stabiliți obiectivele specifice ale proiectului de identificare a celor mai bune practici și standarde internaționale în materie de securitate cibernetică. De exemplu, poate fi vorba de a dezvolta o politică internă de securitate cibernetică sau de a asigura conformitatea cu o anumită normă sau standard internațional.
  - Identificarea surselor de informații: Identificați sursele de informații relevante pentru obiectivele proiectului. Acestea pot include organizații guvernamentale sau non-guvernamentale, organizații de standarde, forumuri de discuții și conferințe de specialitate.
  - Selectarea standardelor relevante: Selectați standardele și normele care sunt relevante pentru obiectivele dvs. De exemplu, ISO/IEC 27001 este un standard internațional pentru managementul securității informațiilor, iar NIST (National Institute of Standards and Technology) oferă un set de ghiduri și instrumente pentru securitatea cibernetică.
  - Evaluarea și analiza standardelor: Analizați și evaluați standardele și normele selectate pentru a înțelege cum acestea se aplică la nevoile și obiectivele dvs. de securitate cibernetică.
  - Compararea standardelor: Comparați standardele selectate pentru a identifica suprapunerile, lacunele și diferențele dintre acestea.
  - Selecția celor mai bune practici: Identificați cele mai bune practici din fiecare standard și normă relevantă, care sunt aplicabile la obiectivele dvs.
- Elaborarea politicii interne de securitate cibernetica, care va include proceduri, reguli, si responsabilitati specifice pentru diferitele departamente si servicii din cadrul Primariei Bistrita
  - Stabilirea echipei de proiect: Desemnați un lider de proiect și o echipă de membri din diferite departamente și servicii ai Primăriei Bistrița, care să colaboreze pentru dezvoltarea politicii de securitate cibernetică.
  - Identificarea riscurilor și amenințărilor: Analizați sistemul informatic al Primăriei și identificați riscurile și amenințările de securitate cibernetică relevante, inclusiv atacurile cibernetice, malware-ul, phishing-ul și ingineria socială.
  - Stabilirea obiectivelor: Stabiliți obiectivele politicii de securitate cibernetică, cum ar fi protejarea sistemului informatic al Primăriei, a datelor și informațiilor confidențiale, asigurarea conformității cu reglementările și standardele aplicabile, și creșterea gradului de conștientizare și educare a angajaților în ceea ce privește securitatea cibernetică.
  - Elaborarea politicilor și procedurilor: Dezvoltați politicile și procedurile specifice care să abordeze riscurile și amenințările identificate, inclusiv politici privind parolele și autentificarea, politici privind utilizarea internetului și a rețelelor sociale, politici privind utilizarea dispozitivelor mobile și politici privind securitatea informațiilor.
  - Identificarea responsabilităților: Identificați rolurile și responsabilitățile specifice ale diferitelor departamente și servicii în implementarea politicilor și procedurilor de securitate cibernetică.
  - Elaborarea planurilor de acțiune: Dezvoltați planuri de acțiune specifice pentru a pune în aplicare politicile și procedurile de securitate cibernetică, inclusiv planuri de gestionare a incidentelor și planuri de testare a securității sistemului informatic.
- Revizuirea si aprobarea politicii de catre consiliul local
  - Finalizarea politicilor și procedurilor: Finalizați politicile și procedurile de securitate cibernetică pentru Primăria Bistrița.
  - Prezentarea politicilor și procedurilor: Prezentați politicile și procedurile de securitate cibernetică membrilor Consiliului Local. Furnizați-le informații detaliate despre necesitatea politicilor și procedurilor de securitate cibernetică și despre beneficiile pe care le aduc.
  - Discutarea politicilor și procedurilor: Deschideți o discuție cu membrii Consiliului Local despre politicile și procedurile de securitate cibernetică. Răspundeți la întrebările și preocupările acestora și încurajați feedback-ul lor.

- Evaluarea politicilor și procedurilor: Evaluarea politicilor și procedurilor de securitate cibernetică în contextul comentariilor și feedback-ului primite de la membrii Consiliului Local.
- Revisuirea politicilor și procedurilor: Revizuiți politicile și procedurile de securitate cibernetică pentru a integra feedback-ul și comentariile primite de la membrii Consiliului Local.
- Prezentarea politicii și procedurilor revizuite: Prezentați versiunea revizuită a politicilor și procedurilor de securitate cibernetică membrilor Consiliului Local. Discutați modificările făcute și justificați-le.
- Dezbaterea politicii și procedurilor revizuite: Deschideți o nouă discuție cu membrii Consiliului Local despre politica și procedurile de securitate cibernetică revizuite. Răspundeți la întrebări și preocupări și încurajați feedback-ul lor.
- Finalizarea politicii și procedurilor: Finalizați versiunea finală a politicilor și procedurilor de securitate cibernetică în funcție de feedback-ul primit de la membrii Consiliului Local.
- Aprobarea politicilor și procedurilor: Adunați votul Consiliului Local pentru a aproba politicile și procedurile de securitate cibernetică revizuite.
- Comunicarea politicilor și procedurilor: Comunicați politicile și procedurile de securitate cibernetică aprobate membrilor Primăriei Bistrița, asigurați-vă că acestea sunt implementate și monitorizați respectarea acestora.

2. Implementarea politicii interne de securitate cibernetica:

- Formarea tuturor angajatilor din cadrul Primariei Bistrita privind politica interna de securitate cibernetica, inclusiv identificarea si abordarea riscurilor de securitate cibernetica
  - Identificarea necesității formării: Identificați necesitatea formării tuturor angajaților din cadrul Primăriei Bistrița cu privire la politica internă de securitate cibernetică. Asigurați-vă că toți angajații înțeleg importanța securității cibernetice și riscurile asociate.
  - Planificarea formării: Planificați o serie de sesiuni de formare pentru toți angajații Primăriei Bistrița pentru a acoperi politicile și procedurile de securitate cibernetică și identificarea și abordarea riscurilor de securitate cibernetică.
  - Identificarea conținutului formării: Identificați conținutul pentru sesiunile de formare, care trebuie să acopere aspecte precum utilizarea responsabilă a parolelor, identificarea phishing-ului și a altor forme de atac cibernetic, securitatea rețelelor și a dispozitivelor mobile, și politici și proceduri interne specifice de securitate cibernetică.
  - Identificarea resurselor de formare: Identificați resursele necesare pentru a livra formarea, cum ar fi prezentări, materiale de formare și ghiduri.
  - Planificarea logisticii: Planificați logistica pentru formare, inclusiv programarea sesiunilor de formare și organizarea spațiului de formare.
  - Realizarea sesiunilor de formare: Livrați sesiunile de formare pentru toți angajații Primăriei Bistrița. Asigurați-vă că toți angajații sunt prezenți la sesiunile de formare și înțeleg conținutul și importanța acestuia.
  - Evaluarea formării: Efectuați o evaluare a formării pentru a măsura gradul de înțelegere a angajaților cu privire la politicile și procedurile de securitate cibernetică și pentru a identifica eventuale lacune în formare.
  - Îmbunătățirea formării: Îmbunătățiți formarea în funcție de feedback-ul primit de la angajați și de evaluarea formării.
- Implementarea politicii in toate departamentele si serviciile Primariei Bistrita, inclusiv monitorizarea si verificarea respectarii regulilor si procedurilor de securitate cibernetica
  - Identificarea responsabililor: Identificați un responsabil pentru implementarea politicii de securitate cibernetică în fiecare departament sau serviciu. Atribuiți-le sarcina de a se asigura că toți angajații respectă politicile și procedurile de securitate cibernetică.
  - Formarea responsabililor: Formați responsabilii pentru implementarea politicilor și procedurilor de securitate cibernetică. Asigurați-vă că aceștia înțeleg politicile și procedurile relevante și cum să le aplice în practică.

- Comunicarea politicilor și procedurilor: Comunicați politicile și procedurile de securitate cibernetică la toți angajații Primăriei Bistrița și asigurați-vă că aceștia le înțeleg și le respectă. Asigurați-vă că toți angajații sunt instruiți cu privire la riscurile și amenințările de securitate cibernetică și că sunt instruiți cu privire la politicile și procedurile relevante.
- Identificarea necesității modificărilor: Identificați eventualele modificări ale politicilor și procedurilor de securitate cibernetică care trebuie implementate în departamentele și serviciile relevante.
- Planificarea implementării: Planificați implementarea modificărilor necesare în politicile și procedurile de securitate cibernetică.
- Implementarea politicilor și procedurilor: Implementați politicile și procedurile de securitate cibernetică în toate departamentele și serviciile Primăriei Bistrița. Asigurați-vă că toți angajații respectă politicile și procedurile relevante.
- Monitorizarea respectării politicii: Monitorizați respectarea politicilor și procedurilor de securitate cibernetică în toate departamentele și serviciile Primăriei Bistrița. Efectuați audituri periodice pentru a vă asigura că politicile și procedurile sunt respectate în mod adecvat.
- Identificarea problemelor: Identificați problemele de securitate cibernetică și soluțiile necesare pentru a le gestiona.
- Evaluarea și îmbunătățirea continuă: Evaluați și îmbunătățiți politicile și procedurile de securitate cibernetică în funcție de feedback-ul și rezultatele obținute.
- Comunicarea rezultatelor: Comunicați periodic rezultatele implementării politicii de securitate cibernetică și îmbunătățirile realizate la conducerea Primăriei și la toți angajații relevanți.

3. Evaluarea si monitorizarea continua a performantei in domeniul securitatii cibernetice:

- Implementarea unui sistem de raportare a incidentelor de securitate cibernetica
  - Identificarea necesității sistemului de raportare: Identificați necesitatea implementării unui sistem de raportare a incidentelor de securitate cibernetică în cadrul Primăriei Bistrița. Asigurați-vă că există o înțelegere clară a importanței raportării incidentelor de securitate cibernetică și a beneficiilor pe care le aduce.
  - Identificarea responsabililor: Identificați un responsabil pentru implementarea și gestionarea sistemului de raportare a incidentelor de securitate cibernetică. Atribuiți-le sarcina de a dezvolta și implementa sistemul de raportare.
  - Definirea tipurilor de incidente: Definiți tipurile de incidente de securitate cibernetică care trebuie raportate în cadrul sistemului de raportare. Asigurați-vă că toate incidentele importante sunt acoperite și că există un proces clar de raportare a acestora.
  - Dezvoltarea sistemului de raportare: Dezvoltați sistemul de raportare a incidentelor de securitate cibernetică. Asigurați-vă că sistemul este ușor de utilizat și că poate fi accesat de toți angajații relevanți.
  - Testarea sistemului: Testați sistemul de raportare a incidentelor de securitate cibernetică pentru a vă asigura că funcționează în mod adecvat și că poate fi utilizat în situații reale.
  - Implementarea sistemului: Implementați sistemul de raportare a incidentelor de securitate cibernetică în cadrul Primăriei Bistrița. Asigurați-vă că toți angajații relevanți sunt instruiți cu privire la utilizarea sistemului de raportare.
  - Monitorizarea sistemului: Monitorizați utilizarea și eficacitatea sistemului de raportare a incidentelor de securitate cibernetică. Efectuați audituri periodice pentru a vă asigura că sistemul funcționează în mod adecvat și că incidentele sunt raportate și gestionate în mod eficient.
  - Evaluarea și îmbunătățirea continuă: Evaluați și îmbunătățiți sistemul de raportare a incidentelor de securitate cibernetică în funcție de feedback-ul și rezultatele obținute. Asigurați-vă că toți angajații sunt instruiți cu privire la modificările aduse sistemului.
  - Comunicarea incidentelor: Comunicați incidentele de securitate cibernetică relevante conducerii Primăriei și altor angajați relevanți în timp util. Asigurați-vă că există o

înțelegere clară a procesului de raportare a incidentelor și că toți angajații sunt instruiți cu privire la acesta.

- Monitorizarea continua a performantei in domeniul securitatii cibernetice si a masurilor de protectie
  - Identificarea necesității monitorizării continue: Identificați necesitatea monitorizării continue a performanței în domeniul securității cibernetice și a măsurilor de protecție. Asigurați-vă că există o înțelegere clară a importanței monitorizării continue și a beneficiilor pe care le aduce.
  - Identificarea responsabililor: Identificați responsabilii pentru monitorizarea performanței în domeniul securității cibernetice și a măsurilor de protecție. Atribuiți-le sarcina de a dezvolta și implementa sistemul de monitorizare.
  - Definirea indicatorilor cheie de performanță (KPIs): Definiți indicatorii cheie de performanță (KPIs) relevanți în domeniul securității cibernetice și a măsurilor de protecție. Asigurați-vă că KPIs-urile acoperă toate aspectele importante și că sunt măsurabile.
  - Dezvoltarea sistemului de monitorizare: Dezvoltați sistemul de monitorizare a performanței în domeniul securității cibernetice și a măsurilor de protecție. Asigurați-vă că sistemul este capabil să colecteze și să stocheze datele relevante și să genereze rapoarte în timp util.
  - Implementarea sistemului de monitorizare: Implementați sistemul de monitorizare a performanței în domeniul securității cibernetice și a măsurilor de protecție în cadrul Primăriei Bistrița. Asigurați-vă că toți angajații relevanți sunt instruiți cu privire la utilizarea sistemului de monitorizare.
  - Monitorizarea performanței: Monitorizați performanța în domeniul securității cibernetice și a măsurilor de protecție utilizând KPIs-urile definite. Asigurați-vă că toate datele relevante sunt colectate și analizate în mod regulat și că există un proces clar de raportare a rezultatelor.
  - Evaluarea și îmbunătățirea continuă: Evaluați și îmbunătățiți sistemul de monitorizare a performanței în funcție de feedback-ul și rezultatele obținute. Asigurați-vă că toți angajații sunt instruiți cu privire la modificările aduse sistemului.
  - Comunicarea rezultatelor: Comunicați periodic rezultatele monitorizării performanței în domeniul securității cibernetice și a măsurilor de protecție la conducerea Primăriei și la toți angajații relevanți. Asigurați-vă că există o înțelegere clară a rezultatelor și a acțiunilor care trebuie luate în funcție de acestea.
  - Identificarea problemelor: Identificați problemele de performanță în domeniul securității cibernetice și a măsurilor de protecție și soluțiile necesare pentru a le gestiona. Asigurați-vă că există un proces clar pentru raportarea problemelor și că acestea sunt gestionate în timp util.
  - Actualizarea politicilor și procedurilor: Actualizați politicile și procedurile de securitate cibernetică și a măsurilor de protecție în funcție de feedback-ul și rezultatele obținute din sistemul de monitorizare a performanței. Asigurați-vă că toți angajații sunt instruiți cu privire la modificările aduse politicilor și procedurilor.
  - Evaluarea periodică a sistemului de monitorizare: Efectuați o evaluare periodică a sistemului de monitorizare a performanței în domeniul securității cibernetice și a măsurilor de protecție pentru a vă asigura că este eficient și că îndeplinește nevoile Primăriei Bistrița.
  - Comunicarea rezultatelor către terți: Comunicați periodic rezultatele monitorizării performanței în domeniul securității cibernetice și a măsurilor de protecție către terți relevanți, cum ar fi furnizorii de servicii IT sau alte organizații cu care Primăria Bistrița colaborează. Asigurați-vă că există o înțelegere clară a rezultatelor și a acțiunilor care trebuie luate în funcție de acestea.
- Evaluarea regulata a politicii interne de securitate cibernetica si a procedurilor aferente
  - Identificarea necesității evaluării regulate: Identificați necesitatea evaluării regulate a politicii interne de securitate cibernetică și a procedurilor aferente. Asigurați-vă că există o înțelegere clară a importanței evaluării regulate și a beneficiilor pe care le aduce.
  - Identificarea responsabililor: Identificați responsabilii pentru evaluarea regulată a politicii interne de securitate cibernetică și a procedurilor aferente. Atribuiți-le sarcina de a dezvolta și implementa procesul de evaluare.

- Stabilirea unui cadru de evaluare: Stabiliți un cadru de evaluare care să cuprindă criterii relevante și măsurabile pentru evaluarea politicii interne de securitate cibernetică și a procedurilor aferente. Asigurați-vă că toate aspectele importante sunt acoperite și că criteriile sunt relevante pentru Primăria Bistrița.
- Implementarea procesului de evaluare: Implementați procesul de evaluare a politicii interne de securitate cibernetică și a procedurilor aferente în cadrul Primăriei Bistrița. Asigurați-vă că toți angajații relevanți sunt instruiți cu privire la procesul de evaluare și că există un proces clar de raportare a rezultatelor.
- Evaluarea politicilor și procedurilor: Efectuați evaluarea politicilor și procedurilor de securitate cibernetică în conformitate cu cadru de evaluare stabilit. Asigurați-vă că toate politicile și procedurile sunt conforme cu cele mai bune practici și standardele internaționale în materie de securitate cibernetică și că sunt relevante pentru Primăria Bistrița.
- Identificarea problemelor: Identificați problemele și deficiențele din politica internă de securitate cibernetică și a procedurilor aferente și soluțiile necesare pentru a le gestiona. Asigurați-vă că există un proces clar pentru raportarea problemelor și că acestea sunt gestionate în timp util.
- Actualizarea politicilor și procedurilor: Actualizați politicile și procedurile de securitate cibernetică în funcție de feedback-ul și rezultatele obținute din procesul de evaluare. Asigurați-vă că toți angajații sunt instruiți cu privire la modificările aduse politicilor și procedurilor.
- Comunicarea rezultatelor: Comunicați periodic rezultatele evaluării politicii interne de securitate cibernetică și a procedurilor aferente către conducerea Primăriei și la toți angajații relevanți. Asigurați-vă că există o înțelegere clară a rezultatelor și a acțiunilor care trebuie luate în funcție de acestea.
- Identificarea nevoilor de formare suplimentară: Identificați nevoile de formare suplimentară în domeniul securității cibernetice și a măsurilor de protecție identificate în timpul procesului de evaluare. Asigurați-vă că angajații sunt instruiți și pregătiți să îndeplinească în mod eficient sarcinile legate de securitatea cibernetică.
- Evaluarea periodică a procesului de evaluare: Efectuați o evaluare periodică a procesului de evaluare a politicii interne de securitate cibernetică și a procedurilor aferente pentru a vă asigura că este eficient și că îndeplinește nevoile Primăriei Bistrița.
- Actualizarea și îmbunătățirea continuă: Actualizați și îmbunătățiți procesul de evaluare a politicii interne de securitate cibernetică și a procedurilor aferente în funcție de feedback-ul și rezultatele obținute. Asigurați-vă că toți angajații sunt instruiți cu privire la modificările aduse procesului de evaluare.

Sustenabilitate si impact

Sustenabilitatea și impactul politicilor de securitate cibernetică sunt cruciale pentru protejarea datelor și resurselor organizației, precum și pentru menținerea unui mediu de lucru sigur și protejat împotriva amenințărilor cibernetice. Implementarea unei politici interne de securitate cibernetică la Primăria Bistrița va avea un impact semnificativ asupra modului în care organizația abordează problemele de securitate cibernetică și protejează informațiile și resursele sale.

În primul rând, implementarea unei politici interne de securitate cibernetică va ajuta la crearea unui cadru solid pentru protejarea informațiilor și resurselor Primăriei Bistrița împotriva amenințărilor cibernetice. Politica va defini și va promova cele mai bune practici și standarde internaționale în materie de securitate cibernetică, precum și reguli și proceduri specifice pentru departamentele și serviciile din cadrul organizației. În acest fel, politica va ajuta la reducerea vulnerabilităților și la creșterea securității cibernetice în organizație.

În al doilea rând, formarea angajaților cu privire la securitatea cibernetică va contribui la dezvoltarea unei culturi a securității cibernetice în cadrul Primăriei Bistrița. Angajații sunt primul și cel mai important nivel de apărare împotriva amenințărilor cibernetice și trebuie să fie conștienți de riscurile și amenințările cibernetice și de importanța protejării datelor și resurselor organizației. Prin urmare, formarea angajaților cu privire la securitatea cibernetică va ajuta la îmbunătățirea capacității organizației de a detecta și a preveni incidente de securitate cibernetică.

În al treilea rând, implementarea unei politici interne de securitate cibernetică va ajuta la protejarea resurselor Primăriei Bistrița și la menținerea unui mediu de lucru sigur. Securitatea cibernetică este esențială pentru protejarea informațiilor și a resurselor organizației împotriva atacurilor cibernetice și a pierderii datelor. În plus, implementarea unei politici interne de securitate cibernetică poate ajuta la evitarea posibilelor amenzi și a costurilor asociate cu recuperarea datelor pierdute sau afectate în urma unui atac cibernetic.

Durata și bugetul proiectului "Politicile interne în privința securității cibernetice" depind de mai mulți factori, cum ar fi dimensiunea și complexitatea Primăriei Bistrița și nivelul de pregătire a angajaților în domeniul securității cibernetice. În general, se estimează că acest proiect va avea o durată de 18 luni.

Bugetul proiectului va fi alocat pentru următoarele activități:

- Dezvoltarea politicii interne de securitate cibernetica, care va include identificarea celor mai bune practici și standarde internaționale în materie de securitate cibernetica, elaborarea politicii și revizuirea și aprobarea acesteia de către consiliul local.
- Implementarea politicii interne de securitate cibernetica, inclusiv formarea tuturor angajaților din cadrul Primariei Bistrita privind politica interna de securitate cibernetica, implementarea politicii în toate departamentele și serviciile Primariei Bistrita și monitorizarea continua a respectarii regulilor si procedurilor de securitate cibernetica.
- Evaluarea si monitorizarea continua a performantei in domeniul securitatii cibernetice, prin implementarea unui sistem de raportare a incidentelor de securitate cibernetica, monitorizarea continua a performantei in domeniul securitatii cibernetice si a masurilor de protectie si evaluarea regulata a politicii interne de securitate cibernetica si a procedurilor aferente.

Estimarea bugetului pentru implementarea proiectului poate varia în funcție de numărul de angajați implicați în procesul de formare și instruire, numărul de departamente și servicii care trebuie să implementeze politica internă de securitate cibernetică și de costurile hardware și software necesare pentru a asigura securitatea informațiilor și resurselor instituției. În general, costurile aferente implementării politicii interne de securitate cibernetică vor fi o investiție în viitorul Primăriei Bistrița, având în vedere riscurile tot mai mari de atacuri cibernetice în prezent.

Având în vedere numărul de angajați din Primăria Bistrița și cele 6 instituții subordonate, se poate estima un buget în intervalul de câteva zeci de mii până la sute de mii de euro pentru implementarea acestui proiect, în funcție de complexitatea care se dorește.

Se pot estima următoarele costuri aproximative pentru implementarea politicilor de securitate cibernetică în cadrul Primăriei Bistrița, având în vedere numărul de angajați din instituție și cele 6 instituții subordonate:

- Formarea angajaților privind securitatea cibernetică: 10.000 - 15.000 EUR (inclusiv costurile de instruire, materiale de formare, etc.)
- Achiziționarea de tehnologie și echipament specializat: 50.000 - 100.000 EUR (inclusiv echipamente de protecție, software de securitate, hardware de rețea securizată, etc.)
- Implementarea măsurilor de securitate: 20.000 - 40.000 EUR (inclusiv costurile de configurare, testare, implementare și monitorizare a soluțiilor de securitate cibernetică)
- Monitorizarea și evaluarea performanței în domeniul securității cibernetice: 10.000 - 15.000 EUR (inclusiv costurile pentru achiziționarea de software specializat, servicii de monitorizare și evaluare, etc.)
- Proiectarea politicilor de securitate cibernetică: Costul elaborării a 47 de politici interne de securitate cibernetică depinde de mulți factori, cum ar fi nivelul de detaliere necesar, timpul necesar pentru cercetarea și dezvoltarea fiecărei politici și necesitățile specifice ale Primăriei Bistrița. În general, costurile pentru a elabora o singură politică internă de securitate cibernetică variază între 500 și 5000 de EUR, în funcție de complexitatea politicii. La o medie de 1000 EUR, rezultă aproximativ 47.000 EUR pentru elaborarea acestor politici.

În total, costurile pentru implementarea politicilor de securitate cibernetică în cadrul Primăriei Bistrița ar putea fi estimate în intervalul de 140.000 - 210.000 EUR. Este important de reținut că aceste costuri sunt doar estimate.

Scenariile de implementare depind de resursele financiare, umane și tehnologice disponibile la Primaria Bistrita. Iată trei posibile scenarii de implementare ale politicii interne de securitate cibernetică, împreună cu o estimare a bugetului pentru fiecare scenariu:

Scenariul 1: Implementare interna În acest scenariu, Primaria Bistrita ar putea alege să implementeze politica interna de securitate cibernetică cu resurse interne. Ar putea fi desemnat un coordonator al proiectului care să dezvolte politica și să coordoneze implementarea. De asemenea, ar putea fi necesară formarea unei echipe interne pentru implementarea politicii și evaluarea continuă a performanțelor în domeniul securității cibernetice. Bugetul estimativ pentru acest scenariu ar fi între 50.000 - 70.000 de euro, pentru formare și resurse interne.

Scenariul 2: Colaborare cu un consultant În acest scenariu, Primaria Bistrita ar putea alege să colaboreze cu un consultant pentru a dezvolta și implementa politica internă de securitate cibernetică. Consultantul ar putea fi responsabil de dezvoltarea politicilor și procedurilor, formarea angajaților, monitorizarea performanței și evaluarea continuă. Bugetul estimativ pentru acest scenariu ar fi între 90.000 - 120.000 de euro pentru costurile de consultanță și de formare a angajaților.

Scenariul 3: Externalizarea implementării În acest scenariu, Primaria Bistrita ar putea externaliza complet implementarea politicii interne de securitate cibernetică către o companie specializată. Aceasta ar fi responsabilă de dezvoltarea politicilor și procedurilor, formarea angajaților, monitorizarea performanței și evaluarea continuă. Bugetul estimativ pentru acest scenariu ar fi între 140.000 - 210.000 de euro pentru costurile de externalizare a implementării.

Scenariul 1 - Implementarea politicii interne de securitate cibernetica de catre personalul existent al Primariei Bistrita:

Plusuri:

- Costurile de formare vor fi reduse deoarece nu va fi necesara angajarea unui consultant extern.
- Angajatii existenti vor fi mai familiarizati cu procesele si procedurile interne ale organizatiei.
- S-ar putea crea o cultura a securitatii cibernetice in interiorul organizatiei, deoarece personalul va fi implicat in procesul de elaborare a politicii.

Minusuri:

- Este posibil ca personalul existent sa nu aiba cunostintele sau experienta necesara pentru a dezvolta si implementa politici eficiente de securitate cibernetica.
- Angajatii existenti ar putea fi prea prinsi cu responsabilitatile lor curente pentru a avea timpul si resursele necesare pentru a se concentra pe acest proiect.

Scenariul 2 - Implementarea politicii interne de securitate cibernetica prin angajarea unui consultant extern:

Plusuri:

- Implicarea unui consultant extern specializat în securitatea cibernetică poate asigura un nivel ridicat de experiență și cunoștințe în elaborarea politicilor interne.
- Având un consultant extern care lucrează exclusiv la proiectul de securitate cibernetică, este posibil să se realizeze o dezvoltare și implementare mai rapidă a politicilor.
- În cazul în care consultantul are experiență în munca cu instituții publice, aceasta poate facilita comunicarea și cooperarea între consultant și personalul Primăriei Bistrița.

Minusuri:

- Costul ridicat poate fi o problemă majoră pentru Primăria Bistrița, în special dacă bugetul proiectului este limitat.
- În cazul în care consultantul nu este local, există posibilitatea ca acesta să nu fie la fel de familiarizat cu contextul specific și cu politicile și practicile locale.
- În funcție de modul în care este elaborat contractul cu consultantul, există posibilitatea ca Primăria Bistrița să nu aibă control total asupra procesului de dezvoltare și implementare a politicilor.

Scenariul 3 - Implementarea politicii interne de securitate cibernetica prin crearea unei echipe de proiect interna:

Plusuri:

- Utilizarea unei echipe mixte de membri din cadrul Primăriei Bistrița și a unui consultant extern poate asigura un nivel ridicat de expertiză și experiență în dezvoltarea politicilor interne.
- Folosirea personalului existent poate reduce costurile și poate asigura o mai bună înțelegere și acceptare a politicilor de către angajați.
- Colaborarea între echipa internă și consultant poate duce la o dezvoltare mai rapidă a politicilor și la o implementare mai eficientă.

Minusuri:

- Există riscul ca personalul din cadrul Primăriei Bistrița să nu aibă suficientă experiență în securitatea cibernetică, ceea ce poate duce la elaborarea politicilor neadecvate sau incomplete.
- Coordonarea și comunicarea între echipele interne și consultantul extern poate fi dificilă, ceea ce poate duce la întârzieri în implementarea politicilor.
- Dacă personalul din cadrul Primăriei Bistrița este supraîncărcat cu munca curentă, implicarea lor în acest proiect poate fi dificilă sau chiar imposibilă.

Calculul ROI (Return on Investment) este dat de formula:

ROI = (Profit - Cost) / Cost x 100

Pentru a estima pierderile aferente unui atac cibernetic major, este necesar sa se ia in considerare o serie de factori, cum ar fi:

- Gravitatea atacului
- Dimensiunea si complexitatea sistemului informatizat
- Tipul de date afectate (sensibile sau nesensibile)
- Costul de recuperare a datelor si resurselor pierdute sau afectate
- Costul de remediere a problemelor de securitate aparute ca urmare a atacului

Dupa ce s-au estimat pierderile aferente unui atac cibernetic major, se poate calcula ROI in cazul implementarii proiectului de politici interne de securitate cibernetica.

Presupunand ca pierderile estimate sunt de 1 milion de euro, iar costul total al proiectului este de 300.000 de euro, inclusiv costul consultantei si al formarii angajatilor, ROI-ul ar fi:

ROI = (1.000.000 - 200.000) / 200.000 x 100 = 400%

Adica, pentru fiecare euro investit in proiectul de politici interne de securitate cibernetica, se asteapta un beneficiu de 4 euro.

Pentru a realiza o evaluare de risc și probabilități al unui atac cibernetic major in urmatorii 6 ani, trebuie să fie urmate următoarele etape:

1. Identificați activitățile și informațiile sensibile: În primul rând, trebuie să identificați activitățile și informațiile sensibile pe care Primaria Bistrita le deține și le gestioneza. Acestea pot include date cu caracter personal ale angajaților și cetățenilor, informații financiare, informații referitoare la contracte sau alte informații confidențiale.
2. Identificați amenințările: În continuare, trebuie să identificați amenințările la adresa acestor activități și informații. Acestea pot include atacuri cibernetice, dezastre naturale sau alte tipuri de incidente care pot afecta securitatea datelor și resurselor.
3. Identificați vulnerabilitățile: După ce ați identificat amenințările, trebuie să identificați și vulnerabilitățile existente în sistemul de securitate cibernetică al Primariei Bistrita. Acestea pot include lacune în politici și proceduri, sisteme și software neactualizate sau alte probleme legate de securitatea cibernetică.
4. Evaluați riscurile: Pe baza informațiilor colectate în primele trei etape, trebuie să evaluați riscurile. Acest lucru implică determinarea probabilității ca amenințările identificate să se materializeze și impactul pe care îl vor avea asupra activităților și informațiilor sensibile ale Primariei Bistrita.

5. Prioritizați riscurile: Pe baza evaluării riscurilor, trebuie să prioritizați riscurile în funcție de impactul lor și probabilitatea de a se materializa. Acestea ar trebui să fie prioritizate în ordine descrescătoare a riscului.
6. Identificați măsurile de protecție: Pe baza prioritizării riscurilor, trebuie să identificați măsurile de protecție care ar putea fi luate pentru a minimiza riscurile identificate. Aceste măsuri pot include politici și proceduri noi, actualizări software, formare a angajaților și implementarea unor soluții de securitate cibernetică.
7. Evaluați și monitorizați riscurile: În final, trebuie să evaluați și să monitorizați riscurile în mod regulat pentru a asigura că măsurile de protecție sunt eficiente și pentru a identifica noi riscuri care pot apărea în timp.

Deși este aproape imposibil să calculam ROI sau NPV pentru proiectele de securitate cibernetică, există o serie de beneficii financiare indirecte care pot fi evaluate:

1. Reducerea costurilor de remediere și recuperare: Investițiile în securitate cibernetică pot reduce riscul de a suferi pierderi financiare semnificative în urma unui atac cibernetic. Aceste pierderi pot include costurile de remediere și recuperare, costurile de reputație și pierderea veniturilor. Prin investirea în soluții de securitate cibernetică, primăria poate minimiza aceste costuri, ceea ce poate duce la economii semnificative pe termen lung.
2. Protejarea datelor și informațiilor sensibile: Protejarea datelor și informațiilor sensibile ale primăriei poate ajuta la prevenirea încălcării legilor și reglementărilor referitoare la confidențialitatea datelor. În caz contrar, există riscul de amenzi semnificative și costuri de litigiu.
3. Reducerea costurilor de asigurare: Companiile de asigurare pot percepe prime mai mici dacă primăria implementează soluții de securitate cibernetică și politici bune de securitate a datelor. Aceste economii pot fi semnificative pe termen lung.
4. Creșterea încrederii publice: Investițiile în securitate cibernetică pot ajuta la consolidarea încrederii publicului în capacitatea primăriei de a proteja datele și informațiile sensibile ale cetățenilor. Această încredere poate duce la o creștere a relațiilor cu cetățenii.

Anexe

Lista politicilor interne de securitate care ar trebui acoperite prin proiect

1. Politica privind parola de acces: Această politică ar trebui să includă cerințe cu privire la complexitatea parolelor, frecvența schimbării parolelor și utilizarea autentificării cu doi factori.
2. Politica privind accesul la rețea și la sistem: Această politică ar trebui să stabilească cine are acces la rețea și la sistemele organizației, precum și să specifice cerințe privind autentificarea și autorizarea utilizatorilor.
3. Politica privind actualizările software: Această politică ar trebui să specifice cerințe privind actualizările software pentru a se asigura că toate sistemele sunt la zi și au cele mai recente patch-uri de securitate.
4. Politica privind utilizarea dispozitivelor personale: Această politică ar trebui să stabilească cerințe privind utilizarea dispozitivelor personale în cadrul organizației, cum ar fi conectarea la rețelele organizației sau utilizarea acestora pentru stocarea datelor organizației.
5. Politica privind utilizarea e-mailului și a internetului: Această politică ar trebui să stabilească reguli și cerințe privind utilizarea e-mailului și a internetului, cum ar fi interzicerea descărcării de fișiere necunoscute sau accesarea de site-uri web nesigure. Această politică ar mai trebui să stabilească cerințe privind utilizarea adreselor de e-mail instituționale, restricționarea trimiterea și primirea de atașamente și instruirea angajaților cu privire la amenințările cibernetice prin intermediul e-mailului.
6. Politica privind protecția și gestionarea datelor și a informațiilor sensibile: Această politică ar trebui să stabilească reguli și proceduri pentru gestionarea datelor și informațiilor sensibile ale organizației, cum ar fi criptarea datelor și restricționarea accesului la informațiile sensibile. Scopul acestei politici este de a proteja prelucrarea și gestionarea datelor personale. Această politică garantează că datele terților sunt colectate, utilizate, partajate, stocate, transportate și trimise în siguranță, pentru a utiliza datele din motive necesare și definite. De asemenea stabilește comportamentul anticipat al angajaților atunci când au de-a face cu un astfel de material. Mai mult decât atât, această politică descrie modul în care întreprinderile ar trebui să gestioneze datele și sumele de consum conștientizarea utilizatorilor pentru a preveni pierderea datelor. Pentru că securitatea datelor este una dintre cele mai importante elemente care afectează reputația, în funcție de tipul de date și nivelul de sensibilitate, fiecare organizație ar trebui să clasifice datele care trebuie să fie monitorizate.
7. Politica de păstrare a datelor: Această politică specifică ce date trebuie păstrate, cât timp ar trebui păstrate și în ce format ar trebui să fie stocat. Scopul acestei politici este de a proteja informațiile vitale prin stocarea acestuia în copii de rezervă de date criptate pentru o anumită perioadă de timp. În plus, asta politica permite arhivarea frecventă pentru a permite personalului din cadrul organizației să facă cu ușurință accesați și ștergeți orice fișiere care nu mai sunt necesare, precum și cheia de criptare care criptează datele. În consecință, Legea privind păstrarea datelor din SUA permite numai serviciul de internet furnizorii să stocheze date timp de doi ani. În timp ce unele instituții au voie să stocheze astfel de date în conformitate cu Legea privind confidențialitatea și responsabilitatea informațiilor despre sănătate, altele nu sunt.
8. Politica privind securitatea fizică: Această politică ar trebui să stabilească reguli și proceduri pentru protejarea echipamentelor și a sistemelor organizației, cum ar fi utilizarea sistemelor de supraveghere și a măsurilor de control al accesului.
9. Politica privind backup-ul datelor: Această politică ar trebui să specifice cerințe privind backup-ul datelor, cum ar fi frecvența backup-ului și locația de stocare a datelor.
10. Politica privind gestionarea incidentelor de securitate cibernetică: Această politică ar trebui să stabilească proceduri pentru gestionarea incidentelor de securitate cibernetică, cum ar fi raportarea incidentelor și evaluarea impactului acestora.
11. Politica privind securitatea informațiilor: Această politică ar trebui să stabilească reguli și cerințe privind securitatea informațiilor organizației, cum ar fi criptarea datelor și controlul accesului la informațiile sensibile.

12. Politica privind accesul fizic: Această politică ar trebui să stabilească reguli și cerințe privind accesul fizic la echipamente și sisteme organizaționale, cum ar fi utilizarea de chei sau carduri de acces, înregistrarea accesului și limitarea accesului la anumite zone.
13. Politica privind utilizarea aplicațiilor terțe: Această politică ar trebui să stabilească cerințe privind utilizarea de aplicații terțe, cum ar fi cerințele de securitate ale aplicațiilor și monitorizarea aplicațiilor pentru a preveni încălcarea politicilor organizației.
14. Politica privind gestionarea dispozitivelor mobile: Această politică ar trebui să stabilească reguli și cerințe privind utilizarea dispozitivelor mobile în cadrul organizației, cum ar fi protejarea datelor, criptarea și blocarea dispozitivelor pierdute sau furate.
15. Politica privind securitatea socială: Această politică ar trebui să stabilească reguli și cerințe privind securitatea socială, cum ar fi instruirea angajaților cu privire la amenințările cibernetice prin intermediul mesajelor de tip phishing sau scamming.
16. Politica privind gestionarea parolelor: Această politică ar trebui să stabilească reguli și cerințe privind instruirea angajaților privind bunele practici pentru gestionarea parolelor și monitorizarea parolelor pentru a preveni încălcarea politicilor organizației.
17. Politica privind criptarea datelor: Această politică ar trebui să stabilească cerințe privind utilizarea criptării datelor pentru a proteja datele sensibile ale organizației.
18. Politica privind actualizările de securitate: Această politică ar trebui să stabilească cerințe privind instalarea promptă a actualizărilor de securitate și a patch-urilor pentru a remedia vulnerabilitățile de securitate.
19. Politica privind gestionarea incidentelor de securitate cibernetică: Această politică ar trebui să stabilească proceduri pentru gestionarea incidentelor de securitate cibernetică, cum ar fi procedurile de raportare, investigație și remediere a incidentelor de securitate cibernetică. Această politică definește cerința de raportare și răspuns la incidente legate de sistemele și operațiunile informaționale ale organizației. Răspunsul la incident oferă organizației capacitatea de a identifica când are loc un incident de securitate. Dacă monitorizarea nu ar exista, amploarea prejudiciului asociat cu incidentul ar fi semnificativ mai mare decât dacă incidentul ar fi notat și corectat.
20. Politica privind utilizarea echipamentelor personale: Această politică ar trebui să stabilească reguli și cerințe privind utilizarea echipamentelor personale, cum ar fi telefoane mobile, laptop-uri sau dispozitive de stocare externă, în cadrul organizației.
21. Politica privind securitatea rețelelor wireless: Această politică ar trebui să stabilească reguli și cerințe privind securitatea rețelelor wireless utilizate de organizație, cum ar fi criptarea datelor, autentificarea și protecția împotriva atacurilor de tip "man-in-the-middle".
22. Politica privind gestionarea datelor de backup: Această politică ar trebui să stabilească cerințe privind gestionarea datelor de backup și a procedurilor de recuperare a datelor în cazul unui incident de securitate cibernetică sau al unei defecțiuni a sistemelor.
23. Politica privind securitatea aplicațiilor web: Această politică ar trebui să stabilească reguli și cerințe privind securitatea aplicațiilor web utilizate de organizație, cum ar fi criptarea datelor, autentificarea și protecția împotriva atacurilor de tip SQL injection sau cross-site scripting.
24. Politica privind securitatea datelor din cloud: Această politică ar trebui să stabilească reguli și cerințe privind utilizarea serviciilor de stocare în cloud, cum ar fi protejarea datelor sensibile, criptarea și restricționarea accesului.
25. Politica privind utilizarea rețelelor sociale: Această politică ar trebui să stabilească reguli și cerințe privind utilizarea rețelelor sociale în cadrul organizației, cum ar fi restricționarea accesului la anumite rețele sociale și instruirea angajaților cu privire la amenințările cibernetice asociate utilizării rețelelor sociale. Utilizarea rețelelor sociale externe (adică Facebook, LinkedIn, Twitter, YouTube etc.) în cadrul organizațiilor este în creștere. Organizația se confruntă cu expunerea unei anumite cantități de informații care pot fi vizibile prietenilor din rețelele sociale. Deși această expunere este un mecanism cheie care conduce la valoare, ea poate crea, de asemenea, un canal inadecvat pentru ca informațiile să treacă între contactele personale și cele de serviciu. Instrumente pentru a stabili bariere între rețelele personale și private și instrumente pentru gestionarea centrală a conturilor abia încep să apară. Implicarea Departamentului IT pentru probleme de securitate, confidențialitate și lățime de bandă este de cea mai mare importanță.

26. Politica privind securitatea sistemelor de control al rețetelor critice: Această politică ar trebui să stabilească reguli și cerințe privind securitatea sistemelor de control utilizate de primărie și subordonate sau subcontractori, cum ar fi protejarea împotriva atacurilor cibernetice care ar putea afecta operațiunile critice.
27. Politica privind securitatea echipamentelor de acces la rețea: Această politică ar trebui să stabilească reguli și cerințe privind securitatea echipamentelor de acces la rețea, cum ar fi ruterul și firewall-ul, pentru a proteja rețeaua organizației împotriva atacurilor cibernetice. Această politică guvernează modul în care firewall-urile vor filtra traficul de internet pentru a atenua riscurile și pierderile asociate cu amenințările de securitate la adresa rețelei și a sistemelor de informații ale organizației.
28. Politica anti-virus: Această politică trebuie stabilită pentru a ajuta la prevenirea infectării computerelor, rețelelor și sistemelor tehnologice ale companiei cu malware și alt cod rău intenționat. Această politică este menită să prevină deteriorarea aplicațiilor, datelor, fișierelor și hardware-ului utilizatorului.
29. Politica de birou curat: Scopul și principiul unei politici de „birou curat" este de a se asigura că datele confidențiale nu sunt expuse persoanelor care pot trece prin zonă, cum ar fi membrii, personalul de serviciu și hoții. Încurajează gestionarea metodică a spațiului de lucru. Din cauza riscului de a fi compromise, informațiile confidențiale trebuie întotdeauna tratate cu grijă.
30. Politica de servicii electronice: Această politică trebuie utilizată atât ca ghid, cât și ca imagine de ansamblu în gestionarea serviciilor electronice ale organizației.
31. Politica de eliminare a hardware-ului și a suporturilor electronice: Surplusul de hardware, computere învechite și orice echipament care nu este reparat sau reutilizat rezonabil, inclusiv mediile, sunt acoperite de această politică. Acolo unde activele nu au ajuns la sfârșitul duratei de viață, este de dorit să se profite de valoarea reziduală prin revânzare, licitație, donație sau reatribuire către o funcție mai puțin critică. Această politică va stabili și defini standarde, proceduri și restricții pentru dispunerea de echipamente și suporturi IT neînchiriate într-o manieră legală și rentabilă.
32. Politica de achiziții în tehnologia informației: Scopul acestei politici este de a defini standarde, proceduri și restricții pentru achiziționarea tuturor hardware-ului IT, software-ului, componentelor legate de computer și serviciilor tehnice achiziționate cu fondurile organizației. Achizițiile de tehnologie și servicii tehnice pentru organizație trebuie să fie aprobate și coordonate prin Departamentul IT.
33. Politica de gestionare a jurnalelor (log-urilor): Gestionarea jurnalelor poate fi de mare beneficiu într-o varietate de scenarii, cu un management adecvat, pentru a îmbunătăți securitatea, performanța sistemului, gestionarea resurselor și conformitatea cu reglementările.
34. Politica de salvgardare a informațiilor angajaților: Scopul acestei politici este de a se asigura că organizația respectă legile de stat existente și de a se asigura că informațiile referitoare la membri sunt păstrate în siguranță și confidențiale.
35. Politica de utilizare acceptabilă pentru securitatea rețelei și VPN: Scopul acestei politici este de a defini standarde pentru conectarea la rețeaua organizației de la orice gazdă. Aceste standarde sunt concepute pentru a minimiza expunerea potențială a organizației de la daune, care pot rezulta din utilizarea neautorizată a resurselor organizației. Daunele includ pierderea de date sensibile sau confidențiale ale organizației, proprietate intelectuală, deteriorarea imaginii publice, deteriorarea sistemelor interne critice ale organizației.
36. Politica de utilizare și securitate acceptabilă a dispozitivelor personale (BYOD – bring your personal device): Această politică definește standardele, procedurile și restricțiile pentru utilizatorii finali care au cerințe legitime pentru a accesa datele organizației folosind dispozitivul lor personal. Această politică se aplică, dar nu se limitează la, oricăror dispozitive mobile deținute de utilizatorii enumerați mai sus care participă la programul BYOD al organizației, care conține date stocate deținute de organizație.
37. Politica de gestionare a corecțiilor (patch-urilor): Vulnerabilitățile de securitate sunt inerente sistemelor și aplicațiilor de calcul. Aceste defecte permit dezvoltarea și propagarea de software rău intenționat, care poate perturba operațiunile normale, pe lângă faptul că pun organizația în pericol. Pentru a atenua eficient acest risc, sunt puse la dispoziție „patch-uri" software pentru a elimina o anumită vulnerabilitate de securitate.

38. Politica de monitorizare și audit a sistemelor: Monitorizarea și auditarea sistemului este utilizată pentru a determina dacă au avut loc acțiuni inadecvate în cadrul unui sistem informațional. Monitorizarea sistemului este folosită pentru a căuta aceste acțiuni în timp real, în timp ce auditarea sistemului le caută după fapt.
39. Politica de evaluarea vulnerabilității: Scopul acestei politici este de a stabili standarde pentru evaluările periodice ale vulnerabilității. Această politică reflectă angajamentul primăriei de a identifica și implementa controale de securitate, care vor menține riscurile pentru resursele sistemului informațional la niveluri rezonabile și adecvate.
40. Politica de funcționare a site-ului web: Scopul acestei politici este de a stabili linii directoare în ceea ce privește comunicarea și actualizările site-ului web al organizației destinat publicului. Protejarea informațiilor de pe și în cadrul site-ului web al organizației, cu aceleași standarde de siguranță și confidențialitate utilizate în tranzacția tuturor serviciilor organizației, este vitală pentru succesul organizației. Utilizarea corectă a aplicațiilor și serviciilor online este definită de această politică. Scopul este de a determina nivelul de securitate și de a identifica vulnerabilitățile site-urilor web. De asemenea servește la protejarea informațiilor critice ale cetățenilor care folosesc serviciile online de pe portalul primăriei de scripturile dăunătoare de pe alte pagini. În acest sens, politica de securitate a conținutului conturează tehnicile tipice pentru încărcarea materialelor pe site-uri web. În plus, politica permite date despre a doua pagină web cu aceeași origine ca prima care va fi accesată.
41. Politica de securitate pentru configurarea stației de lucru: Scopul acestei politici este de a îmbunătăți securitatea și starea de funcționare de calitate pentru stațiile de lucru utilizate în organizație. Resursele IT trebuie să utilizeze aceste linii directoare atunci când implementează toate echipamentele noi ale stațiilor de lucru. Se așteaptă ca utilizatorii stațiilor de lucru să mențină aceste reguli și să lucreze în colaborare cu resursele IT pentru a menține regulile care au fost implementate.
42. Politica de virtualizare server: Scopul acestei politici este de a stabili cerințele de virtualizare a serverului care definesc achiziția, utilizarea și gestionarea tehnologiilor de virtualizare a serverului. Această politică oferă controale care asigură că problemele Enterprise sunt luate în considerare, împreună cu obiectivele de afaceri, atunci când se iau decizii legate de virtualizarea serverului. Politicile, standardele și liniile directoare ale arhitecturii platformei vor fi utilizate pentru a achiziționa, proiecta, implementa și gestiona toate tehnologiile de virtualizare a serverelor. Virtualizarea serverului este folosită pentru a masca resursele serverului de utilizatorii serverului. Aceasta poate include numărul și identitatea sistemelor de operare, procesoarelor și serverelor fizice individuale. Virtualizarea serverului este procesul de împărțire a unui server fizic în mai multe servere virtuale unice și izolate prin intermediul unei aplicații software. Fiecare server virtual poate rula propriile sisteme de operare în mod independent.
43. Politica de conectivitate wireless (Wi-Fi): Scopul acestei politici este de a securiza și proteja activele informaționale deținute de organizației și de a stabili conștientizarea și practicile sigure pentru conectarea la Wi-Fi gratuit și nesecurizat și la cele care pot fi furnizate de organizație. Orgaizația furnizează dispozitive informatice, rețele și alte sisteme informatice electronice pentru a îndeplini misiunile, obiectivele și inițiativele. Organizația acordă acces la aceste resurse ca un privilegiu și trebuie să le gestioneze în mod responsabil pentru a menține confidențialitatea, integritatea și disponibilitatea tuturor activelor informaționale.
44. Politica de telecommuting: În sensul acestei politici, se face referire la angajatul definit de telecommuting care își desfășoară activitatea în mod regulat dintr-un birou care nu se află în clădirea organizației. Lucrul la distanță ocazional de către angajați sau munca la distanță de către non-angajați nu este inclusă aici. Concentrându-se pe echipamentul IT furnizat în mod obișnuit unui telecommuter, această politică abordează aranjamentul de lucru la telecommuting și responsabilitatea pentru echipamentul furnizat de organizație.
45. Politica privind internetul obiectelor: Scopul acestei politici este de a stabili o structură IoT definită pentru a se asigura că datele și operațiunile sunt securizate corespunzător. Dispozitivele IoT (ex. camere web) continuă să fie tot mai mult aplicate; prin urmare, este necesar ca organizația să aibă această structură în vigoare.

46. Politica de pregătirea personalului privind securitatea cibernetică: Recunoașterea diverselor tipuri de atacuri cibernetice si a bunelor practici.
47. Politica de confidențialitate: Obiectivul acestei politici este de a modela utilizarea corectă a datelor personale sensibile, în condițiile convenite de justificarea utilizării acestor date personale sensibile și pentru a le proteja de încălcări. În consecință, împiedică dezvăluirea, utilizarea, accesul, colectarea, transferul și schimbul a datelor personale sensibile fără cunoștința persoanelor, prin înăsprirea controlului prin consimțământul utilizatorului sau responsabilitatea de a păstra datele în siguranță de către o organizație care controlează datele. În plus, o politică de confidențialitate protejează atât proprietatea intelectuală cât și datele personale. Această politică respectă drepturile omului la confidențialitate și protecția datelor sensibile. În plus, stabilește sancțiuni pentru oricine încalcă confidențialitatea datelor cetățenilor.

FISA DE PROIECT FANION

Titlu

Completarea infrastructurii de securitate cibernetică în Primăria Bistrița

Coordonator din partea consultantului

Stelian Brad

Elemente de referință

Soluțiile de securitate cibernetică sunt instrumente și servicii tehnologice care ajută la protejarea organizațiilor împotriva atacurilor cibernetice, care pot duce la oprirea activității, furtul de date sensibile, deteriorarea reputației, amenzile de conformitate și alte consecințe adverse.

În mediul modern de securitate, cu o mare varietate de amenințări în continuă schimbare, instrumentele specializate sunt o parte esențială a securității cibernetice. Există mai multe categorii de soluții de securitate cibernetică:

▪ Soluții de securitate a aplicațiilor — ajută la testarea aplicațiilor software pentru vulnerabilități împotriva atacurilor cibernetice.

▪ Securitate end-point – implementată pe dispozitive end-point, cum ar fi serverele și stațiile de lucru ale angajaților, previn amenințările precum programele malware și accesul neautorizat și ajută la detectarea și oprirea încălcărilor pe măsură ce apar.

▪ Securitatea rețelei — monitorizează traficul de rețea, identifică traficul potențial rău intenționat și permite organizației să blocheze, să filtreze sau să atenueze în alt mod amenințările.

▪ Securitate Internet of Things (IoT) — ajută la obținerea vizibilității și la aplicarea controalelor de securitate rețelei în creștere de dispozitive IoT, care sunt din ce în ce mai folosite pentru aplicații critice și stochează date sensibile, dar sunt adesea nesecurizate prin proiectare.

▪ Securitate în cloud — ajută la obținerea controlului asupra mediilor cloud complexe publice, private și hibride, detectând configurațiile greșite și vulnerabilitățile de securitate și ajutând la remedierea acestora.

Soluțiile de securitate pentru instituții publice le ajută să aplice politicile de securitate cibernetică în infrastructura lor. Managementul securității cibernetice este practica de implementare a politicilor de securitate în scopul protejării ecosistemelor complexe.

Managementul securității cibernetice (MSC) cuprinde configurarea, implementarea și monitorizarea politicilor de securitate în mai multe medii și instrumente de securitate. Scopul managementului securității cibernetice este de a permite instituțiilor publice să obțină un control mai bun asupra unui mediu distribuit și complex.

Instituțiile publice pot folosi MSC pentru a aborda problemele legate de accesul neautorizat, precum și pentru a îndeplini cerințele de confidențialitate și conformitate. MSC protejează atât datele în repaus, cât și datele în tranzit. Instituțiile publice pot folosi MSC pentru a proteja informațiile pe măsură ce acestea trec prin diferite conexiuni, dispozitive și medii, inclusiv dispozitive deținute personal, sisteme distribuite și infrastructură cloud. De obicei, echipa de conducere a instituției publice este responsabilă pentru conducerea eforturilor MSC. În mod ideal, MSC ar trebui să ajute la protejarea instituției publice împotriva amenințărilor externe și interne.

Un plan de guvernare a securității cibernetice a instituției publice o ajută să definească o foaie de parcurs pentru îndeplinirea cerințelor de reglementare, controlul riscurilor, gestionarea operațiunilor de securitate. În mod ideal, un cadru de guvernare a securității instituției publice aliniază obiectivele publice și obiectivele de conformitate cu misiunea și viziunea organizației. Managementul securității instituției publice este practicat în conformitate cu strategia generală de guvernare a securității instituției publice.

Direcții posibile de intervenție

Securitatea aplicațiilor

Procesele și instrumentele de securitate a aplicațiilor ajută instituția publică să descopere, să remedieze și să remedieze continuu amenințările de securitate ale aplicațiilor. Pentru a fi cu adevărat eficace, securitatea aplicațiilor ar trebui aplicată la toate nivelurile, inclusiv software și hardware. Un router, de exemplu, poate ajuta la prevenirea pătrunderii traficului neautorizat în rețea, iar un scaner de vulnerabilități poate ajuta la descoperirea și remedierea vulnerabilităților înainte de apariția unei breșe. Împreună, ele protejează diferite componente ale aplicației.

Web Application Firewall (WAF)

WAF este un filtru bazat pe politici situat în fața unei aplicații web și auditează traficul HTTP/S care se deplasează între Internet și aplicație. Un WAF încearcă să detecteze și să prevină amenințările și activitățile rău intenționate.

Securitate API

Interfețele de programare a aplicațiilor (API) permit comunicarea între diferite aplicații. Deoarece acest proces permite să transferăm informații între servicii și aplicații, este foarte vulnerabil la interceptări. Soluțiile de securitate API ajută la protejarea API-urilor și la prevenirea exploatării transmisiilor sau a vulnerabilităților. Pentru interoperabilitate acest aspect este foarte important.

Protecție DDoS

Un atac de tip denial-of-service (DoS) încearcă să întrerupă operațiunile normale ale unui singur server sau ale unei întregi rețele. Dacă atacul are succes, dispozitivul, aplicația sau rețeaua vizată suferă o întrerupere sau o întrerupere care împiedică operațiunile normale. Un atac de refuz de serviciu distribuit (DDoS) vizează de obicei site-urile web. Protecția DDoS poate ajuta la prevenirea întreruperilor în timpul atacurilor. Acest lucru trebuie asociat cu site-ul primăriei, chiar dacă serviciul este externalizat. Se recomandă reproiectarea site-ului primăriei pe tehnologii noi (ex. TYPO 3) care oferă posibilitatea actualizării informației de pe site direct de la nivel de compartimente ale primăriei. În relația cu cetățeanul acest lucru este de dorit. Externalizarea acestei activități implică un cost nejustificat și este lent reactiv. Poate fi gândit un proiect pentru reingineria site-ului sub forma unui portal.

Analiza compoziției software (SCA)

Soluțiile Software Composition Analysis (SCA) analizează componentele open-source ale aplicațiilor. După ce SCA identifică software-ul open-source, instrumentul oferă informații despre fiecare bibliotecă, inclusiv informații despre licențiere și date despre vulnerabilitățile de securitate detectate. Versiunile Enterprise ale SCA oferă adesea capabilități suplimentare, cum ar fi politici automate.

Testarea securității aplicațiilor (SAST/DAST/IAST)

▪ Testarea securității aplicațiilor statice (SAST) — instrumente care utilizează testarea „cutie albă” pentru a inspecta codul sursă static și pentru a furniza rapoarte despre problemele de securitate. SAST se aplică pentru a verifica codul necompilat pentru erori de sintaxă și matematică și pentru a rula analizoare binare pe codul compilat. Acest lucru se justifică dacă se dezvoltă diverse aplicații contractate de către primărie pentru a verifica că soluțiile livrate sunt robuste sub aspectul securității cibernetice.

▪ Testare dinamică de securitate a aplicațiilor (DAST) — instrumente care utilizează testarea „cutie neagră” pentru a inspecta codul în timpul rulării și pentru a oferi informații despre potențialele vulnerabilități de securitate, cum ar fi scurgeri, autentificare, injectare de date și șiruri de interogări. DAST se aplică pentru a simula un număr mare de scenarii.

▪ Testare interactivă de securitate a aplicațiilor (IAST) — instrumente care folosesc atât abordările DAST, cât și SAST pentru a descoperi o gamă mai largă de vulnerabilități. Instrumentele IAST sunt implementate în serverul de aplicații, unde inspectează dinamic codul sursă compilat în timpul rulării.

▪ Runtime Application Self-Protection (RASP) — instrumente care folosesc IAST, DAST și SAST și pot detecta și preveni o gamă mai mare de amenințări de securitate. Instrumentele RASP pot analiza traficul utilizatorilor și traficul aplicațiilor în timpul rulării, de exemplu. Odată ce amenințările sunt detectate, instrumentele RASP pot răspunde activ la eveniment.

Securitatea datelor

Managementul datelor sensibile

Soluțiile de gestionare a datelor sensibile ajută primăria să identifice și să gestioneze diferite tipuri de date sensibile, inclusiv:

▪ Informații de identificare cu caracter personal (PII)

▪ Date privind cardurile de plată (PCI)

▪ Informații despre aspecte personale protejate (PHI)

▪ Proprietatea intelectuală asupra unor date (IP)

Soluțiile de gestionare a datelor sensibile se integrează de obicei cu mai multe sisteme, asigurându-se că primăria poate gestiona informațiile sensibile răspândite în diferite aplicații, baze de date și puncte finale ale utilizatorilor.

Conformitatea datelor

Procesele de conformitate a datelor ajută primăria să se asigure că informațiile protejate sunt organizate și gestionate în mod corespunzător în conformitate cu cerințele de reglementare relevante. Acest lucru începe de obicei cu identificarea tipului de date și apoi implementarea măsurilor adecvate de securitate și confidențialitate. Se pot folosi mai multe soluții pentru a atinge conformitatea, inclusiv instrumente care identifică automat tipurile de date.

Prevenirea amenințărilor

Soluțiile de prevenire a amenințărilor ajută primăria să detecteze și să prevină amenințările și vulnerabilitățile avansate cunoscute. Acest proces implică filtrarea și distribuirea datelor relevante către mai multe instrumente, care oferă asistență suplimentară, răspuns și analiză.

Guvernarea datelor

Procesele de guvernare a datelor ajută primăria să gestioneze întregul ciclu de viață al datelor. Scopul este de a menține disponibilitatea, integritatea și capacitatea de utilizare a datelor. O soluție de guvernare a datelor oferă capabilități care ajută primăria să definească politici și procese, să specifice proprietarii de date și să controleze și să gestioneze eficient mișcarea datelor.

Descoperirea în cloud

Instrumentele de descoperire în cloud ajută primăria să identifice instanțe de cloud care rulează într-un anumit moment de timp. Aceasta include aplicații, containere, baze de date și orice altă componentă bazată pe cloud. Scopul este de a oferi primăriei o vedere centralizată a tuturor componentelor cloud, inclusiv informații despre date, stocare și performanță. De obicei, instrumentele de descoperire în cloud oferă capabilități de descoperire automată care funcționează

în medii multi-cloud. Acest lucru trebui avut în vedere pentru momentul adopției cloud-ului guvernamental.

Securitatea punctelor terminale

Platforma de protecție a punctelor terminale (EPP)

Odată ce fișierele intră în rețea, instrumentul APP îl scanează și caută amenințări cunoscute. Soluțiile antivirus tradiționale (AV), de exemplu, scanează fișierele în timp ce caută amenințări cunoscute bazate pe semnături.

Detectarea și remedierea punctelor finale (EDR)

Soluțiile EDR oferă protecție activă prin monitorizarea proactivă și continuă a tuturor fișierelor și aplicațiilor care intră pe dispozitiv. Soluțiile EDR oferă vizibilitate și analiză granulară și detectează o serie de amenințări, mai degrabă decât atacuri bazate pe semnături. De exemplu, EDR poate detecta ransomware, malware fără fișiere, atacuri polimorfe și multe altele.

Detectare și răspuns extins (XDR)

Soluțiile XDR oferă protecție extinsă și răspuns pe mai multe niveluri de securitate. XDR implică un set de instrumente și capabilități care folosesc analiza și automatizarea inteligente atunci când se efectuează detectarea și răspunsul amenințărilor. Acest lucru permite soluțiilor XDR să ofere mai multă vizibilitate și să colecteze și să coreleze o cantitate imensă de date despre amenințări.

Securitatea rețelei

▪ Controlul accesului la rețea—permite primăriei să controleze și să restricționeze accesul la rețea. Caracteristicile notabile includ interzicerea accesului la rețea la dispozitivele neconforme, plasarea dispozitivelor în zone de carantină și restricționarea accesului la resurse.

▪ Segmentarea rețelei—permite primăriei să controleze fluxul de trafic. Se poate face segmentarea rețelei pentru a opri tot traficul dintr-o zonă de rețea să nu ajungă în alta și pentru a limita fluxul de trafic în funcție de sursă, tip și destinație.

▪ Network-Based IDS (NIDS) — soluții concepute pentru a monitoriza o întreagă rețea. Instrumentele NIDS oferă vizibilitate asupra întregului trafic care circulă prin rețea. Instrumentul poate face determinări în funcție de metadatele și conținutul pachetului și poate detecta amenințările.

▪ Firewall-uri de generație următoare (NGFW) — concepute pentru a securiza conexiunile dintre rețea, firewall și Internet. Soluțiile NGFW folosesc de obicei filtrarea statică și dinamică a pachetelor, suport VPN, liste albe și IPS bazate pe semnături atunci când impun securitatea.

Alte aspecte de securitate

DMARC

Autentificarea, raportarea și conformitatea mesajelor bazate pe domeniu (DMARC) este un protocol de autentificare creat special pentru comunicarea prin e-mail. Protocolul DMARC folosește cadrul politicii expeditorului (SPF) și e-mailurile identificate DomainKeys (DKIM) pentru a autentifica mesajele de e-mail. DMARC adaugă un alt nivel de încredere, susținând eforturile generale de securitate ale primăriei. Puteți adăuga DMARC pentru a completa efortul de securitate, dar nu oferă o acoperire completă.

Autentificare fără parolă

Autentificarea fără parolă permite primăriei să înlocuiască parolele cu alte forme de autentificare, cum ar fi generatoare de parole, semnături biometrice și jetoane. Scopul este de a reduce numărul de parole slabe create de utilizatori și de a împiedica utilizatorii să-și folosească parolele personale în scopuri profesionale. Autentificarea fără parolă poate îmbunătăți atât securitatea, cât și experiența utilizatorului.

Încredere zero

Încrederea zero este un model de securitate care impune controale stricte de acces. Scopul este de a se asigura că nu numai perimetrul tradițional de securitate este acoperit, ci și toate activele distribuite în diferite locații. Un laptop conectat la rețea, un dispozitiv mobil conectat la serverul primăriei, un mediu SaaS partajat cu părți externe - toate acestea ar trebui tratate cu zero încredere. La cel mai elementar nivel, aceasta înseamnă aplicarea unei autentificări stricte pentru tipurile de utilizatori granulari. De asemenea, se folosește securitatea punctelor terminale pentru a impune încredere zero.

Îmbunătățirea confidențialității

Analizele de îmbunătățire a confidențialității poate permite primăriei să protejeze informațiile private. Un obiectiv crucial aici este de a oferi un mediu de încredere pentru procesarea datelor sensibile. În plus, tehnologiile de îmbunătățire a confidențialității folosesc algoritmi de învățare automată (ML) care țin cont de confidențialitate pentru a descentraliza procesarea și analiza datelor. Calculul de îmbunătățire a confidențialității implică adesea utilizarea criptării homomorfe - un tip de criptografie care permite terților să proceseze date criptate. Terțul returnează apoi proprietarului datelor numai rezultate criptate, fără a furniza informații despre rezultate sau date. Acest proces permite colaboratorilor să partajeze date fără a încălca confidențialitatea.

Hiper automatizarea

Hiper-automatizarea este practica de automatizare a cât mai multor procese IT. Acest lucru implică de obicei utilizarea mai multor procese de decizie și tehnologii de automatizare, cum ar fi inteligența artificială (AI), învățarea automată (ML) și automatizarea proceselor (RPA). Scopul este de a ajuta primăria să reducă cheltuielile generale și ineficiența asociate cu sistemele vechi prin crearea de canale eficiente, automate și interconectate.

Cadru pentru a ajuta primăria să administreze securitatea cibernetică

Este necesară implementarea unui cadru de securitate cibernetică pentru a securiza toate mediile. Acest cadru se aplică pe patru mari direcții, după cum urmează:

Figura: Arhitectura de securitate cibernetică

1. Protejare

▪ Antivirus: selectarea celei mai potrivite soluții antivirus pentru calculatoare, mobile și servere (a se vedea: TotalAV, Norton, Bitdefender, Panda, PC Protect, Avira, McAfee, Avast)

▪ Managementul parolelor: selectarea unei soluții pentru managementul parolelor (a se vedea NordPass, Bitdefender, TotalAV, Keeper, Norton, 1passowrd, etc.)

▪ Detectare și răspuns gestionat (MDR): a se vedea Cynet, Rapid7, Cybereason, SentinelOne Vigilance, CrowdStrike, eSentire, Expulza, Secureworks, Fidelis Cybersecurity, FireEye Mandiant)

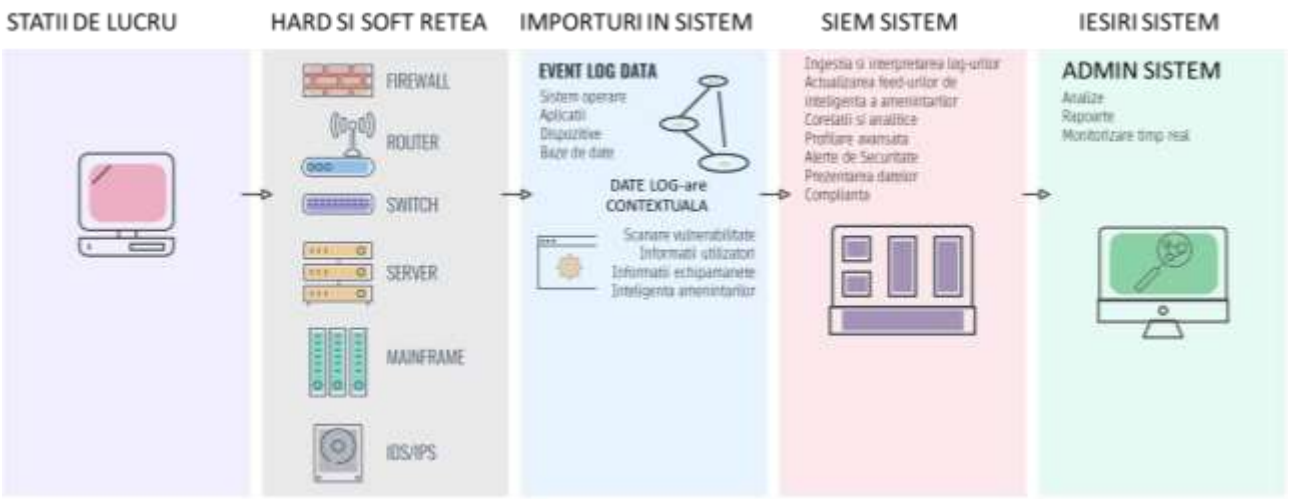
▪ Firewall cu Total Security Suite: hardware și software – soluțiile alese pot fi similare cu cele pentru afaceri de dimensiune mică

▪ Patch-uri MS și de terță parte

▪ Filtrarea SPAM: de regulă cuprinse în sistemele antivirus

▪ Securitate e-mail: soluții software specializate (ex. SkyExtractor, SkyFlow, proofpoint, Avanan, Mimecast, Barracuda, Cisco, etc.)

▪ Securitate și management al evenimentelor (SIEM): a se vedea platforma plug-and-play Cyrebro, Log360, IBM QRadar, McAfee Enterprise Security Manager, etc.



▪ Autentificare cu mai mulți factori (MFA): a se vedea Telesign, Microsoft Authenticator, Google Authenticator, Duo Security, LastPass, Authy, RSA SecurID® Access, OneLogin, Okta MFA for Fortinet VPN

▪ Instruirea utilizatorilor pe probleme de securitate cibernetică

▪ Politici de utilizare a computerului

▪ Securitatea site-ului web: Let's Encrypt - SSL Certificate; Cloudflare - Web Application Firewall; Cloud CDN - Global Content Delivery Network; LogicMonitor - Website Monitoring Service; Duo Security - Two-Factor Authentication; GoDaddy - Secure Site Hosting; Dropmysite - Website Backup

▪ Securitatea navigării pe web: suport pentru browser-e multiple (ex. Browser Security Plus, Cisco, Perimeter 81, WebTitan, Broadcom, iboss, Forcepoint, Menlo Security, Palo Alto, Trend Micro, ZScaler)

2. Detectare

▪ Antivirus

▪ Detectare și răspuns gestionat (MDR): O platformă de securitate MDR este considerată un control avansat de securitate 24/7, care include adesea o serie de activități de securitate fundamentale, inclusiv securitate gestionată în cloud pentru organizațiile care nu își pot menține propriul centru de operațiuni de securitate. Serviciile MDR combină analize avansate, informații despre amenințări și expertiză umană în investigarea incidentelor și răspunsul implementat la nivel de gazdă și rețea. Pe măsură ce volumul, varietatea și sofisticarea amenințărilor la adresa securității cibernetice cresc exponențial, organizațiile se luptă să mențină centre de operațiuni de securitate dotate cu personal și resurse foarte calificate. Ca rezultat, furnizorii de Managed Detection and Response oferă un pachet rentabil de servicii concepute pentru a îmbunătăți apărarea unei organizații în domeniul securității cibernetice și pentru a minimiza riscul fără o investiție inițială în securitate cibernetică. Serviciile MDR oferă analiști cu un nivel mai înalt de calificare care utilizează instrumente de securitate de ultimă oră și baze de date globale de ultimă oră, dincolo de atingerea și rentabilitatea majorității bugetelor, nivelurilor de calificare și resurselor organizației. Serviciile MDR oferă o alternativă de securitate avansată prin integrarea instrumentelor de detectare și răspuns la punctele finale (EDR). Ca rezultat, nivelul de monitorizare, detectare și analiză a amenințărilor unei întreprinderi este îmbunătățit fără provocarea și cheltuielile necesare pentru a menține o echipă de securitate internă complet echipată și la curent cu cele mai recente date despre amenințări. Serviciile MDR nu se limitează la capacități mai mari de detectare și răspuns.

▪ Firewall cu Total Security Suite

▪ Securitate e-mail

▪ Informații de securitate și management al evenimentelor (SIEM)

▪ Monitorizare Dark Web (opțional, dacă se dorește verificarea prezenței unor date ale primăriei care se tranzacționează în acest spațiu): ex. Norton 360, Bitdefender. Dark Web Monitoring vă permite să conștientizați și să luați măsuri dacă sunteți notificat că informațiile dvs. au fost găsite pe dark web. De exemplu, dacă aflați că adresa dvs. de e-mail sau un număr de cont a fost găsit pe dark web, puteți actualiza parola pe care o utilizați pentru a vă conecta la acel cont cu o parolă nouă, unică și complexă.

▪ Sistem de management al schimbării: Managementul schimbărilor este o componentă cheie de securitate a informațiilor pentru menținerea sistemelor de înaltă disponibilitate. Managementul schimbărilor implică solicitarea, aprobarea, validarea și înregistrarea modificărilor la sisteme. Acest proces poate aduce beneficii semnificative unei organizații. Poate întări capacitatea de luare a deciziilor prin instruirea personalului pentru a gândi și evalua pe deplin schimbările înainte de a fi efectuate și oferă o bază de cunoștințe despre schimbările trecute și lecțiile învățate din situații. Securitatea informațiilor poate fi împărțită în trei secțiuni: confidențialitate, integritate și disponibilitate, adesea numite triada CIA. Disponibilitatea este extrem de importantă. Dacă datele nu sunt disponibile utilizatorilor autorizați atunci când au nevoie de ele, la ce folosesc? Disponibilitatea ridicată este un alt termen care descrie un sistem care este accesibil utilizatorilor 24×7, cu timp de nefuncționare programat minim. O metodă adesea menționată pentru obținerea unei disponibilități ridicate include redundanța hardware, cum ar fi firewall-urile active/pasive, serverele în cluster, echilibrarea sarcinii rețelei și DNS-ul round robin. Redundanța este un aspect pe care trebuie să îl aibă rețelele de înaltă disponibilitate. Cu toate acestea, un alt factor important în obținerea unei disponibilități ridicate este o politică de management al schimbării. Orice schimbare are potențialul de a crea noi vulnerabilități sau de a reduce disponibilitatea sistemelor. Desigur, procesul de întreținere a sistemelor și de gestionare a obiectivelor de afaceri necesită schimbare. Prin urmare, organizațiile trebuie să stabilească cum să echilibreze nevoia de

schimbare cu minimizarea riscului. Răspunsul este prin managementul schimbării. Aceasta începe cu o politică de management al schimbării care duce apoi la un program de management al schimbării, prin care managementul schimbării este implementat în întreaga organizație.

- Managementul rețelei, monitorizarea și managementul de la distanță (RMM): a se vedea Atera, NinjaOne, GoToResolve, Central, etc.

3. Răspuns

- Antivirus
- Detectare și răspuns gestionat (MDR)
- Securitate e-mail
- Informații de securitate și management al evenimentelor (SIEM)
- Administrare rețea
- Monitorizare și management de la distanță (RMM)

4. Recuperare

- Backup Disaster Recovery
- Planul de continuitate
- Administrare rețea
- Gestionarea incidentelor

FISA DE PROIECT FANION

Titlu

Diagnoza competentelor de bază în privința securității cibernetice

Coordonator din partea consultantului

Stelian Brad

Context si justificare

Proiectul de diagnoza a competentelor de baza ale angajatilor din Primaria Bistrita in securitate cibernetica si GDPR se justifica prin nevoia de a imbunatati nivelul de securitate cibernetica si de a asigura conformitatea cu reglementarile privind protectia datelor cu caracter personal. In ultimii ani, au existat numeroase cazuri de atacuri cibernetice si incalcari ale confidentialitatii datelor, iar o primarie cu o infrastructura IT complexa si cu o baza de date cu informatii confidentiale despre cetateni este expusa la riscuri majore. Mai mult decat atat, conformitatea cu GDPR este obligatorie si Primaria Bistrita trebuie sa asigure respectarea acestor reglementari pentru a proteja drepturile cetatenilor privind prelucrarea datelor lor cu caracter personal.

Obiective si rezultate

Obiectivele proiectului sunt urmatoarele:

- Testarea a 10-20% dintre angajatii Primariei Bistrita in ceea ce priveste competentele de baza in securitatea cibernetica si GDPR;
- Identificarea nevoilor de formare a angajatilor in aceste domenii;
- Dezvoltarea unor planuri de formare personalizate pentru angajati, bazate pe rezultatele testelor;
- Cresterea nivelului de constientizare si responsabilitate a angajatilor in ceea ce priveste securitatea cibernetica si GDPR;
- Cresterea securitatii si protectiei datelor cu caracter personal ale Primariei Bistrita.

Rezultatele asteptate ale proiectului sunt:

- Testarea a cel putin 10-20% dintre angajatii Primariei Bistrita in ceea ce priveste competentele de baza in securitatea cibernetica si GDPR;
- Identificarea nevoilor de formare a angajatilor in aceste domenii;
- Dezvoltarea planurilor de formare personalizate pentru angajati;
- Realizarea si livrarea programelor de formare pentru angajati;
- Imbunatatirea nivelului de constientizare si responsabilitate a angajatilor in ceea ce priveste securitatea cibernetica si GDPR;
- Cresterea securitatii si protectiei datelor cu caracter personal ale Primariei Bistrita.

Planul de implementare

Proiectul va fi implementat in urmatoarele etape:

- Etapa 1: Elaborarea bateriei de teste pentru competentele de baza in securitatea cibernetica si GDPR (2 luni);
- Etapa 2: Testarea a 10-20% dintre angajatii Primariei Bistrita (0.1 luni);
- Etapa 3: Analiza si interpretarea rezultatelor testelor (0.5 luni);
- Etapa 4: Dezvoltarea planurilor de formare pentru angajati (0.5 luni);
- Etapa 5: Realizarea si livrarea programelor de formare pentru angajati (6 luni);
- Etapa 6: Monitorizarea si evaluarea rezultatelor formarii angajatilor (6 luni).

Primele trei etape se realizează în contextul proiectului de informatizare a Primăriei Bistrita.

Pentru viitor trebuie alocat doar bugetul pentru etapele 4, 5 si 6. Bugetul estimat este de 35.000 euro. Aceasta suma va fi alocata pentru achizitionarea de licente software necesare pentru testarea angajatilor, elaborarea planurilor de formare, realizarea programelor de formare, precum si pentru evaluarea si monitorizarea rezultatelor formarii.

Sustenabilitate si impact

Acest proiect fanion va avea un impact semnificativ asupra comunitatii locale prin cresterea nivelului de constientizare a angajatilor privind importanta securitatii cibernetice si a GDPR, si, prin urmare, imbunatatirea nivelului de protectie al informatiilor personale si confidentiale detinute de Primaria Bistrita. De asemenea, va creste nivelul de competente in ceea ce priveste securitatea cibernetica si GDPR, ceea ce va ajuta la imbunatatirea proceselor si procedurilor in ceea ce priveste stocarea si manipularea datelor personale.

Pentru a asigura sustenabilitatea acestui proiect, vom organiza sesiuni periodice de formare si instruire a personalului si vom continua sa actualizam si sa imbunatatim bateria de teste pentru securitatea cibernetica si GDPR. De asemenea, vom colabora cu alte institutii si organizatii pentru a schimba experiente si pentru a imbunatati practicile privind protectia datelor cu caracter personal si securitatea cibernetica.

In ceea ce priveste impactul economic, implementarea acestui proiect fanion va ajuta la reducerea costurilor asociate cu breach-urile de securitate si incalcarea GDPR, si, prin urmare, va economisi bani si resurse. De asemenea, imbunatatirea proceselor de protectie a datelor va ajuta la evitarea pierderii de reputatie a Primariei Bistrita si va creste increderea cetatenilor in aceasta institutie.

Impactul social al acestui proiect va fi semnificativ, deoarece protectia datelor cu caracter personal si securitatea cibernetica sunt probleme importante care afecteaza toate aspectele vietii moderne, de la afaceri si guvernare pana la viata personala.

Anexe

Testul pentru evaluarea competentelor de securitate cibernetica

Testul pentru evaluarea competentelor de GDPR

EVALUARE CUNOȘTINȚE GENERALE PRIVIND PROTEJAREA ÎMPOTRIVA ATACURILOR CIBERNETICE

Durata: 2 ore

1. Imaginați-vă că sunteți angajat în departamentul de impozite al unei primării și primiți o notificare de la un cetățean care susține că a fost victima unui atac cibernetic. Cetățeanul spune că a primit un e-mail care pretindea că era de la primărie și a cerut să își introducă informațiile personale și bancare pentru a plăti taxele. Ulterior, aceste informații au fost folosite pentru a efectua tranzacții frauduloase pe contul său bancar. Ce ați face în această situație și cum ați preveni astfel de situații în viitor?

Răspuns:

2. Primiți acest mesaj pe email:

   Subiect: Verificare de securitate a contului

   Stimate coleg/colegă,

   În încercarea noastră de a asigura securitatea conturilor din Primărie, am implementat o funcție nouă de verificare a securității. Acest proces ajută să ne asigurăm că informațiile dvs. sunt protejate și să identificăm orice activitate suspectă.

   Vă rugăm să urmați acest link pentru a vă conecta la contul dvs. și a completa procesul de verificare. Dacă aveți întrebări sau îngrijorări, vă rugăm să contactați echipa noastră de suport tehnic.

   Vă mulțumim pentru cooperare,

   Director ……

   Este acesta un atac cibernetic sau nu? Daca da, din ce categorie face parte?

Răspuns:

3. Care dintre următoarele este cel mai important pas pe care trebuie să îl urmați pentru a evita phishing-ul?
   a) Faceți clic pe link-uri suspecte și verificați dacă URL-ul pare legitim.
   b) Verificați adresa de e-mail a expeditorului și căutați semne de phishing.
   c) Descărcați atașamentele din e-mail și verificați-le cu un program antivirus.
   d) Furnizați informații de cont sau personale prin intermediul unui e-mail.

Răspuns:

4. Primiți un e-mail care provine de la o sursă necunoscută. Acesta poate fi periculos, însă la Primărie vin tot felul de solicitări de la diverși cetățeni. Ce pași urmați pentru a vă asigura ca emailul respectiv nu este malițios? Nu sunt adecvate răspunsuri de tipul "Îl contactez pe directorul IT". Trebuie singur/ă să știți ce pași să urmați, nefiind nevoie de alt ajutor pentru această situație.

Răspuns:

5. **Primiți emailul de mai jos:**

   Subiect: Ofertă specială de la eMAG pentru angajații primăriei

   Dragi angajați ai primăriei,

   Ne face plăcere să vă informăm că sunteți eligibili pentru o ofertă specială de la compania noastră. Vă oferim un discount de 50% la produsele noastre, disponibile exclusiv pentru angajații primăriei.

   Pentru a beneficia de această ofertă, tot ce trebuie să faceți este să dați click pe link-ul de mai jos și să completați formularul de înscriere. Oferta este valabilă doar pentru o perioadă limitată de timp!

   https://bestdealsforu.com/buy-now-50off-ipad

   Cu stimă,

   George Barbu
   Director marketing eMag

   Întrebare: Ce trebuie să faceți pentru a beneficia de ofertă?

Răspuns:

6. Deschideți emailul și în listă aveți un mesaj cu subiectul de mai jos:

   Subiect: Important – Vulnerabilitate de Securitate

   Stimate Utilizator,

   Vă informăm că sistemul vostru a fost compromis de un virus periculos și că toate fișierele dvs. personale au fost criptate. Pentru a recupera accesul la fișierele dvs., sunteți obligat să plătiți o sumă de 10000 de lei în termen de 24 de ore.

   Pentru a plăti, accesați acest link. Dacă nu plătiți în termenul specificat, vom fi nevoiți să distrugem toate fișierele criptate. Pentru mai multe detalii, contactați departamentul nostru de suport la adresa de e-mail.

   Ce tip de atac este acesta si cum trebuie sa procedați?

Răspuns:

7. Deschideți calculatorul și pe ecran vă apare un pop-up (o fereastră) cu următorul mesaj:

   „Fișierele dvs. au fost criptate cu algoritmi puternici de criptare. Dacă doriți să vă recuperați fișierele, trebuie să plătiți o răscumpărare de 10.000 USD în Bitcoin în 72 de ore. Dacă nu plătiți răscumpărarea, fișierele dvs. vor fi șterse definitiv și veți pierde pentru totdeauna accesul la ele. Nu încercați să vă recuperați fișierele folosind niciun software de terță parte, deoarece acest lucru va duce doar la deteriorarea ulterioară a fișierelor dvs. Urmați instrucțiunile din fișierul atașat pentru a efectua plata și a primi cheia de decriptare.”

   Ce tip de atac este acesta si cum trebuie sa procedați?

Răspuns:

8. Angajatul X a primit un e-mail cu subiectul "Actualizare importantă a software-ului de securitate. Descărcați fișierul atașat. Este posibil ca după aceea calculatorul dvs. Să funcționeze puțin mai lent, însă nu fiți îngrijorat pentru că este vorba despre sistemul antivirus care scanează permanent buna funcționare a calculatorului". Mesajul conținea un link care a dus la descărcarea unui fișier .exe. Angajatul X a descărcat și a rulat fișierul, după care a observat că calculatorul său merge mult mai lent decât de obicei. Ce s-a întâmplat și ce ar trebui să facă X?

Răspuns:

9. Angajații primăriei au observat că site-ul lor este blocat și nu poate fi accesat de către cetățeni. După o verificare, ați descoperit că site-ul este supus unui atac cibernetic.
   Cum se numește acest tip de atac cibernetic?

Răspuns:

Cum trebuie procedat in astfel de cazuri?

A. Închiderea site-ului web pentru o perioadă de timp pentru a evita mai multe atacuri
B. Restricționarea accesului la site doar pentru anumite adrese IP
C. Contactarea furnizorului de servicii de internet și solicitarea ajutorului pentru a filtra traficul nedorit
D. Plata răscumpărării cerute de atacator pentru a opri atacul

Răspuns:

10. Un coleg de serviciu ți-a trimis prin email un fișier atașat. Mesajul spune că este important să descarci fișierul și să îl deschizi pentru că este legat de un proiect important al primăriei. Ce faci?
    Opțiuni:
    A) Descarci și deschizi fișierul, deoarece este important.
    B) Nu descarci și nu deschizi fișierul, deoarece suspectezi că ar putea fi un virus sau malware.
    C) Descarci fișierul, dar nu îl deschizi, ci îl verifici cu un program antivirus înainte de a-l deschide.

Răspuns:

11. Cum puteți recunoaște un e-mail de phishing?

Răspuns:

12. Dați un exemplu de parola slabă și un exemplu de parolă puternică.

Răspuns:

Ce face să fie o parolă suficient de puternică?

Răspuns:

13. Ești un angajat al primăriei și încerci să accesezi contul tău de email de la birou. În mod normal, introduci doar numele de utilizator și parola pentru a te autentifica. Dar de data aceasta, apare o pagină suplimentară de autentificare cu un cod unic generat de o aplicație mobilă. Ce înseamnă acest lucru?

Răspuns:

14. Ca simplu utilizator de Internet, aveți posibilitatea de a vă configura emailul personal (ex. gmail.com, yahoo.com) pentru autentificare cu factori multipli?

Răspuns:

15. În timp ce navigați pe internet, ați găsit un site care oferă un joc distractiv și interesant. Vă înscrieți și începeți să jucați, dar apoi observați că tastatura dvs. nu funcționează la fel de bine ca înainte. Câteva zile mai târziu, vă dați seama că contul dvs. bancar a fost golit. **Întrebare:** Ce s-a întâmplat cu tastatura dvs. și cum a dus la golirea contului bancar?

Răspuns:

16. Ce este un virus informatic?
    A) Un program care se replică și se răspândește în mod independent prin sistemul informatic
    B) O unealtă de securitate pentru protejarea sistemelor informatice
    C) Un document important stocat în calculator

Răspuns:

Care dintre următoarele sunt semne ale unei infecții cu virus informatic?
A) Calculatorul rulează mai rapid decât de obicei
B) Apare un mesaj de avertisment de la antivirus
C) Imaginile și fișierele se deschid impropriu sau deloc

Răspuns:

Cum poate fi evitată infecția cu un virus informatic?
A) Descărcând programe de pe site-uri nesigure
B) Deschizând e-mail-uri suspecte sau atașamente
C) Utilizând un software antivirus actualizat și evitând site-urile nesigure

Răspuns:

Ce este un Trojan?
A) Un virus care se replică și se răspândește în mod independent prin sistemul informatic
B) O unealtă de securitate pentru protejarea sistemelor informatice
C) Un program care se prezintă ca o aplicație utilă, dar în realitate este un instrument de atac

Răspuns:

Ce este un worm?
A) Un virus care se replică și se răspândește în mod independent prin sistemul informatic
B) O unealtă de securitate pentru protejarea sistemelor informatice
C) Un program care urmărește activitatea utilizatorilor și stochează informațiile colectate

Răspuns:

17. Ce este un atac de tip "man-in-the-middle" și cum poate fi prevenit?
    a) Este un tip de atac în care un hacker interceptează comunicarea între două părți și își asumă controlul asupra acesteia.
    b) Este un tip de atac în care un hacker trimite mesaje false unei părți dintr-o comunicare.
    c) Este un tip de atac în care un hacker obține acces la un dispozitiv prin intermediul unei conexiuni WiFi publice nesecurizate.

Răspuns:

Ce este un atac de tip "zero-day" și cum poate fi prevenit?
a) Este un tip de atac în care un hacker utilizează o vulnerabilitate necunoscută dispozitivului pentru a obține acces neautorizat.
b) Este un tip de atac în care un hacker trimite un mesaj de spam către un utilizator pentru a obține acces la dispozitivul acestuia.
c) Este un tip de atac în care un hacker obține acces la un dispozitiv prin intermediul unei conexiuni WiFi publice nesecurizate.

Răspuns:

Ce este un atac de tip "phishing" și cum poate fi prevenit?
a) Este un tip de atac în care un hacker trimite un mesaj fals către un utilizator, de obicei prin e-mail, pentru a îl convinge să ofere informații personale sau financiare.
b) Este un tip de atac în care un hacker interceptează comunicarea între două părți și își asumă controlul asupra acesteia.
c) Este un tip de atac în care un hacker obține acces la un dispozitiv prin intermediul unei conexiuni WiFi publice nesecurizate.

Răspuns:

18. Care dintre următoarele este cel mai sigur mod de autentificare?
A) Autentificare cu factori multipli
B) Autentificare biometrică
C) Toate sunt la fel de sigure

Răspuns:

Ce trebuie să faceți pentru a vă proteja dispozitivele personale împotriva atacurilor cibernetice?
A) Actualizați software-ul și sistemul de operare
B) Instalați un program antivirus
C) Nu utilizați aceeași parolă pentru mai multe conturi
D) Toate cele de mai sus

Răspuns:

Ce este keylogging-ul?
A) Un program care încetinește viteza calculatorului
B) Un tip de malware care urmărește și înregistrează toate tastările de pe un calculator
C) Un tip de atac care trimite mesaje spam la adresele de e-mail
D) Toate cele de mai sus

Răspuns:

19. Imaginați-vă că sunteți într-un loc public, cum ar fi o cafenea, și ați lăsat telefonul mobil pe masă în timp ce mergeți să luați o cafea. Când vă întoarceți, observați că telefonul dvs. lipsește. Ce ați putea face in avans pentru a fi sigur ca datele personale stocate pe dispozitivul dvs. furat nu pot fi accesate?

Răspuns:

20. Dacă utilizați un laptop sau un calculator personal, cum vă asigurați că datele și informațiile dvs. sunt protejate împotriva accesului neautorizat? Care sunt câteva exemple de măsuri de securitate pe care le puteți lua pentru a vă proteja informațiile personale?

Răspuns:

21. Ce măsuri de securitate puteți lua pentru a vă proteja conturile de social media și alte conturi online? Ce trebuie să faceți dacă descoperiți că unul dintre conturile dvs. a fost compromis?

Răspuns:

22. Ce înseamnă termenul "criptare" în contextul securității cibernetice?
    a. Protejarea dispozitivelor împotriva virușilor și malware-ului
    b. Ascunderea informațiilor de către hackeri prin utilizarea unui cod secret
    c. Stocarea datelor sensibile într-un loc sigur și protejat

Răspuns:

Care dintre următoarele opțiuni este cel mai sigur mod de a trimite informații confidențiale prin e-mail?
a. Folosirea unui e-mail cu parola puternica si user complicat
b. Utilizarea unui serviciu de e-mail criptat
c. Folosirea unui e-mail cu parola puternica si user simplu

Răspuns:

Care metode sunt adecvate pentru a partaja o parolă cu o altă persoană?
a. Trimiterea parolei într-un fișier separat, protejat cu o parolă
b. Trimiterea parolei prin intermediul unui serviciu de e-mail criptat
c. Utilizarea unui serviciu de gestionare a parolelor, cum ar fi LastPass sau 1Password, care permite partajarea securizată a parolelor cu alți utilizatori
d. Utilizarea autentificării cu doi factori, în care parola este împreună cu un alt element de autentificare, cum ar fi un cod unic generat prin intermediul unei aplicații de autentificare sau un SMS trimis pe un telefon mobil
e. Utilizarea unui protocol de comunicare criptată, cum ar fi PGP (Pretty Good Privacy) sau S/MIME (Secure/Multipurpose Internet Mail Extensions), care permite criptarea conținutului mesajelor de e-mail, inclusiv a parolelor trimise
f. Toate metodele de mai sus sunt suficient de sigure

Răspuns:

Ce este o cheie de criptare?
a. Un cod secret utilizat pentru a accesa un cont online
b. Un cod de securitate generat de dispozitivul mobil
c. Un cod secret utilizat pentru a cripta și decripta informațiile

Răspuns:

Cum poate fi utilizată tehnologia blockchain în securitatea cibernetică?
a. Pentru a cripta și proteja informațiile personale
b. Pentru a oferi o metodă sigură de stocare și transfer de date
c. Pentru a preveni accesul neautorizat la dispozitivele personale

Răspuns:

23. Cum poți să trimiți un e-mail criptat către un coleg de la locul de muncă folosind un serviciu de e-mail criptat? Cum îi transmiți parola de decriptare?

Răspuns:

24. Care dintre următoarele opțiuni sunt caracteristici ale unui e-mail criptat?
    a) Îmbunătățește viteza de livrare a e-mailului și reduce riscul de interceptare a informațiilor.
    b) Îți permite să împărtășești informații confidențiale în siguranță cu alte persoane.
    c) Permite furnizarea de mesaje personalizate către destinatarii e-mailului.

Răspuns:

25. Ce este un cod de amestecare a textului în ceea ce privește e-mailurile criptate?
    a) Un fișier de securitate care trebuie descărcat și instalat înainte de a putea citi conținutul e-mailului criptat.
    b) Un instrument care permite expedierea de e-mailuri criptate și care este instalat în mod automat în toate programele de e-mail.
    c) Un cod de amestecare a textului e-mailului trimis, care îl face ilizibil pentru persoanele care nu dețin codul corespunzător.
    d) Un limbaj de programare utilizat pentru a cripta și decripta e-mailurile.

Răspuns:

26. Care este cel mai mare risc de securitate atunci când utilizați telefonul de serviciu într-o cafenea cu o rețea wireless publică?
    a) Încălcarea confidențialității datelor dvs. prin interceptarea traficului de date al rețelei publice.
    b) Descărcarea unui virus care poate afecta telefonul de serviciu și rețeaua companiei.
    c) Utilizarea excesivă a datelor și facturarea suplimentară.
    d) Vizualizarea de către alții a datelor de contact și a mesajelor salvate pe telefon.

Răspuns:

27. Ce trebuie să faceți pentru a vă proteja telefonul de serviciu în timp ce utilizați o rețea wireless publică într-un aeroport?
    a) Utilizați un serviciu VPN pentru a vă proteja traficul de date și a păstra confidențialitatea informațiilor.
    b) Închideți toate aplicațiile care nu sunt necesare pentru a reduce expunerea la amenințările de securitate.
    c) Setarea parolei de blocare a ecranului telefonului pentru a proteja accesul la datele și aplicațiile dvs.
    d) Deconectați-vă de la rețeaua publică wireless imediat după ce ați terminat de utilizat telefonul.

Răspuns:

28. Care este cea mai sigură metodă de a efectua o tranzacție bancară prin intermediul telefonului mobil dintr-o locație publică?
    a) Se poate realiza si prin intermediul conexiuni wireless publice.
    b) Prin intermediul unei conexiuni wireless private și criptate.
    c) Prin intermediul unei rețele 4G private.
    d) Prin utilizarea autentificării cu doi factori.
    e) Prin utilizarea unei conexiuni VPN.
    f) Prin utilizarea unui browser securizat care are capacitatea de a bloca conexiunile nesigure și vulnerabile.

Răspuns:

Ce informații ar trebui să furnizați atunci când faceți o tranzacție bancară prin intermediul telefonului mobil dintr-o locație publică?
a) Numărul cardului bancar, numele titularului și data expirării.
b) Parola cardului bancar și codul CVV.
c) Doar informațiile strict necesare pentru tranzacție, cum ar fi suma și numărul contului bancar.

Răspuns:

Ce ar trebui să faceți după finalizarea tranzacției bancare prin intermediul telefonului mobil dintr-o locație publică?
a) Să închideți imediat aplicația bancară și să vă deconectați de la rețeaua wireless.
b) Să păstrați telefonul mobil închis până când ajungeți la locul de muncă și vă conectați la rețeaua securizată a primăriei.

Răspuns:

Care dintre următoarele este cel mai important aspect de luat în considerare atunci când efectuați o tranzacție bancară prin intermediul telefonului mobil dintr-o locație publică?

a) Utilizarea aplicației puse la dispoziție de bancă pe telefonul mobil.

b) Criptarea datelor transmise.

Argumentați:

Răspuns:

29. Ce pericole pot apărea atunci când utilizați rețelele publice de internet, cum ar fi cele dintr-o cafenea, aeroport sau benzinărie?

a) Atacuri de tip phishing, unde utilizatorii sunt înșelați să dezvăluie informații personale sau financiare prin intermediul unor mesaje sau site-uri false.

b) Atacuri de tip malware, unde programe rău intenționate sunt descărcate pe dispozitivul utilizatorului fără acordul acestuia, pentru a-i fura datele sau pentru a-i prelua controlul.

c) Atacuri de tip denial-of-service (DoS), unde rețeaua este inundată cu trafic fals, ceea ce duce la blocarea serviciilor și la nefuncționarea rețelei.

d) Toate cele de mai sus.

Răspuns:

Ce măsuri de securitate puteți lua pentru a vă proteja în timp ce utilizați rețele publice de internet?

a) Utilizarea unei rețele VPN pentru a cripta datele transmise între dispozitivul dvs. și rețeaua publică.

b) Verificarea adresei web și a certificatului digital al site-ului pe care îl accesați pentru a evita site-urile false.

c) Actualizarea sistemului de operare și a aplicațiilor dvs. pentru a elimina vulnerabilitățile de securitate.

d) Toate cele de mai sus.

Răspuns:

Ce ar trebui să faceți dacă ați fost victima unui atac cibernetic în timp ce utilizați o rețea publică de internet?

a) Schimbați imediat parolele pentru toate conturile dvs. și verificați tranzacțiile financiare.

b) Deconectați-vă imediat de la rețea și opriți conexiunea de date a dispozitivului dvs.

c) Raportați incidentul companiei care gestionează rețeaua publică și contactați furnizorul dvs. de servicii de internet pentru a vă ajuta să vă protejați.

d) Toate cele de mai sus.

Răspuns:

Ce măsuri puteți lua pentru a vă proteja dispozitivul atunci când utilizați rețele publice de internet?

a) Dezactivați funcția de partajare a fișierelor și imprimantelor.

b) Schimbați setările de securitate ale rețelei Wi-Fi pentru a vă asigura că utilizatorii neautorizați nu pot accesa dispozitivul dvs.

c) Blocați funcția Bluetooth atunci când nu o utilizați.

d) Toate cele de mai sus.

Răspuns:

Care dintre următoarele ar putea fi semne ale unui atac cibernetic în timp ce utilizați o rețea publică de internet?

a) Dispozitivul dvs. funcționează încet sau se blochează în mod repetat.

b) Ați primit mesaje nesolicitate de pe site-uri web sau prin e-mail.

c) Aplicațiile dvs. sau sistemul de operare necesită actualizări de securitate frecvente.

d) Ați observat că fișierele sau datele dvs. personale lipsesc sau au fost modificate în mod neautorizat.

e) Toate variantele enumerate pot fi semne ale unui atac cibernetic în timp ce utilizați o rețea publică de internet.

Răspuns:

30. Imaginați-vă următorul scenariu: sunteți în aeroport și primiți un apel de la dl. primar care vă cere să faceți o tranzacție bancară urgentă. Pentru a face acest lucru, aveți nevoie să accesați contul dvs. de la distanță, dar nu aveți un laptop sau un dispozitiv mobil la îndemână. Însă ați observat că aeroportul oferă calculatoare publice pentru pasageri. Cum procedați?

Răspuns:

31. Ce sunt actualizările de securitate?
    a) Actualizări care îmbunătățesc performanța sistemului și protejează sistemul de atacuri cibernetice.
    b) Actualizări care repară vulnerabilitățile de securitate și protejează datele și sistemele împotriva accesului neautorizat.
    c) Actualizări care adaugă noi caracteristici în sistem pentru a proteja sistemul de atacuri cibernetice.

Răspuns:

Ce pot face actualizările de securitate?
a) Ele pot preveni atacuri cibernetice și alte forme de amenințări la adresa securității.
b) Ele pot proteja împotriva malware-ului și a altor programe software malițioase.
c) Toate cele de mai sus.

Răspuns:

Cum poate un utilizator să verifice dacă sistemul său este actualizat pentru securitate?
a) Verificând manual actualizările disponibile.
b) Configurând sistemul pentru a se actualiza automat.
c) Verificând log-urile de sistem.

Răspuns:

32. Ce este criptarea?
    a) Un proces de transformare a datelor într-o formă ilizibilă pentru persoanele care nu au permisiunea să acceseze acele date.
    b) Un proces de transformare a datelor într-o formă cu caractere cunoscute doar de către cei care corespondează.
    c) Un proces de transfer securizat al datelor între dispozitive.

Răspuns:

Ce este o cheie de criptare?
a) O serie de caractere folosită pentru a converti datele într-o formă criptată.
b) O serie de caractere folosită pentru a converti datele înapoi în forma lor originală.
c) O serie de caractere folosită pentru a transfera datele între dispozitive.

Răspuns:

33. Cum pot fi backdoor-urile utilizate de hackeri?
    a) Pentru a obține acces neautorizat la un sistem sau la datele stocate pe acel sistem.
    b) Pentru a bloca sistemul.
    c) Pentru a folosi sistemul pentru DDoS.

Răspuns:

34. Cine creează de obicei backdoor-uri?
    a) Dezvoltatorii sau administratorii de sistem.
    b) Utilizatorii obișnuiți ai sistemului.
    c) Hackerii.

Răspuns:

Cum se pot proteja sistemele împotriva backdoor-urilor?
a) Prin utilizarea unor politici de securitate solide și prin monitorizarea accesului la sistem.
b) Prin instalarea de antivirus și firewall-uri pe sisteme.
c) Prin utilizarea de parole puternice și actualizarea sistemului la ultima versiune.

Răspuns:

35. Ce este un atac man-in-the-middle?
    a) Un atac în care un atacator interceptează și manipulează comunicarea între două părți care comunică direct.
    b) Un atac în care un atacator încearcă să intre în posesia parolelor utilizatorilor prin intermediul unui site web.
    c) Un atac în care un atacator încearcă să preia controlul asupra unui sistem prin utilizarea unei conexiuni nesigure.
    d) Toate cele de mai sus.

Răspuns:

Cum funcționează un atac man-in-the-middle?
a) Atacatorul interceptează și manipulează comunicarea între două părți care comunică direct, fără ca acestea să fie conștiente de acest lucru.
b) Atacatorul trimite un mesaj prin intermediul unui site web, încercând să obțină informații personale sau să preia controlul asupra unui sistem.
c) Atacatorul încearcă să intre în posesia parolelor utilizatorilor prin intermediul unui site web.
d) Toate cele de mai sus.

Răspuns:

Care sunt metodele prin care un atacator poate efectua un atac man-in-the-middle?
a) Atacatorul poate folosi o rețea WiFi publică nesecurizată, poate efectua un atac de tip phishing sau poate utiliza malware pentru a prelua controlul unui sistem.
b) Atacatorul poate efectua un atac prin intermediul unui site web, poate utiliza un exploit de securitate sau poate utiliza o conexiune nesecurizată.
c) Toate opțiunile de mai sus.

Răspuns:

Cum se pot proteja utilizatorii împotriva atacurilor man-in-the-middle?
a) Prin utilizarea unei conexiuni securizate, cum ar fi HTTPS sau VPN, și prin evitarea utilizării rețelelor WiFi publice nesecurizate.
b) Prin utilizarea de parole puternice și prin actualizarea sistemului la ultima versiune.
c) Prin monitorizarea accesului la sistem și prin utilizarea de soluții de securitate, cum ar fi antivirus și firewall-uri.
d) Toate cele de mai sus.

Răspuns:

36. Angajatul X lucrează într-un birou din primăria locală, unde operează cu o mulțime de informații confidențiale ale cetățenilor, inclusiv informații privind adresele de domiciliu, numere de telefon, numere de identificare personală și alte informații sensibile. Într-o zi, când se întoarce la birou după o pauză de prânz, constată că a lăsat calculatorul pornit și deblocat, iar un coleg este în birou și operează pe calculatorul său. Ce decizie ar trebui să ia angajatul X în această situație? Opțiuni de răspuns:
    a) Ignoră incidentul fiind o practică uzuală între colegi.
    b) Contactează imediat superiorii săi și informează despre incident.
    c) Încearcă să remedieze situația singur prin schimbarea parolei.

Răspuns:

37. Care este cel mai important motiv pentru a utiliza un password manager?
    a) Să păstrați o listă a tuturor parolelor pe care le folosiți.
    b) Să vă ajute să creați parole complexe și unice.
    c) Să vă protejați împotriva atacurilor de tip brute force.
    d) Să vă ajute să vă amintiți parolele.

Răspuns:

Ce trebuie să faceți înainte de a utiliza un password manager?
a) Să alegeți o parolă puternică pentru contul de email.
b) Să actualizați toate parolele folosite pentru conturile online.
c) Să instalați un program antivirus pe computer.
d) Să schimbați frecvent parolele.

Răspuns:

Cum funcționează un password manager?
a) Înregistrează și păstrează toate parolele într-un fișier text.
b) Criptează și stochează toate parolele într-un depozit securizat.
c) Generează parole complexe și unice pentru fiecare cont în parte.
d) Sincronizează parolele cu un server online.

Răspuns:

Ce beneficii obțineți prin utilizarea unui password manager?
a) Protejează parolele împotriva atacurilor de tip brute force.
b) Vă ajută să vă amintiți parolele.
c) Simplifică procesul de autentificare.
d) Toate cele de mai sus.

Răspuns:

Ce măsuri de securitate trebuie să luați în considerare când utilizați un password manager?
a) Actualizarea frecventă a parolelor.
b) Autentificarea cu o parolă master puternică.
c) Autentificarea cu o autentificare în doi pași.
d) Toate cele de mai sus.

Răspuns:

38. Ce este o parolă de deschidere în contextul unui document Office (ex. Word, Excel, Power Point)?

Răspuns:

Ce este o parolă de protecție în contextul unui document Office?

Răspuns:

Ce este o semnătură digitală și cum poate fi folosită pentru a proteja un document Office?

Răspuns:

Ce este o protecție cu permisiuni și cum poate fi folosită pentru a proteja un document Office?

Răspuns:

Ce este criptarea fișierelor și cum poate fi folosită pentru a proteja un document Office?

Răspuns:

39. Ce este un password manager?

Răspuns:

Care sunt avantajele utilizării unui password manager?

Răspuns:

Care este avantajul de a utiliza un password manager în comparație cu memorarea parolelor pe hârtie sau în minte?

Răspuns:

Cum poate un password manager să ajute la protejarea datelor personale?

Răspuns:

Ce informații ar trebui să fie stocate într-un password manager?

Răspuns:

Cum se poate accesa un password manager?

Răspuns:

Ce trebuie să faci pentru a începe să folosești un password manager?

Răspuns:

Care sunt caracteristicile de securitate importante pentru un password manager?

Răspuns:

Care este diferența dintre un password manager gratuit și unul plătit?

Răspuns:

Ce trebuie să faci dacă îți uiți parola de la password manager?

Răspuns:

Care sunt cele mai bune practici pentru utilizarea unui password manager?

Răspuns:

Cum poate un atacator să obțină parolele tale și cum te poate ajuta un password manager să eviți acest lucru?

Răspuns:

40. Care este cea mai importantă parolă de protejat cu un password manager?

Răspuns:

Ce se întâmplă dacă uitați parola de master pentru un password manager?

Răspuns:

Cum trebuie să vă gestionați parolele și conturile atunci când folosiți un password manager?

Răspuns:

41. Unde sunt salvate parolele atunci când le introduceți pe site-uri web?
    a) Pe serverele web
    b) Pe dispozitivul dvs. personal
    c) Pe serverele companiei producătoare a aplicației

Răspuns:

42. Dorim sa intram într-o aplicație pe web iar sistemul ne cere sa cream un cont sau sa intram cu contul nostru de Google sau Facebook deja creat. Ce se întâmplă cu datele noastre dacă intrăm cu contul de Google sau Facebook? Este acest lucru o formă de atac cibernetic sau nu?

Răspuns:

43. Pentru a vă proteja informațiile personale și financiare atunci când folosiți un calculator sau un dispozitiv mobil public, ce ar trebui să faceți?

Răspuns:

44. Ce informații personale ar trebui să evitați să postați pe rețelele sociale?

Răspuns:

Ce setări de confidențialitate ar trebui să verificați și să modificați pe contul dvs. de rețea socială pentru a proteja datele personale?

Răspuns:

Ce trebuie să faceți dacă observați activități suspecte pe contul dvs. de rețea socială sau dacă bănuiți că ați fost hackuit?

Răspuns:

Cum puteți evita trimiterea de informații personale și confidențiale către persoane necunoscute pe rețelele sociale, cum ar fi phishing-ul și scam-urile?

Răspuns:

45. Ce este un atac cu ransomware?

Răspuns:

Cum poate fi livrat un atac cu ransomware?

Răspuns:

Cum funcționează atacul cu ransomware?

Răspuns:

Ce se întâmplă cu fișierele infectate de ransomware?

Răspuns:

Cum pot fi protejate sistemele și fișierele împotriva atacurilor cu ransomware?

Răspuns:

Ce trebuie să faceți dacă sunteți victima unui atac cu ransomware?

Răspuns:

Ce sunt backup-urile și de ce sunt importante în lupta împotriva atacurilor cu ransomware?

Răspuns:

Ce măsuri de securitate suplimentare pot fi luate pentru a preveni atacurile cu ransomware?

Răspuns:

46. Într-o zi, angajatul deschide calculatorul și observă că majoritatea fișierelor sale personale, precum documente Word, prezentări PowerPoint și imagini, nu mai sunt accesibile. În plus, a găsit un fișier text pe desktop cu un mesaj care cere o sumă de bani în schimbul deblocării fișierelor. Ce credeți că s-a întâmplat?
    a. Calculatorul a fost infectat cu un virus care a criptat fișierele și cere o răscumpărare în schimbul lor.
    b. Calculatorul a fost spart și un hacker a preluat controlul asupra acestuia.

Răspuns:

47. Care sunt semnele de avertizare că un site web ar putea fi fals?

Răspuns:

Ce măsuri suplimentare de protecție puteți lua pentru a vă proteja împotriva site-urilor web false?

Răspuns:

48. Cum puteți verifica autenticitatea unui site web de pe care faceți cumpărături online?

Răspuns:

49. Ce trebuie să faceți dacă sunteți îndrumat să faceți o plată prin intermediul unui site web de ecommerce?

Răspuns:

50. Ați primit un e-mail care pretinde că este de la o bancă din România și vă informează că trebuie să vă actualizați informațiile personale pentru a continua să utilizați serviciile online ale băncii. E-mailul conține un link către o pagină web unde trebuie să introduceți informațiile personale și de cont bancar.
    Ce ar trebui să faceți în această situație?

Răspuns:

Ce informații ar trebui să furnizați vreodată pe un site web care vă solicită să introduceți informații financiare?

Răspuns:

Cum puteți verifica dacă un site web este legitim și nu este o pagină falsă?

Răspuns:

Ce ar trebui să faceți dacă ați furnizat informații financiare pe un site web fals?

Răspuns:

51. Sunteți în căutarea unui laptop nou și găsiți un site de ecommerce care pare să aibă prețuri incredibil de mici și oferte exclusive.
    Ce ar trebui să faceți înainte de a face o tranzacție financiară prin intermediul site-ului de ecommerce?

Răspuns:

Ce ar trebui să verificați pentru a vă asigura că site-ul de ecommerce este legitim?

Răspuns:

Ce trebuie să faceți dacă sunteți înșelați de un site de ecommerce fals și pierdeți bani?

Răspuns:

52. Sunteți în căutarea unui produs pe un site de ecommerce. Ați găsit un site care pare să aibă prețuri bune și produse de calitate. Vreți să faceți o achiziție, dar sunteți îngrijorat cu privire la siguranța tranzacției. Ce trebuie să verificați pentru a vă asigura că site-ul web este securizat?

Răspuns:

Care este cel mai sigur mod de plată pe un site de ecommerce?

a) Transfer bancar

b) Plata cu cardul de credit/debit

c) Plata prin intermediul unui serviciu de plată, cum ar fi PayPal

Răspuns:

Ce trebuie să faceți dacă sunteți redirecționat către o altă pagină de plată în timpul tranzacției?

Răspuns:

53. Primăria furnizează laptopuri angajaților săi pentru a facilita munca la distanță și pentru a le permite să lucreze de acasă. Cu toate acestea, angajații folosesc aceste laptopuri personale și pentru activități de navigare pe internet și de descărcare a fișierelor personale. Acest lucru creează o vulnerabilitate de securitate care poate fi exploatată de către hackeri. Scenariu: Angajatul Y a descărcat un fișier aparent inofensiv de pe un site web necunoscut și a deschis fișierul în laptopul său de serviciu. În acest fișier a fost încorporat un malware care poate permite atacatorilor să obțină acces la toate datele de pe laptopul respectiv.
Ce măsuri de securitate ar trebui să fie luate de către angajatul Y pentru a evita astfel de situații?

Răspuns:

Ce măsuri ar trebui luate de către primărie pentru a preveni astfel de situații?

Răspuns:

54. Ce este un atac brute-force?

a) Un atac prin care un hacker încearcă să ghicească parola prin încercarea repetată a diferitelor combinații de caractere.

b) Un atac prin care un hacker încearcă să convingă utilizatorii să dezvăluie informații personale prin intermediul unor mesaje false.

c) Un atac prin care un hacker interceptează comunicațiile dintre un server și un client pentru a accesa datele personale.

Răspuns:

Cum puteți să vă protejați împotriva atacurilor brute-force?

Răspuns:

Cum puteți să vă gestionați și să vă organizați parolele într-un mod sigur și eficient pentru a vă proteja împotriva atacurilor brute-force?

Răspuns:

55. Atunci când un utilizator accesează un site web securizat cu un certificat SSL, browserul acestuia verifică dacă certificatul este autentic și dacă a fost emis de o autoritate de încredere. Cum știți dacă site-ul web este sau nu este securizat cu certificate SSL?

Răspuns:

56. Cum poate un operator obișnuit să prevină vulnerabilitățile rețelei în ceea ce privește utilizarea unei multifuncționale (copiator) conectate la Internet?

Răspuns:

57. Care este prima acțiune pe care trebuie să o faceți pentru a verifica dacă aveți instalat un antivirus pe calculator?

a) Deschideți un browser web

b) Accesați panoul de control

c) Porniți calculatorul

Răspuns:

Cum se numește programul care poate detecta și elimina amenințările de securitate pe calculatorul dvs.?

a) Firewall

b) Antivirus

c) Antispam

Răspuns:

Cum puteți verifica dacă antivirusul dvs. este la zi?
a) Accesați site-ul web al producătorului antivirusului și verificați ultima versiune disponibilă
b) Verificați data ultimei actualizări din antivirusul dvs.
c) Nu trebuie să verificați, antivirusul se actualizează automat

Răspuns:

Care dintre următoarele acțiuni pot duce la dezactivarea antivirusului?
a) Descărcarea și instalarea unui software nesigur
b) Accesarea unui site web infectat
c) Folosirea unui cablu de alimentare defect

Răspuns:

Ce trebuie să faceți dacă observați că antivirusul dvs. este dezactivat sau nu funcționează corect?
a) Reinstalați antivirusul
c) Reporniți calculatorul și verificați din nou antivirusul

Răspuns:

58. Poate un antivirus să ne protejeze de toate atacurile cibernetice? Dacă da, de ce? Dacă nu, unde apar vulnerabilitățile? Dacă nu, ce ar mai trebui adăugat?

Răspuns:

59. Un antivirus actualizat cu cele mai recente semnături de virus și amenințări cibernetice ne protejează de toate atacurile cibernetice care vin pe calea internetului, cum ar fi spargerea parolei? Justificați răspunsul.

Răspuns:

60. Daca pe calculator aveți instalat sistemul de operare Windows sunteți sau nu vulnerabil la atacuri cibernetice din exterior, prin Internet? Dar dacă folosiți sistemul de operare Linux?

Răspuns:

61. Cum puteți să vă protejați împotriva spam-ului și a mesajelor nesolicitate?

Răspuns:

62. Ce este si cum puteți să vă protejați de identitatea falsă online?

Răspuns:

63. Cum puteți ști că este vorba despre o identitate falsă pe rețeaua Facebook sau altă rețea socială?

Răspuns:

64. La birou utilizezi camera web, căști și microfon pentru video-conferințe. Ești sau nu vulnerabil la atacuri cibernetice? Dacă da, ce tipuri de vulnerabilități există?

Răspuns:

65. Cum poți ști dacă camera web de la calculator sau conectată la calculator este deja preluată în control de către hackeri?

Răspuns:

66. Cum poți ști dacă hackerii au preluat controlul asupra boxelor tale, căștilor tale, care sunt legate la computer și de acolo ascultă ce se întâmplă în birou?

Răspuns:

67. Cum poți să te protejezi împotriva preluării controlului camerei web, a căștilor și difuzoarelor de către hackeri?

Răspuns:

68. În calitate de simplu angajat într-o Primărie, sunteți obligat să fiți informat asupra unor statistici de atacuri cibernetice monitorizate de către departamentul de specialitate sau de către furnizorii de servicii IT, sau nu?

Răspuns:

69. Cum poate fi introdus un dispozitiv de atac cibernetic în Primărie cu concursul indirect al dvs.? La ce trebuie să fiți atent în acest sens ca angajat în Primărie?

Răspuns:

70. Cum poate fi folosit un atac cu semnal sonor (Sonic sau Acoustic attack) pentru a compromite securitatea cibernetică a Primăriei? Ce poate face un angajat obișnuit pentru a minimiza acest risc?

Răspuns:

EVALUAREA CUNOȘTINȚELOR REFERITOARE LA REGULAMENTUL GDPR

Durata: 2 ore

1. Ce înseamnă GDPR?

2. Care este obiectivul principal al GDPR?

3. Cine este responsabil de implementarea GDPR într-o organizație?

4. Ce este un drept al persoanei vizate în conformitate cu GDPR?

5. Care este vârsta minimă la care o persoană poate oferi consimțământul său în conformitate cu GDPR?

6. Ce este un consimțământ valabil în conformitate cu GDPR?

7. Care sunt principalele informații care trebuie incluse într-o declarație de confidențialitate?

8. Ce este un Ofițer de Protecție a Datelor și când este necesară numirea unuia?

9. Care sunt principalele drepturi ale persoanelor vizate conform GDPR?

10. Ce înseamnă "date cu caracter personal" conform GDPR?

11. Care sunt principalele categorii de date cu caracter personal?

12. Care sunt principalele motive pentru care o organizație poate colecta și prelucra date cu caracter personal?

13. Ce înseamnă "procesare" în contextul GDPR?

14. Ce este o evaluare a impactului asupra protecției datelor și când este necesară?

15. Care sunt principalele măsuri de securitate care trebuie luate pentru protejarea datelor cu caracter personal?

16. Ce este notificarea unei încălcări a securității datelor și când trebuie făcută?

17. Ce este o cerere de acces a persoanei vizate și cum trebuie gestionată?

18. Ce sunt datele sensibile și cum trebuie protejate conform GDPR?

19. Care sunt principalele obligații ale operatorilor de date conform GDPR?

20. Ce este un transfer de date în afara UE și cum este reglementat de GDPR?

21. Ce este un consimțământ clar și afirmativ conform GDPR?

22. Ce este un registru de prelucrare a datelor și când trebuie creat?

23. Ce sunt regulile privind portabilitatea datelor și când se aplică?

24. Care sunt principalele măsuri de securitate fizică care trebuie luate pentru protejarea datelor cu caracter personal?

25. Ce este confidențialitatea și cum trebuie protejată conform GDPR?

26. Ce este un transfer internațional de date și cum este reglementat de GDPR?

27. Ce sunt regulile privind durata stocării datelor și când se aplică?

28. Ce este un acord de procesare a datelor și când este necesar?

29. Ce este un registru de activități de prelucrare și ce informații trebuie să conțină?

30. Ce este un raport de evaluare a impactului asupra protecției datelor și când trebuie realizat?

31. Situație: Un cetățean vă cere să ștergeți toate datele personale pe care le aveți despre el în conformitate cu GDPR. Ce trebuie să faceți?
    a) Respingeți cererea cetățeanului și păstrați datele pentru a le utiliza mai târziu.
    b) Ștergeți toate datele personale ale cetățeanului.
    c) Întârziați răspunsul până când puteți determina dacă aveți dreptul să păstrați datele sau nu.

32. Situație: Un angajat primește o cerere de la un cetățean care solicită accesul la datele sale personale. Ce trebuie să facă angajatul?
    a) Ignoră cererea deoarece aceasta nu a fost adresată în mod direct Primăriei.
    b) Răspunde la cerere și furnizează datele personale solicitate în termen de 30 de zile.
    c) Întârzie răspunsul până când poate determina dacă are sau nu dreptul să furnizeze datele.

33. Situație: Un angajat primește un e-mail care conține informații cu caracter personal despre un cetățean. Ce trebuie să facă angajatul?
    a) Ignoră e-mailul și nu face nimic.
    b) Păstrează informațiile în e-mail pentru referințe viitoare.
    c) Șterge informațiile din e-mail și se asigură că nu sunt stocate în altă parte.

34. Situație: Un cetățean dorește să-și modifice adresa de e-mail în baza de date a Primăriei. Ce trebuie să facă angajatul?
    a) Acceptă cererea și actualizează baza de date a Primăriei.
    b) Refuză cererea deoarece adresa de e-mail a cetățeanului este utilizată într-un sistem de automatizare.
    c) Întârzie răspunsul până când poate determina dacă poate actualiza baza de date.

35. Situație: Un angajat observă că sistemul de securitate al calculatorului a fost compromis. Ce trebuie să facă angajatul?
    a) Anunță imediat departamentul de IT sau responsabilul de securitate cibernetică al Primăriei.
    b) Întârzie notificarea, mai întâi verifică dacă fișierele cu datele personale au fost compromise.

36. Situație: Primăria dorește să utilizeze datele personale ale cetățenilor pentru a le trimite informații personalizate, cum ar fi newsletter-uri. Ce trebuie să facă Primăria?
    a) Întreabă fiecare cetățean individual dacă este de acord cu utilizarea datelor sale personale.
    b) Furnizează o notificare clară cetățenilor privind utilizarea datelor lor personale și oferă opțiunea de dezabonare.
    c) Utilizează datele fără a solicita consimțământul cetățenilor.

37. Situație: Un cetățean român solicită să-și transfere datele personale la o altă Primărie din Elveția, unde urmează să se mute. Ce trebuie să facă Primăria?
    a) Refuză cererea deoarece datele personale nu pot fi transferate în afara UE.
    b) Furnizează datele personale solicitate într-un format ușor de utilizat și transferat către Primăria dorită de cetățean.
    c) Întârzie răspunsul până când poate determina dacă transferul datelor este permis.

38. Situație: Un angajat primește un e-mail care pare să fie de la o persoană de încredere și solicită să-i fie furnizate informații confidențiale. Ce trebuie să facă angajatul?
    a) Furnizează informațiile solicitate.
    b) Verifică autenticitatea e-mailului și solicită verificarea cererii.
    c) Ignoră cererea și nu furnizează informațiile.

39. Situație: Un cetățean dorește să știe cum sunt stocate și protejate datele lor personale în baza de date a Primăriei. Ce trebuie să facă Primăria?
    a) Refuză cererea deoarece este prea complexă.

b) Furnizează o descriere clară și detaliată a modului în care sunt stocate și protejate datele personale ale cetățeanului.
c) Întârzie răspunsul până când poate determina dacă poate furniza aceste informații.

40. Situație: Un angajat primește un e-mail cu un link către un site web care pare a fi suspect. Ce trebuie să facă angajatul?
a) Accesează linkul și investighează site-ul.
b) Ignoră e-mailul și îl șterge.
c) Raportează e-mailul departamentului de IT sau responsabilului de securitate cibernetică.

41. Situație: Primăria dorește să utilizeze datele personale ale cetățenilor pentru a dezvolta un serviciu nou, în cadrul unei platforme digitale bazate pe inteligență artificială. Ce trebuie să facă Primăria?
a) Întreabă fiecare cetățean individual dacă este de acord cu utilizarea datelor sale personale în acest scop.
b) Furnizează o notificare clară și transparentă cetățenilor privind utilizarea datelor lor personale și oferă opțiunea de respingere.
c) Utilizează datele fără a solicita consimțământul cetățenilor.

42. Situație: Un client dorește să primească o copie a datelor personale pe care le deține compania. Ce trebuie să facă compania?
a) Refuză cererea deoarece datele personale nu pot fi furnizate în format electronic.
b) Furnizează datele personale solicitate într-un format ușor de utilizat și transferat către client.
c) Întârzie răspunsul până când poate determina dacă poate furniza datele solicitate.

43. Situație: Un angajat utilizează calculatorul de la birou pentru a accesa site-uri web personale și pentru a comunica cu prietenii. Este acest lucru permis conform GDPR?
a) Da, angajatul are dreptul la confidențialitate în utilizarea computerului de la birou.
b) Nu, utilizarea computerului de la birou este strict pentru activități legate de serviciu.
c) Depinde de politicile interne ale companiei.

44. Situație: Un client solicită să i se explice în detaliu cum sunt colectate și utilizate datele lor personale. Ce trebuie să facă compania?
a) Refuză cererea deoarece este prea complexă.
b) Furnizează o notificare clară și transparentă clienților privind utilizarea datelor lor personale.
c) Întârzie răspunsul până când poate determina dacă poate furniza aceste informații.

45. Situație: O companie dorește să dezvolte o aplicație mobilă care să colecteze date personale ale utilizatorilor. Ce trebuie să facă compania?
a) Să colecteze datele fără a solicita consimțământul utilizatorilor.
b) Să solicite consimțământul explicit al utilizatorilor înainte de a colecta datele lor personale.
c) Să solicite consimțământul implicit al utilizatorilor prin intermediul politicii de confidențialitate a aplicației.

46. Situație: Un angajat primește un e-mail de la un client care solicită să fie șters din baza de date a companiei. Ce trebuie să facă angajatul?
a) Ignoră e-mailul și nu face nimic.
b) Întârzie răspunsul până când poate determina dacă cererea este validă.
c) Șterge informațiile despre client din baza de date a companiei.

47. Situație: Un client UE solicită să-și actualizeze informațiile personale în baza de date a companiei. Ce trebuie să facă compania?
a) Refuză cererea deoarece datele personale nu pot fi modificate.

b) Actualizează informațiile personale solicitate în baza de date a companiei.
c) Întârzie răspunsul până când poate determina dacă modificarea datelor este permisă.

48. Situație: O companie utilizează un serviciu de cloud computing pentru a stoca date personale ale clienților. Ce trebuie să facă compania?
a) Să nu utilizeze servicii de cloud computing pentru a stoca date personale.
b) Să verifice politicile de securitate ale serviciului de cloud computing și să se asigure că sunt conforme cu GDPR.
c) Să nu comunice nicio informație despre clienți prin intermediul serviciului de cloud computing.

49. Situație: Un angajat primește un e-mail de la un coleg care solicită să-i fie furnizate informații confidențiale. Ce trebuie să facă angajatul?
a) Furnizează informațiile solicitate.
b) Verifică autenticitatea e-mailului și solicită verificarea cererii.
c) Ignore cererea și nu furnizează informațiile.

50. Situație: Un client solicită să-și transfere datele personale la o altă companie. Ce trebuie să facă compania?
a) Refuză cererea deoarece datele personale sunt proprietatea companiei.
b) Furnizează datele personale solicitate într-un format ușor de utilizat și transferat către client.
c) Întârzie răspunsul până când poate determina dacă transferul datelor este permis.

51. Primăria colectează date personale în cadrul unui sistem de înregistrare a cererilor cetățenilor. Ce trebuie să facă Primăria pentru a se asigura că datele personale sunt protejate conform GDPR?

52. Primăria utilizează camere de supraveghere pentru a monitoriza clădirile și spațiile publice. Ce trebuie să facă Primăria pentru a se asigura că activitatea de supraveghere respectă prevederile GDPR?

53. Primăria angajează o companie terță pentru a procesa date personale în numele său. Ce trebuie să facă Primăria pentru a se asigura că compania terță respectă prevederile GDPR?

54. Primăria colectează date personale în scopul distribuirii de știri și informații despre evenimente publice. Ce trebuie să facă Primăria pentru a se asigura că colectarea și utilizarea datelor personale respectă prevederile GDPR?

55. Primăria organizează online un concurs de proiecte de dezvoltare locală în care participanții trebuie să ofere informații personale pentru a se înregistra. Ce trebuie să facă Primăria pentru a se asigura că informațiile personale sunt protejate și procesate conform GDPR?

56. Primăria utilizează servicii de cloud computing pentru a stoca date personale ale cetățenilor. Ce trebuie să facă Primăria pentru a se asigura că datele personale sunt protejate și procesate conform GDPR?

57. Un angajat al Primăriei primește un e-mail de la un coleg, cerând date personale ale unui cetățean. Ce trebuie să facă angajatul?

58. Primăria utilizează cookie-uri pe site-ul său web. Ce trebuie să facă Primăria pentru a se asigura că utilizarea cookie-urilor este conformă cu prevederile GDPR?

59. Angajatul Maria primește o notificare de la sistemul de securitate al Primăriei, care indică faptul că un cont de utilizator neautorizat a încercat să acceseze baza de date a Primăriei. În același timp, Ion observă că un computer al unui coleg de la alt departament este utilizat pentru a accesa informații confidențiale despre clienții Primăriei.
    Întrebări:
    Care sunt semnele unui posibil acces neautorizat la date personale?

    Ce măsuri trebuie luate pentru a preveni accesul neautorizat la date personale?

    Cum poate Primăria proteja datele personale și informațiile confidențiale împotriva accesului neautorizat?

60. Primăria trebuie să se conformeze cu prevederile GDPR pentru a proteja datele personale ale cetățenilor. Angajații trebuie să dezvolte un plan de acțiune pentru a se asigura că Primăria respectă toate prevederile GDPR și că este pregătită să răspundă la cererile cetățenilor. Ce informații ați furnizat dvs. Ofițerului cu Protecția Datelor din Primărie pentru a fi sigur că Primăria se conformează cu prevederile GDPR și cum aplicați dvs. strict regulamentul GDPR în activitatea de zi-cu-zi?

FISA DE PROIECT FANION

Titlu

Implementare Centru de date modular

Coordonator din partea consultantului

Bogdan CIOTLAUS

Rezumat

1. Scop

Scopul proiectului de față este design-ul unui centru de date caracterizat de redundanță, flexibilitate și scalabilitate care să ofere infrastructura IT capabilă să susțină obiectivele și proiectele derivate din strategia de digitalizare a Primăriei Bistrița.

Proiectul va fi fundamentat pe analiza detaliată a situației curente la nivelul infrastructurii IT a Primăriei Bistrița, a riscurilor sistemice, a categoriilor principale de nevoi dictate de digitalizare în domeniul infrastructurii IT. În elaborarea proiectului va fi prioritizat principiul maximizării libertății instituției de a adopta o paletă largă de inițiative de digitalizare.

2. Obiective

Obiectivele pe termen lung ale prezentului proiect sunt:

1. Crearea unei infrastructuri scalabile și redundante, capabile să susțină o paletă cât largă de scenarii de digitalizare a instituției
2. Creșterea capacității instituționale de a planifica, opera și gestiona resurse critice pentru infrastructura IT în condiții de transparență și predictibilitate
3. Creșterea sustenabilității infrastructurii IT prin monitorizarea și minimizarea amprentei energetice, ecologice și economice
4. Simplificarea și eficientizarea mentenabilității infrastructurii IT a instituției

Obiectivele pe termen scurt ale prezentului proiect sunt:

1. Crearea unei abordări fundamentate pe o analiză detaliată a situației curente, a riscurilor sistemice, a categoriilor principale de nevoi dictate de procesele de digitalizare în domeniul infrastructurii IT
2. Crearea premiselor pentru spațiu fizic securizat
3. Crearea unui mediu fizic optimizat pentru găzduirea echipamentelor de comunicații, stocare și procesare

3. Beneficiari

Beneficiarii acestui proiect pot fi împărțiți în două categorii: beneficiari direcți și indirecți. Beneficiarii direcți ai acestui proiect sunt instituția Primăriei, managementul și angajații acesteia. Beneficiarii indirecți sunt reprezentați de cetățenii din comunitate și organizații terțe care oferă servicii digitalizate (sau cu componente digitalizate) către cetățeni.

4. Rezultate așteptate

- Securizare fizică a componentelor esențiale ale infrastructurii IT
- Crearea unui mediu fizic adecvat pentru operarea componentelor esențiale ale infrastructurii IT ale Primăriei
- Creșterea cu câteva ordine de magnitudine a rezilienței în caz de dezastru prin crearea de redundanțe esențiale, proceduri menite să crească continuitatea operațională a instituției
- Creșterea predictibilității și transparenței în planificarea, operarea și gestionarea resurselor critice pentru infrastructura IT
- Creșterea flexibilității și scalabilității proceselor organizaționale prin crearea de sisteme capabile să opereze în model „in house", model de servicii externalizate sau orice combinație între acestea
- Creșterea gradului de mentenabilitate a întregii infrastructuri IT și reducerea concomitentă a resurselor dedicate pentru aceasta
- Creșterea încrederii cetățenilor în capacitatea instituției de face față provocărilor exigențelor procesului de digitalizare

I. Context & Justificare

Primăria Bistrița are nevoie de o infrastructură IT capabilă să susțină o organizației digitalizată robust, ale cărei componentă structurală și organizațională fundamentală este un centrul de date caracterizat de:

- integrare
- redundanță
- scalabilitate
- securitate
- flexibilitate
- mentenabilitate facilă

Situația prezentă a infrastructurii IT prezintă carențe și riscuri semnificative pe toate dimensiunile menționate și, în consecință, nu poate asigura capacitățile și funcționalitățile necesare pentru a susține majoritatea scenariilor de digitalizare robustă propuse.

Implementarea prezentului proiect se justifică prin necesitate de a elimina riscuri sistemice ale infrastructurii IT, de a asigura un nivel de securitate și funcționalitate capabil să susțină multiple scenarii potențiale de digitalizare.

Probleme

Din analiza datelor preliminare rezultă carențe semnificative pe următoarele dimensiuni:

- Caracteristici fizice suboptime ale spațiului care găzduiește componentele esențiale ale infrastructurii IT ale instituției
- Lipsă acces adecvat, dar și partajat pentru furnizorii de conectivitate
- Controlul adecvat și monitorizat al accesului fizic și funcțional la componentele esențiale ale infrastructurii IT ale instituției
- Redundanță sistemică redusă a componentelor esențiale ale infrastructurii IT ale instituției
- Integrare redusă a resurselor IT puse la dispoziția instituției
- Capacitate redusă de monitorizare și întreținere registre (logs) separate și accesibile de la distanță pentru componentele esențiale ale infrastructurii IT ale instituției
- Capacitate redusă de identificare, înregistrare și monitorizare echipamente, active, resurse pe întreaga durată a ciclului lor de viață.
- Capacitate redusă de înregistrare și monitorizarea și gestionare a modificărilor la nivel de echipamente, resurse, sisteme sau proceduri de lucru.
- Sisteme de procesare si stocare date uzate din punct de vedere tehnic si fara suport de la furnizori.

Oportunități

- Reziliența în caz de dezastru (redundanțe sistemice și securizarea infrastructurii IT & de suport)
- Capacitate de scalare facilă a infrastructurii în funcție de nevoie și predictibilitate a costurilor și direcțiilor de dezvoltare
- Creșterea trasabilității proceselor și a transparenței decizionale: de la achiziții, la administrare, la dezvoltare programatică
- Flexibilitate organizațională, manifestată în abilitatea de a pute funcționa și/sau trece cu ușurință de la un model in house la un model hibrid în care în care o parte din servicii sunt externalizate la terți

Soluții la nevoi identificate

- Identificarea și adoptarea de standarde adecvate la nivel tehnic, funcțional și management pentru infrastructura IT & de suport

- Implementare programatică a redundanțelor în infrastructura IT & de suport în vederea eliminării punctelor unice de eroare (i.e. single point of failure) cu scopul de a crește reziliența și mentenabilitatea de ansamblu a infrastructurii IT
- Implementare sisteme de monitorizare în timp real, jurnalizare incidente și sistem de alertare programabil al tuturor componentelor de infrastructură IT sau de suport
- Implementare sistemelor de acces securizat de la distanță pentru toate componentele de infrastructură IT sau infrastructură de suport
- Standardizare, integrare și centralizare comunicații critice pentru infrastructura IT
- Prioritizarea arhitecturilor modulare de tip „plug-and-play"
- Prioritizarea infrastructură capabilă să susțină sisteme flexibile și scalabile de tip multi-tenant
- Soluții de securizare modulară a infrastructurii IT și a dispozitivelor utilizatorilor dependente de această infrastructură
- Definire și automatizare procese legate de infrastructura IT în vederea minimizării resurselor umane necesare pentru operarea și mentenanța infrastructurii; creșterea capacității de externalizare modulară a proceselor de administrare și mentenanță a infrastructurii IT.

II. Obiective & Rezultate

Obiective termen lung

1. Crearea unei infrastructuri scalabile și redundante, capabile să susțină o paletă cât largă de scenarii de digitalizare a instituției
2. Creșterea capacității instituționale de a planifica, opera și gestiona resurse critice pentru infrastructura IT în condiții de transparență și predictibilitate
3. Creșterea sustenabilității infrastructurii IT prin monitorizarea și minimizarea amprentei energetice, ecologice și economice
4. Simplificarea și eficientizarea mentenabilității infrastructurii IT a instituției

Obiective termen scurt

1. Crearea unei abordări a strategiei infrastructurii IT fundamentate pe o analiză detaliată a situației curente, a riscurilor sistemice, a categoriilor principale de nevoi dictate de procesele de digitalizare în domeniul infrastructurii IT
2. Crearea premiselor pentru spațiu fizic securizat
3. Crearea unui mediu fizic optimizat pentru găzduirea echipamentelor de comunicații, stocare și procesare

Măsurarea & evaluarea obiectivelor

A. Raport audit detaliat a situației curente, a riscurilor sistemice, a categoriilor principale de nevoi dictate de procesele de digitalizare în domeniul infrastructurii IT
B. Spațiu fizic alocat centrului de date al Primăriei Bistrița securizat conform standardelor: ECB-S sau echivent, Uptime Institute Tier3 sau echivalent
C. Mediul fizic și ambiental optimizat pentru găzduirea echipamentelor de comunicații, stocare și procesare, conform standardelor: ECB-S sau echivent, Uptime Institute Tier3 sau echivalent
D. Infrastructură redundantă, conform standardelor ...
E. Infrastructură scalabilă în care să existe rezervă disponibilă de 30%
F. Grad de monitorizare a infrastructurii IT și de suport de minim 90%
G. Clasă consum energetic conform uptime institute Tier III sau echivalent
H. Creșterea capacității instituționale de a planifica, opera și gestiona resurse critice pentru infrastructura IT în condiții de transparență și predictibilitate, conform Uptime Institute Tier III sau echivalent

I. Simplificarea și eficientizarea mentenabilității infrastructurii IT a instituției, conform Uptime Institute Tier III sau echivalent

Rezultate așteptate

- Securizare fizică a componentelor esențiale ale infrastructurii IT
- Mediu fizic adecvat pentru operarea componentelor esențiale ale infrastructurii IT ale Primăriei
- Reziliență crescută cu câteva ordine de magnitudine în caz de dezastru prin crearea de redundanțe esențiale, proceduri menite să crească continuitatea operațională a instituției
- Predictibilitate și transparență crescută în planificarea, achiziția, operarea și gestionarea resurselor critice pentru infrastructura IT
- Flexibilitate și scalabilitate crescută a proceselor organizaționale prin crearea de sisteme capabile să opereze în model „in house", model de servicii externalizate sau orice combinație între acestea
- Mentenabilitate crescută a întregii infrastructuri IT și reducerea concomitentă a resurselor dedicate pentru aceasta
- Încredere crescută a cetățenilor în capacitatea instituției de face față provocărilor exigențelor procesului de digitalizare

III. Plan de implementare

Activitățile principale

- Analiza detaliată a situației curente a infrastructurii IT și a infrastructurilor de suport, a sistemelor de management utilizate pentru gestionarea infrastructurii IT & de suport (politici, proceduri, resurse umane, mecanisme de jurnalizare & raportare) și a vulnerabilităților infrastructurii IT & de suport
- Analiza scenariilor de digitalizare și a implicațiilor acestora asupra caracteristicilor infrastructurii IT, infrastructuri de suport și sistemelor de management ale acestora; prezentarea rezultatelor analizei sub formă de raport cost/beneficiu pentru facilitarea procesului decizional al instituției Primăriei în vederea selectarea modelului preferat (i.e. „in house" vs „externalizare")
- Investiții în crearea / achiziționarea unui spațiu fizic adecvat, conform bunelor practici și recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate
- Investiții în crearea / achiziționarea sistemelor necesare implementării unui mediu fizic adecvat, conform bunelor practici și a recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate
- Investiții în crearea / achiziționarea sistemelor care formează infrastructura de suport adecvată, conform bunelor practici și a recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate
- Investiții în crearea / achiziționarea sistemelor de comunicații, procesare, stocare necesare implementării unui mediu fizic adecvat, conform bunelor practici și a recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate
- Investiții în dezvoltarea de politici, proceduri și protocoale pentru gestionarea infrastructurii de IT & suport
- Audit infrastructură IT, infrastructură suport, sisteme de management după faza de implementare

Responsabilități

Echipa responsabilă de proiect va fi formata din specialiști cu experiență în domeniul infrastructurilor IT, infrastructurilor de suport și sistemelor de management ale infrastructurilor IT & suport, de preferință în domeniul implementării și gestionării centrelor de date.

Primăria Bistrița va fi responsabila de supervizarea și coordonarea proiectului, asigurând o buna comunicare intre membrii echipei de proiect.

Durata proiectului

Durata estimată de implementare a proiectului se ridică la 18 -24 luni.

Nr	Activitate	Durata estimată
1	Analiza detaliată a situației curente a infrastructurii IT și a infrastructurilor de suport, a sistemelor de management utilizate pentru gestionarea infrastructurii IT & de suport (politici, proceduri, resurse umane, mecanisme de jurnalizare & raportare) și a vulnerabilităților infrastructurii IT & de suport	2 luni
2	Analiza scenariilor de digitalizare și a implicațiilor acestora asupra caracteristicilor infrastructurii IT, infrastructuri de suport și sistemelor de management ale acestora; prezentarea rezultatelor analizei sub formă de raport cost/beneficiu pentru facilitarea procesului decizional al instituției Primăriei în vederea selectarea modelului preferat (i.e. „in house" vs. „hibrid" vs. „externalizare")	2 luni

3	Investiții în crearea / achiziționarea unui spațiu fizic adecvat, conform bunelor practici și recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate	2 luni
4	Investiții în crearea / achiziționarea sistemelor necesare implementării unui mediu fizic adecvat, conform bunelor practici și a recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate	2 luni
5	Investiții în crearea / achiziționarea sistemelor care formează infrastructura de suport adecvată, conform bunelor practici și a recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate	4 luni
6	Investiții în crearea / achiziționarea sistemelor de comunicații, procesare, stocare necesare implementării unui mediu fizic adecvat, a unei platforme cloud interoperabila, conform bunelor practici și a recomandărilor din acest domeniu și care va face referință explicită la dimensiunile critice și criteriile de evaluare acceptate	8 luni
7	Investiții în dezvoltarea de politici, proceduri și protocoale pentru gestionarea infrastructurii de IT & suport	3 luni
8	Audit infrastructură IT, infrastructură suport, sisteme de management după faza de implementare	2 luni

IV. Sustenabilitate & impact

Finanțarea & Construcția bugetului

Construcția și valoarea totală a bugetului proiectului va fi proiectată pentru a putea varia în funcție de opțiunile strategice ale instituției Primăriei Bistrița, a priorităților proiectelor de digitalizare și a resurselor disponibile. Construcția bugetului va include următoarele categorii de costuri:

- Costuri legate de analiză, consultanță și audit
- Costuri legate de locația și caracteristicile spațiului / spațiilor fizice care vor găzdui componentele critice ale infrastructurii IT & de suport
- Costuri legate de sistemele infrastructurii de suport: control mediu, control acces, asigurarea și distribuția energiei, sisteme de protecție, sisteme de monitorizare etc.
- Costuri legate de sistemele infrastructurii IT: comunicații, procesare, stocare
- Costuri legate de training și formare resurse umane
- Costuri legate de dezvoltarea de sisteme de management: politici, proceduri, protocoale, jurnalizare, raportare

În funcție de specificul și dimensiunea proiectului, bugetul total poate varia între 1.200.000 și 2.400.000 de Euro. Este important să se realizeze o estimare detaliată a costurilor și o alocare corespunzătoare a resurselor pentru a asigura succesul proiectului și implementarea tuturor măsurilor necesare pentru protejarea, operarea eficientă și reziliența infrastructurii IT ca parte a strategiei instituționale de asigurarea a continuității activităților și recuperare în caz de dezastru.

Sustenabilitate

Sustenabilitatea proiectului va fi asigurată prin:

- Crearea unei infrastructuri IT scalabile și flexibile, capabilă să deservească o paletă largă de servicii digitalizate oferite de către Primăria Bistrița cetățenilor și/sau altor instituții
- Proiectarea unei infrastructuri IT eficiente din punct de vedere al consumului de resurse prin reducerea consumului de energie și creșterea gradului de monitorizare a proceselor interne
- Crearea unui sistem de management transparent, capabil de monitorizare și jurnalizare al tuturor aspectelor infrastructurii IT și ia decizii informate pentru investiții în tehnologii inteligente
- Implementarea unui program de educarea personalului în domeniul infrastructurii IT, pentru a asigura o infrastructura viabilă, rezilientă și securizată.
- Asigurarea unei bune coordonări și comunicări între membrii echipei de proiect și angajații Primăriei Bistrița, pentru a menține nivelul ridicat de implicare.
- Sensibilizarea și educarea cetățenilor în ceea ce privește valoarea unei infrastructuri IT securizate, flexibile și eficiente pentru o instituție publică.

Impact social, economic, mediu

Impactul social, economic și de mediu al proiectului va fi pozitiv și se va manifesta prin:

- Creșterea nivelului de disponibilitate și reziliență a infrastructurii IT & de suport din Primăria Bistrița în vederea furnizării de servicii digitalizate de calitate în condiții de securitate și confidențialitate informațională.
- Creșterea încrederii cetățenilor în capacitatea instituțională a Primăriei Bistrița de a oferi servicii digitale și impact pozitiv la dezvoltarea socioeconomica a comunității locale
- Reducerea costurilor și a timpului alocat pentru remedierea incidentelor legate de infrastructura IT.

- Creșterea eficienței și transparenței decizionale prin asigurarea unui cadru care să permită monitorizarea digitală a unei multitudini de parametri relevanți pentru instituția Primăriei
- Reducerea impactului asupra mediului prin creșterea eficientei și a siguranței infrastructurii IT, reducând astfel consumul de energie și emisiile de gaze cu efect de sera
- Creșterea globală a flexibilității instituționale.

V. Anexe

Fig. 1. Exemplu de centru de date de tip modular cu subsistemele sale

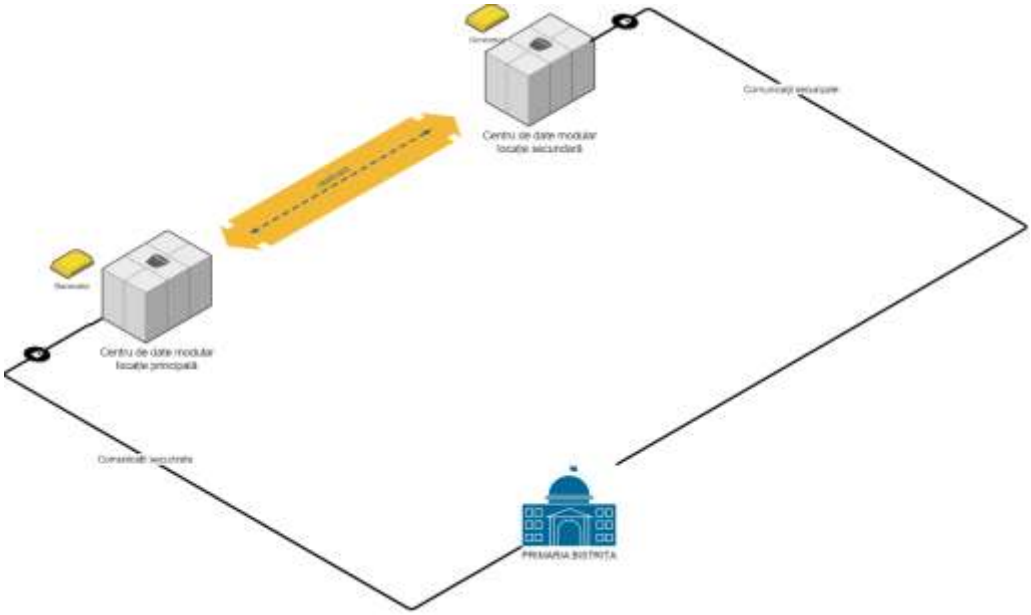


Fig. 2. Reprezentare grafică a schemei topologice pentru centre de date modulare propuse pentru Primăria Bistrița

FISA DE PROIECT FANION

Titlu

Implementare Dispecerat Central / Centru de Operațiuni Digitale pentru Primăria Bistrița

Coordonator din partea consultantului

Bogdan CIOTLAUS

Rezumat

Scop

Scopul proiectului de față este analiza design-ului și a implicațiilor legate de implementarea unui Centru de Operațiuni Digitale (COD) pentru primăria Bistrița. Centrul de Operațiuni Digitale poate fi conceptualizat ca o combinare și extindere a atribuțiilor tipice pentru un SOC (Security Operation Center), un NOC (Network Operation Center, cuplate cu capacități caracteristice unui APMC (Application Performance Monitoring Center) și unui BPMC (Business Process Monitoring Center).

Un COD are atribuțiuni în domeniul gestionării și monitorizării aspectelor digitale ale unei organizații, inclusiv securitate, operațiuni rețea, performanța aplicațiilor și procesele de digitalizare. Scopul acestei structuri este de a optimiza infrastructura digitală a organizației și de a asigura funcționarea optimă a serviciilor sale digitale.

Proiectul va fi fundamentat pe analiza detaliată a situației curente la nivelul proceselor Primăriei Bistrița, a riscurilor sistemice, a categoriilor principale de nevoi dictate de digitalizare. În elaborarea proiectului va fi prioritizat principiul maximizării libertății instituției de a adopta o paletă largă de inițiative de digitalizare.

Obiective

Obiectivele prezentului proiect sunt:

1. Definirea și crearea unei arhitecturi informatice integrate: design și planificare sistem scalabil și redundant, capabil să susțină o paletă cât largă de scenarii de digitalizare a instituției
2. Monitorizare centralizată: monitorizarea centralizată a aplicațiilor, infrastructurii IT, proceselor organizaționale și securității, facilitând gestionarea eficientă a acestora și reducând complexitatea operațională.
3. Detectarea și remedierea rapidă a problemelor: Prin monitorizarea în timp real și analiza datelor, creșterea ratei și vitezei de detecție a problemelor și incidentelor, remediere în timp util pentru a preveni reducerea performanței sistemului și experiență negativă pentru utilizatori.
4. Optimizarea performanței și eficienței: îmbunătățirea performanței aplicațiilor de bază și a eficienței proceselor interne prin analiza datelor și implementarea de îmbunătățiri continue.
5. Gestionarea riscurilor de securitate: monitorizarea și gestionarea riscurilor de securitate cibernetică într-un mod proactiv, protejând astfel instituția și informațiile sensibile ale acesteia.
6. Asigurarea conformității: respectarea reglementărilor și standardelor în vigoare prin implementarea unor politici și proceduri adecvate și monitorizarea lor.
7. Îmbunătățirea experienței utilizatorilor: monitorizarea performanței aplicațiilor și a proceselor organizaționale ajută la identificarea și soluționarea problemelor care afectează experiența utilizatorilor, conducând la o mai bună satisfacție a utilizatorilor (angajați, cetățeni, terți).
8. Accelerarea proceselor de luare a deciziilor: date și informații valoroase pentru luarea deciziilor bazate pe date, accelerând procesul de luare a deciziilor și îmbunătățind rezultatele organizației.
9. Colaborare îmbunătățită: colaborare facilă între echipele de IT, securitate, dezvoltare de aplicații și managementul proceselor interne; comunicare eficientă și o abordare coerentă a problemelor comune.
10. Reducerea costurilor operaționale: costuri operaționale reduse prin optimizarea resurselor IT, eliminarea redundanțelor și îmbunătățirea eficienței operaționale.
11. Scalabilitate și flexibilitate: adaptare rapidă la schimbări în mediul legislativ, evoluții demografice, schimbări socioeconomice; dezvoltare instituțională eficientă.

Beneficiari

Un Centru de Operațiuni Digitale (COD) contribuie la îmbunătățirea serviciilor publice și a eficienței operaționale. Beneficiarii unui COD implementat în cadrul Primării includ:

1. Cetățenii: ajută la îmbunătățirea serviciilor oferite cetățenilor prin monitorizarea și optimizarea aplicațiilor și proceselor utilizate în furnizarea serviciilor publice; conduce la o experiență mai bună pentru cetățeni și un nivel mai înalt de satisfacție.
2. Angajații primăriei: facilitează munca angajaților primăriei prin monitorizarea și îmbunătățirea aplicațiilor și proceselor interne, reducând astfel timpul necesar pentru a efectua sarcini și a soluționa probleme.
3. Echipele de IT și securitate: permite echipelor de IT și securitate să monitorizeze și să gestioneze în mod eficient infrastructura IT, aplicațiile și procesele, asigurând securitatea datelor și conformitatea cu reglementările în vigoare.
4. Managerii și decidenții: furnizează informații valoroase pentru manageri și decidenți, ajutându-i să ia decizii mai informate și bazate pe date în ceea ce privește alocarea resurselor, prioritizarea inițiativelor și implementarea îmbunătățirilor.
5. Partenerii și furnizorii de servicii: crește nivelul colaborării și comunicării cu partenerii și furnizorii de servicii, facilitând schimbul de informații și coordonarea activităților.
6. Agenții guvernamentale / alte instituții publice: consolidarea cooperării și comunicării între Primărie și alte instituții publice, promovând schimbul de bune practici și îmbunătățirea serviciilor publice la nivel regional și național.

Rezultate așteptate

- Creșterea eficienței operaționale: optimizarea proceselor și a aplicațiilor va duce la o îmbunătățire a eficienței operaționale și la reducerea costurilor.
- Îmbunătățirea calității serviciilor publice: monitorizarea și optimizarea serviciilor publice digitale vor duce la o experiență mai bună pentru cetățeni și la o îmbunătățire a calității acestor servicii.
- Reacție mai rapidă la incidente și probleme: capacitatea de a detecta și remedia rapid problemele va reduce timpul de întrerupere al serviciilor și va minimiza impactul asupra cetățenilor.
- Creșterea securității cibernetice și a conformității: monitorizarea și gestionarea proactivă a riscurilor de securitate, protejând datele sensibile și asigurând conformitatea cu reglementările în vigoare.
- Luarea deciziilor fundamentate pe date: accesul la date și informații relevante va facilita luarea deciziilor bazată pe date, îmbunătățind astfel rezultatele și eficacitatea primăriei.
- Îmbunătățirea comunicării și colaborării între departamente: integrarea datelor și a proceselor va îmbunătăți comunicarea și colaborarea între diferitele departamente ale primăriei, contribuind la o abordare mai coerentă și coordonată a problemelor comune.
- Creșterea transparenței și responsabilității: implementarea unui COD va crește transparența și responsabilitatea în cadrul primăriei, ajutând la consolidarea încrederii cetățenilor în instituție.
- Adaptabilitate și scalabilitate: permite instituției Primăriei să se adapteze rapid la schimbările din mediul de afaceri, social, legislativ, tehnologic și să crească eficient pe măsură ce nevoile sale evoluează.
- Reducerea riscurilor operaționale: monitorizarea și gestionarea activelor și proceselor digitale vor reduce riscurile operaționale și vor sprijini continuitatea organizațională.
- Promovarea inovației și a transformării digitale: va stimula inovația și va sprijini transformarea digitală în cadrul primăriei, creând noi oportunități pentru îmbunătățirea serviciilor și a eficienței.

I. Context & Justificare

În contextul digital actual, administrațiile publice se confruntă cu numeroase provocări și oportunități în oferirea serviciilor publice și gestionarea activităților cotidiene. Necesitatea de a adopta soluții tehnologice avansate și eficiente pentru îmbunătățirea calității serviciilor pentru cetățeni și optimizarea proceselor interne este imperativă

în această perioadă.

Implementarea unui Centru de Operațiuni Digitale (COD) în cadrul Primăriei Bistrița reprezintă un pas esențial în atingerea acestor obiective. Un COD poate ajuta la monitorizarea și optimizarea aplicațiilor, proceselor și infrastructurii IT, permițând o mai bună gestionare a resurselor și o eficiență crescută în furnizarea serviciilor publice.

Nevoia de a implementa un COD în cadrul Primăriei Bistrița derivă din câteva aspecte critice, cum ar fi:

- Creșterea așteptărilor cetățenilor: cetățenii se așteaptă la servicii publice mai rapide, mai accesibile și mai eficiente, iar un COD poate sprijini primăria în atingerea acestor așteptări prin digitalizarea și optimizarea proceselor.
- Securitatea cibernetică: cu o creștere a amenințărilor cibernetice și a incidentelor, primăriile trebuie să ia măsuri pentru a proteja datele sensibile și a asigura conformitatea cu reglementările în vigoare. Un COD poate oferi monitorizare și gestionare proactivă a riscurilor de securitate.
- Disponibilitate crescută a infrastructurii de comunicații: un COD poate ajuta la monitorizarea și întreținerea rețelelor și infrastructurii de comunicații, asigurând o conexiune stabilă și sigură pentru toate serviciile și aplicațiile digitale ale primăriei.
- Eficiența operațională: un COD poate reduce costurile și crește eficiența prin optimizarea proceselor și a resurselor, permițând primăriei să aloce mai multe resurse pentru alte inițiative esențiale.
- Luarea deciziilor bazată pe date: un COD furnizează date și informații relevante care ajută la luarea deciziilor bazată pe date, contribuind la eficientizarea operațiunilor și la creșterea gradului de satisfacție al cetățenilor.
- Adaptabilitatea și scalabilitatea: implementarea unui COD permite primăriei să se adapteze rapid la schimbările din mediul de afaceri, legislativ, social, tehnologic și să crească eficient pe măsură ce nevoile sale evoluează.

Având în vedere aceste aspecte, implementarea unui Centru de Operațiuni Digitale în cadrul Primăriei Bistrița este esențială pentru a face față provocărilor actuale și pentru a îmbunătăți calitatea serviciilor publice, securitatea cibernetică și eficiența operațională..

Probleme

Din analiza datelor preliminare rezultă carențe semnificative pe următoarele dimensiuni:

- Ineficiența proceselor: procesele manuale, birocrația și lipsa de coordonare pot duce la întârzieri și ineficiențe în furnizarea serviciilor publice. Un COD optimizează și digitalizează procesele pentru a îmbunătăți eficiența și a reduce timpul de răspuns.
- Acces limitat la servicii: cetățenii pot întâmpina dificultăți în accesarea serviciilor publice din cauza programelor de lucru restrânse sau a procedurilor complicate. Un COD facilitează accesul la serviciile digitale, permițând cetățenilor să interacționeze cu Primăria într-un mod mai convenabil și eficient.
- Lipsa de securitate cibernetică: primăria este vulnerabilă la atacuri cibernetice și incidente de securitate. Un COD ajută la monitorizarea, prevenirea și gestionarea riscurilor de securitate cibernetică, protejând datele sensibile și asigurând conformitatea cu reglementările în vigoare.
- Comunicarea și colaborarea ineficiente: lipsa de comunicare și colaborare între diferitele departamente ale Primăriei poate rezulta în soluții incoerente și ineficiente. Un COD îmbunătățește comunicarea și colaborarea între departamente, facilitând o abordare coordonată a problemelor comune.

- Infrastructură IT învechită și lipsa de monitorizare: Sistemele IT și rețelele de comunicații sunt parțial depășite și insuficient monitorizate. Un COD permite monitorizarea și întreținerea rețelelor și infrastructurii de comunicații, asigurând o conexiune stabilă și sigură.
- Lipsa de transparență și responsabilitate: Primăria are dificultăți în a se asigura că este percepută ca fiind transparentă și responsabilă în administrarea resurselor și în furnizarea serviciilor publice. Un COD sporește transparența și responsabilitatea prin monitorizarea performanței și furnizarea de rapoarte detaliate.
- Decizii bazate pe informații insuficiente sau inexacte: lipsa de date și informații relevante duce la decizii neinformate sau ineficiente. Un COD oferă informații în timp real și date analitice, facilitând luarea deciziilor bazată pe date și îmbunătățirea rezultatelor.
- Dificultatea de adaptare la schimbări și inovații tehnologice: Primăria întâmpină dificultăți în a se adapta la schimbările din mediul socioeconomic, legislativ și la noile tehnologii. Un COD sprijină adaptabilitatea și inovația, permițând Primăriei să răspundă rapid la schimbări și să integreze noile tehnologii în operațiunile și serviciile sale.
- Costurile ridicate de operare și întreținere: resursele financiare limitate și costurile crescânde vor pune presiune din ce în ce mai mare pe bugetul Primăriei. Un COD contribuie la reducerea costurilor și la optimizarea utilizării resurselor prin monitorizarea și gestionarea eficientă a operațiunilor și infrastructurii IT.
- Satisfacția redusă a cetățenilor: este incert gradul de satisfacție al cetățenilor cu privire la calitatea și eficiența serviciilor publice, precum și de interacțiunea cu primăria. Un COD poate îmbunătăți satisfacția cetățenilor prin optimizarea proceselor, accelerarea răspunsurilor și îmbunătățirea comunicării.

Oportunități

- Reziliență organizațională: Un COD poate îmbunătăți capacitatea primăriei de a face față unor evenimente neprevăzute, cum ar fi atacurile cibernetice, întreruperile de servicii sau schimbările legislative, prin monitorizarea proactivă și gestionarea eficientă a riscurilor.
- Poziție competitivă consolidată: Prin optimizarea proceselor și îmbunătățirea serviciilor, primăria poate consolida poziția sa în raport cu alte instituții publice și poate deveni un model de bună practică în gestionarea eficientă a resurselor și a tehnologiei.
- Atragerea și retenția talentelor: Un mediu de lucru modern, digitalizat și eficient poate atrage și reține angajați talentați, ceea ce poate contribui la creșterea productivității și la îmbunătățirea calității serviciilor furnizate de primărie.
- Dezvoltarea competențelor digitale: Implementarea unui COD în cadrul primăriei poate stimula dezvoltarea competențelor digitale în rândul angajaților, pregătindu-i pentru a răspunde la provocările și oportunitățile dintr-un mediu tehnologic în continuă evoluție.
- Inovare și adaptabilitate: Un COD poate ajuta primăria să identifice și să adopte rapid noi tehnologii și abordări inovatoare, permițând organizației să rămână relevantă și competitivă într-un mediu în continuă schimbare.
- Parteneriate și colaborări strategice: Prin dezvoltarea de competențe și expertiză în domeniul digital, primăria poate atrage parteneriate și colaborări strategice cu alte entități publice, organizații private sau instituții de cercetare.
- Creșterea încrederii cetățenilor: Îmbunătățirea calității și accesibilității serviciilor publice, precum și consolidarea securității cibernetice, pot contribui la creșterea încrederii cetățenilor în instituția primăriei și în capacitatea sa de a răspunde nevoilor lor.
- Sustenabilitate și responsabilitate socială: Un COD poate ajuta primăria să-și îndeplinească obiectivele de sustenabilitate și responsabilitate socială, prin reducerea consumului de resurse, optimizarea proceselor și promovarea unor practici ecologice și sociale responsabile.

- Inteligență operațională îmbunătățită: Implementarea unui COD va permite primăriei să colecteze, să analizeze și să folosească datele în mod eficient pentru a lua decizii informate și a anticipa nevoile cetățenilor și ale comunității.
- Promovarea incluziunii și accesului egal: Un COD poate contribui la reducerea inegalităților digitale și la asigurarea unui acces egal la serviciile publice pentru toți cetățenii, indiferent de statutul socio-economic sau de alte bariere.
- Consolidarea colaborărilor interdepartamentale: Un COD poate facilita o colaborare mai strânsă între departamentele primăriei și poate contribui la identificarea și exploatarea sinergiilor, permițând organizației să abordeze problemele și să dezvolte soluții integrate.

Soluții la nevoi identificate

Soluțiile identificate țin atât de domeniul software cât și hardware și sunt listate mai jos:

1. Soluții de Network monitoring: e.g. Nagios, Zabbix sau PRTG Network Monitor pentru a urmări și analiza performanța rețelei.
2. Securitate: Software de securitate precum antivirus, antimalware, firewall, soluții de detecție și prevenire a intruziunilor (IPS/IDS) și alte tehnologii de protecție a datelor și a infrastructurii; SIEM (Security Information and Event Management) - soluții precum Splunk, LogRhythm sau AlienVault pentru a colecta, analiza și corela evenimente de securitate în timp real; GRC (Governance, Risk, and Compliance) - software pentru gestionarea conformității și a riscurilor, cum ar fi RSA Archer, MetricStream sau Lockpath Keylight; soluții și măsuri adecvate pentru a asigura protecția și confidențialitatea datelor și a informațiilor stocate în cadrul sistemului. - set politici, proceduri și standarde de securite, soluții de criptare a datelor (e.g AES-256 și TLS), soluții de autentificare și autorizare, detecție și protecția împotriva atacurilor cibernetice, soluții de backup redundant și recuperare a datelor.
3. BPM (Business Process Management): aplicații pentru modelarea, executarea, monitorizarea și optimizarea proceselor organizaționale, cum ar fi Appian, Pega sau Bonita BPM.
4. APM (Application Performance Monitoring): soluții precum Dynatrace, New Relic sau AppDynamics pentru a monitoriza și optimiza performanța aplicațiilor.
5. Sisteme de gestionare a incidentelor și problemelor: soluții precum ServiceNow, Jira Service Management sau Zendesk pentru a urmări și gestiona incidentele și problemele IT.
6. Backup și disaster recovery: software de backup și recuperare în caz de dezastre, cum ar fi Veeam, Acronis sau Bacula.
7. Un sistem de management al bazelor de date: Aceasta va stoca toate datele relevante pentru administrația locală, precum datele cadastrale, taxele locale, datele de identificare ale cetățenilor și alte informații esențiale. În contextul Primăriei, un astfel de sistem trebuie să fie capabil să gestioneze o varietate de tipuri de date, inclusiv date cadastrale, taxe locale, date de identificare ale cetățenilor și alte informații esențiale.
8. Un sistem de gestiune a documentelor: Un astfel de sistem va permite stocarea, accesarea și gestionarea documentelor electronice, precum hârtii oficiale, cereri, formulare și rapoarte. În cazul Primăriei, un DMS este utilizat pentru a gestiona documente precum hârtii oficiale, cereri, formulare, rapoarte și alte înregistrări administrative și trebuie să aibă următoarele caracteristici: import și captură de documente în diverse formate, capacitate de organizare flexibilă a documentelor (ierarhii, etichetare), stocare centralizată și securizată, control al versionării, mecanisme de colaborare și partajare, funcții pentru crearea și gestionarea de fluxuri de lucru, precum aprobări, revizuiri și semnături electronice, capacitate de a gestiona eficient arhivarea, facilități de interoperabilitate și integrare, funcții care să asigure accesibilitatea și mobilitatea, funcții de raportare și audit; sisteme de management al documentelor și cunoștințelor: soluții precum Confluence, SharePoint sau OpenText.
9. Un sistem de workflow și automatizare: Acesta va facilita procesele interne și va reduce timpul necesar pentru a rula și coordona diferite sarcini în cadrul administrației locale. Caracteristici importante: motor de workflow, proiectare și modelare de procese, integrare cu alte sisteme, monitorizare și raportare.

10. **Soluții de comunicare și colaborare**: Soluții software pentru a facilita comunicarea între angajații primăriei, inclusiv email, chat, videoconferințe, platforme de colaborare în timp real (e.g. Microsoft SharePoint, Google Workspace, Atlassian Confluence și Trello); toate fiind securizate de un sistem de autentificare de tip Single Sign On / SSO și criptarea informațiilor end-to end.
11. **Soluții ce vizează interoperabilitatea**: Abilitatea de a se integra și comunica cu alte sisteme software, cum ar fi cele ale agențiilor guvernamentale, autorităților locale și regionale și alți furnizori de servicii. Interoperabilitatea este esențială pentru un sistem informatic integrat într-o primărie, în special în contextul legislației europene și colaborării cu alte agenții guvernamentale, autorități locale și regionale și furnizori de servicii. Caracteristici esențiale: standarde și protocoale comune (XML, JSON, RDF și CSV pentru reprezentarea și schimbul de date, precum și HTTP, HTTPS, SOAP și REST pentru comunicarea între sisteme), conformitatea cu legislația și standardele europeane (EIF - European Interoperability Framework, Core Public Service Vocabulary Application Profile / CPSV-AP, ISA² Core Vocabularies sau European Interoperability Reference Architecture / EIRA), API-uri și servicii web (RESTful, GraphQL sau gRPC), sistem de management al identității și accesului (conforme standardelor SAML, OpenID Connect sau OAuth), middleware și adaptori (e.g. soluții de Enterprise Service Bus /ESB, Data Integration Tools), integrarea cu alte platforme și soluții (e.g. sisteme e-guvernare, platforme de achiziții publice, soluții de management al datelor cadastrale).
12. **Scalabilitate și flexibilitate**: Sistemul ar trebui să poată fi ușor adaptat și extins pentru a face față cerințelor viitoare și pentru a permite implementarea de noi funcționalități și servicii caracterizate de: utilizare microservicii, cloud computing, containerizare și orchestrare (e.g. Docker, Kubernetes), soluții de monitorizare și management al performanței, sistem de gestionare a schimbărilor, compatibilitate și interoperabilitate nativă (standarde și protocoale deschise și bine stabilite, precum RESTful APIs, JSON, XML și OAuth).
13. **Business Intelligence și Analytics**: soluții precum Tableau, Power BI sau QlikView pentru a analiza și vizualiza datele procesate de instituție și pentru a facilita luarea deciziilor bazate pe date.
14. **Integrarea și automatizarea proceselor**: software precum MuleSoft, Apache Nifi sau Microsoft Power Automate pentru a integra diferite sisteme și a automatiza procesele organizaționale.
15. **Gestionarea identității și accesului**: soluții precum Microsoft Azure Active Directory, Okta sau OneLogin pentru a gestiona autentificarea, autorizarea și gestionarea accesului la resursele IT.
16. **Virtualizare și soluții cloud**: tehnologii precum VMware, Hyper-V, OpenStack sau soluții de cloud public precum Amazon Web Services, Microsoft Azure sau Google Cloud Platform pentru a permite virtualizarea și gestionarea resurselor IT.

II. Obiective & Rezultate

Obiective

1. Definirea și crearea unei arhitecturi informatice integrate: design și planificare sistem scalabil și redundant, capabil să susțină o paletă cât largă de scenarii de digitalizare a instituției
2. Monitorizare centralizată: monitorizarea centralizată a aplicațiilor, infrastructurii IT, proceselor organizaționale și securității, facilitând gestionarea eficientă a acestora și reducând complexitatea operațională.
3. Detectarea și remedierea rapidă a problemelor: Prin monitorizarea în timp real și analiza datelor, creșterea ratei și vitezei de detecție a problemelor și incidentelor, remediere în timp util pentru a preveni reducerea performanței sistemului și experiență negativă pentru utilizatori.
4. Optimizarea performanței și eficienței: îmbunătățirea performanței aplicațiilor de bază și a eficienței proceselor organizaționale prin analiza datelor și implementarea de îmbunătățiri continue.
5. Gestionarea riscurilor de securitate: monitorizarea și gestionarea riscurilor de securitate cibernetică într-un mod proactiv, protejând astfel instituția și informațiile sensibile ale acesteia.
6. Asigurarea conformității: respectarea reglementărilor și standardelor în vigoare prin implementarea unor politici și proceduri adecvate și monitorizarea lor.
7. Îmbunătățirea experienței utilizatorilor: monitorizarea performanței aplicațiilor și a proceselor organizaționale ajută la identificarea și soluționarea problemelor care afectează experiența utilizatorilor, conducând la o mai bună satisfacție a utilizatorilor (angajați, cetățeni, terți).
8. Accelerarea proceselor de luare a deciziilor: date și informații valoroase pentru luarea deciziilor bazate pe date, accelerând procesul de luare a deciziilor și îmbunătățind rezultatele organizației.
9. Colaborare îmbunătățită: colaborare facilă între echipele de IT, securitate, dezvoltare de aplicații și managementul proceselor interne; comunicare eficientă și o abordare coerentă a problemelor comune.
10. Reducerea costurilor operaționale: costuri operaționale reduse prin optimizarea resurselor IT, eliminarea redundanțelor și îmbunătățirea eficienței operaționale.
11. Scalabilitate și flexibilitate: adaptare rapidă la schimbări în mediul legislativ, evoluții demografice, schimbări socioeconomice; dezvoltare instituțională eficientă.

Măsurarea & evaluarea obiectivelor

Obiectiv	Modalități de evaluare	Impact estimat
1. Definirea și crearea unei arhitecturi informatice integrate	- Procentul de sisteme și aplicații integrate - Timpul necesar pentru a implementa noi servicii și aplicații	Îmbunătățirea eficienței operaționale și a adaptabilității la noi tehnologii și cerințe
2. Monitorizare centralizată	- Timpul mediu de rezoluție a incidentelor - Procentul de incidente nerezolvate	Reducerea complexității operaționale și îmbunătățirea timpului de răspuns la incidente
3. Detectarea și remedierea rapidă a problemelor	- Timpul mediu de detectare a problemelor - Procentul de probleme remediate în timp util	Îmbunătățirea performanței sistemului și a experienței utilizatorilor
4. Optimizarea performanței și eficienței	- Procentul de îmbunătățire a performanței aplicațiilor și proceselor organizaționale - Reducerea costurilor operaționale asociate cu procesele optimizate	Îmbunătățirea productivității și a satisfacției utilizatorilor
5. Gestionarea riscurilor de securitate	- Numărul de incidente de securitate prevenite - Procentul de reducere a riscurilor de securitate	Protejarea datelor și resurselor instituției și menținerea încrederii utilizatorilor
6. Asigurarea conformității	- Procentul de conformitate cu reglementările și standardele aplicabile - Numărul de audituri trecute cu succes	Evitarea sancțiunilor legale și menținerea încrederii părților interesate

Obiectiv	Modalități de evaluare	Impact estimat
7. Îmbunătățirea experienței utilizatorilor	- Scorul de satisfacție a utilizatorilor - Numărul de reclamații și probleme raportate de utilizatori	Creșterea satisfacției utilizatorilor și a eficienței în utilizarea resurselor IT
8. Accelerarea proceselor de luare a deciziilor	- Timpul mediu de luare a deciziilor - Procentul de decizii corecte bazate pe date	Îmbunătățirea rezultatelor organizației și a eficienței proceselor de decizie
9. Colaborare îmbunătățită	- Procentul de probleme soluționate în echipă - Scorul de satisfacție al angajaților în ceea ce privește colaborarea	Consolidarea comunicării și a sinergiei între echipe și departamente
10. Reducerea costurilor operaționale	- Procentul de reducere a costurilor operaționale - Reducerea costurilor totale de deținere și exploatare a infrastructurii IT	Economii financiare care pot fi redirecționate către alte proiecte și inițiative
11. Scalabilitate și flexibilitate	- Timpul necesar pentru a scala resursele IT în funcție de cerințe - Capacitatea de a integra noi tehnologii și de a se adapta la schimbări în mediul de reglementare	Dezvoltare instituțională eficientă și adaptabilitate în fața schimbărilor și provocărilor externe

Rezultate așteptate pentru proiect

1. Promovarea inovației și a transformării digitale: În cadrul Primăriei se vor stimula inovația și transformarea digitală, creându-se noi oportunități pentru îmbunătățirea serviciilor și eficienței.
2. Îmbunătățirea calității serviciilor publice: Serviciile publice digitale vor fi monitorizate și optimizate pentru a oferi o experiență mai bună cetățenilor și pentru a îmbunătăți calitatea acestora.
3. Creșterea eficienței operaționale: Procesele și aplicațiile vor fi optimizate pentru a îmbunătăți eficiența operațională și pentru a reduce costurile.
4. Reducerea riscurilor operaționale: Se vor monitoriza și gestiona activitățile și procesele digitale pentru a reduce riscurile operaționale și pentru a sprijini continuitatea organizațională.
5. Reacție mai rapidă la incidente și probleme: Capacitatea de a detecta și remedia rapid problemele va reduce timpul de întrerupere al serviciilor și va minimiza impactul asupra cetățenilor.
6. Creșterea securității cibernetice și a conformității: Se vor monitoriza și gestiona proactiv riscurile de securitate pentru a proteja datele sensibile și pentru a asigura conformitatea cu reglementările în vigoare.
7. Luarea deciziilor fundamentate pe date: Accesul la date și informații relevante va facilita luarea deciziilor bazată pe date, îmbunătățind astfel rezultatele și eficacitatea Primăriei.
8. Îmbunătățirea comunicării și colaborării între departamente: Integrarea datelor și a proceselor va îmbunătăți comunicarea și colaborarea între diferitele departamente ale primăriei, contribuind la o abordare mai coerentă și coordonată a problemelor comune.
9. Creșterea transparenței și responsabilității: Implementarea proiectului COD va crește transparența și responsabilitatea în cadrul primăriei, ajutând la consolidarea încrederii cetățenilor în instituție.
10. Adaptabilitate și scalabilitate: Primăria va putea să se adapteze rapid la schimbările socioeconomice, demografice, tehnologice și/sau legislative și să crească eficient pe măsură ce nevoile sale evoluează.

III. Plan de implementare

Activitățile principale

- Realizarea unui audit tehnic și funcțional al sistemelor existente: analiza sistemelor și infrastructurii IT existente, identificarea punctelor tari și a punctelor slabe, precum și stabilirea cerințelor tehnice și funcționale pentru noul sistem.
- Crearea unei echipe de proiect multidisciplinare: echipa trebuie să includă reprezentanți din diferite departamente, precum IT, management, resurse umane, financiar, juridic și comunicare, precum și experți externi în domeniul tehnologiei informației și al transformării digitale.
- Definirea obiectivelor și a indicatorilor de performanță ai proiectului: dezvoltarea unei baze solide pentru a măsura progresul și succesul implementării sistemului informatic integrat.
- Selecția soluțiilor hardware și software: evaluarea și compararea diferitelor soluții disponibile pe piață, în funcție de cerințele identificate în auditul tehnic și funcțional; evaluarea interdependențelor reciproce între soluțiile de hardware și software în vederea eliminării incompatibilităților și/sau limitărilor create de acestea
- Achiziția soluțiilor hardware și software: evaluarea și compararea diferitelor soluții disponibile pe piață, în funcție de bugetul alocat proiectului, a condițiilor de livrare, service și suport pe durata ciclului de viață a produselor și serviciilor
- Dezvoltarea și personalizarea soluțiilor software: configurarea și personalizarea soluțiilor software achiziționate pentru a se potrivi nevoilor și proceselor specifice ale primăriei.
- Implementarea infrastructurii hardware și a soluțiilor software: instalarea și configurarea echipamentelor hardware și a soluțiilor software, inclusiv integrarea acestora cu sistemele existente.
- Migrarea datelor și a informațiilor existente: transferul și consolidarea datelor și informațiilor din sistemele vechi către noul sistem informatic integrat, precum și verificarea integrității și acurateței acestora.
- Testarea și validarea sistemului: verificarea funcționalității și a performanței noului sistem informatic integrat, precum și identificarea și remedierea eventualelor probleme și deficiențe.
- Pregătirea personalului și dezvoltarea competențelor: organizarea de sesiuni de instruire și workshop-uri pentru a familiariza personalul cu noul sistem și a dezvolta competențele necesare pentru utilizarea eficientă a acestuia.
- Lansarea și monitorizarea sistemului: punerea în funcțiune a noului sistem informatic integrat și monitorizarea performanței și eficienței acestuia în timp real, precum și ajustarea și îmbunătățirea continuă a acestuia pe baza feedback-ului și a nevoilor identificate.
- Evaluarea impactului și a rezultatelor proiectului: măsurarea și raportarea progresului și succesului proiectului în funcție de obiectivele și indicatorii de performanță stabiliți

Responsabilități

Echipa responsabilă de proiect va fi formata din specialiști cu experiență în domeniul IT, management, resurse umane, financiar, juridic și comunicare, precum și experți externi în domeniul tehnologiei informației și al transformării digitale.

Primăria Bistrița va fi responsabila de supervizarea și coordonarea proiectului, asigurând o buna comunicare intre membrii echipei de proiect.

Durata proiectului

Durata estimată de implementare a proiectului se ridică la 8 -12 luni.

Nr	Activitate	Durată estimată (săpt.)
1	Audit tehnic și funcțional	2-4
2	Crearea unei echipe de proiect	2-4
3	Definirea obiectivelor și indicatorilor	1-2
4	Selectarea soluțiilor hardware și software	3-4
5	Achiziționarea soluțiilor hardware și software	2-4
6	Dezvoltarea și personalizarea soluțiilor software	4-6
7	Implementarea infrastructurii hardware și a soluțiilor software	4-6
8	Migrarea datelor și a informațiilor existente	2-4
9	Testarea și validarea sistemului	2-4
10	Pregătirea personalului și dezvoltarea competențelor	2-4
11	Lansarea și monitorizarea sistemului	2-4
12	Evaluarea impactului și a rezultatelor	1-2
	TOTAL	27 - 48

IV. Sustenabilitate & impact

Finanțarea & Construcția bugetului

Construcția și valoarea totală a bugetului proiectului va fi proiectată pentru a putea varia în funcție de opțiunile strategice ale instituției Primăriei Bistrița, a priorităților proiectelor de digitalizare și a resurselor disponibile. Construcția bugetului va include următoarele categorii de costuri:

- Costuri legate de analiză, consultanță și audit
- Costuri legate de achiziția soluțiilor hardware
- Costuri legate de achiziția soluțiilor software
- Costuri legate de dezvoltarea și personalizarea soluțiilor
- Costuri legate instalarea și configurarea echipamentelor hardware
- Costuri legate de migrarea datelor
- Costuri legate de training și formare resurse umane

În funcție de specificul și dimensiunea proiectului, bugetul total poate varia între 1.000.000 și 1.500.000 EUR. Este important să se realizeze o estimare detaliată a costurilor și o alocare corespunzătoare a resurselor pentru a asigura succesul proiectului și implementarea tuturor măsurilor necesare pentru protejarea, operarea eficientă și reziliența sistemului integrat informatic.

Sustenabilitate

Sustenabilitatea proiectului va fi asigurată prin:

- Stabilirea unui plan de întreținere și actualizare continuă a sistemului: Dezvoltarea unui plan care să prevadă actualizări regulate ale software-ului și hardware-ului, pentru a menține securitatea și eficiența sistemului pe termen lung.

- Asigurarea finanțării pe termen lung: Identificarea unor surse stabile de finanțare pentru implementarea, întreținerea și dezvoltarea continuă a sistemului, inclusiv fonduri guvernamentale, fonduri europene sau alte surse de finanțare.
- Formarea și dezvoltarea personalului: Organizarea de cursuri de formare și dezvoltare profesională pentru personalul primăriei, pentru a asigura o utilizare eficientă și sustenabilă a sistemului.
- Implementarea unui sistem de monitorizare și evaluare: Monitorizarea și evaluarea performanței sistemului în mod regulat, pentru a identifica posibile probleme și a asigura eficiența acestuia pe termen lung.
- Încheierea unor contracte de suport tehnic și mentenanță cu furnizorii de software și hardware: Aceste contracte vor asigura suportul tehnic necesar pentru remedierea eventualelor probleme și pentru menținerea sistemului într-o stare de funcționare optimă.
- Dezvoltarea de parteneriate cu alte instituții și organizații: Stabilirea unor parteneriate cu alte primării, instituții guvernamentale, universități și organizații pentru a împărtăși bune practici și resurse în domeniul sistemelor informatice integrate.
- Implementarea unei strategii de comunicare și diseminare a informațiilor: Dezvoltarea și punerea în aplicare a unei strategii de comunicare pentru a informa cetățenii și alte părți interesate despre beneficiile și rezultatele sistemului, pentru a crește gradul de acceptare și utilizare.
- Stabilirea unor proceduri și politici de securitate a datelor și a informațiilor: Implementarea unor măsuri de protecție adecvate pentru a asigura securitatea și confidențialitatea datelor și informațiilor stocate în cadrul sistemului.
- Documentarea și standardizarea proceselor și procedurilor: Elaborarea unor documente care să descrie în detaliu procesele și procedurile asociate cu sistemul informatic, pentru a facilita gestionarea, dezvoltarea și întreținerea acestuia pe termen lung.

Impact social, economic, mediu

Impactul social, economic și de mediu al proiectului va fi pozitiv și se va manifesta prin:

Impact social:

- Accesibilitate sporită: Implementarea unui sistem informatic integrat va facilita accesul cetățenilor la serviciile oferite de primărie, inclusiv informații și formulare online. Astfel, se va îmbunătăți comunicarea și interacțiunea dintre cetățeni și administrația locală.
- Transparență și responsabilitate: Un astfel de sistem va permite o mai bună monitorizare și control al activităților desfășurate în cadrul primăriei, contribuind la transparența și responsabilizarea instituției.
- Eficientizarea proceselor interne: Personalul primăriei va beneficia de un mediu de lucru mai eficient și organizat, ceea ce va duce la creșterea productivității și îmbunătățirea serviciilor oferite.

Impact economic:

- Reducerea costurilor administrative: Prin digitalizarea proceselor și serviciilor, primăria va economisi resurse financiare și umane, reducând costurile administrative.
- Creșterea veniturilor: O mai bună gestionare a resurselor și optimizarea colectării taxelor și impozitelor vor duce la creșterea veniturilor locale.
- Atracția de investiții: O administrație locală eficientă și transparentă este mai atractivă pentru investitori, ceea ce poate contribui la dezvoltarea economică a comunității.

Impact de mediu:

- Reducerea consumului de hârtie: Digitalizarea documentelor și a proceselor de lucru va duce la o scădere semnificativă a consumului de hârtie, ceea ce va avea un impact pozitiv asupra mediului.

- Reducerea emisiilor de carbon: Implementarea unui sistem informatic integrat va reduce necesitatea deplasărilor cetățenilor și a personalului primăriei pentru a accesa și furniza anumite servicii, contribuind astfel la diminuarea emisiilor de carbon.
- Promovarea practicilor sustenabile: Un sistem informatic eficient poate ajuta la monitorizarea și gestionarea mai bună a resurselor naturale și a infrastructurilor, promovând astfel dezvoltarea durabilă în cadrul comunității.

V. Anexe

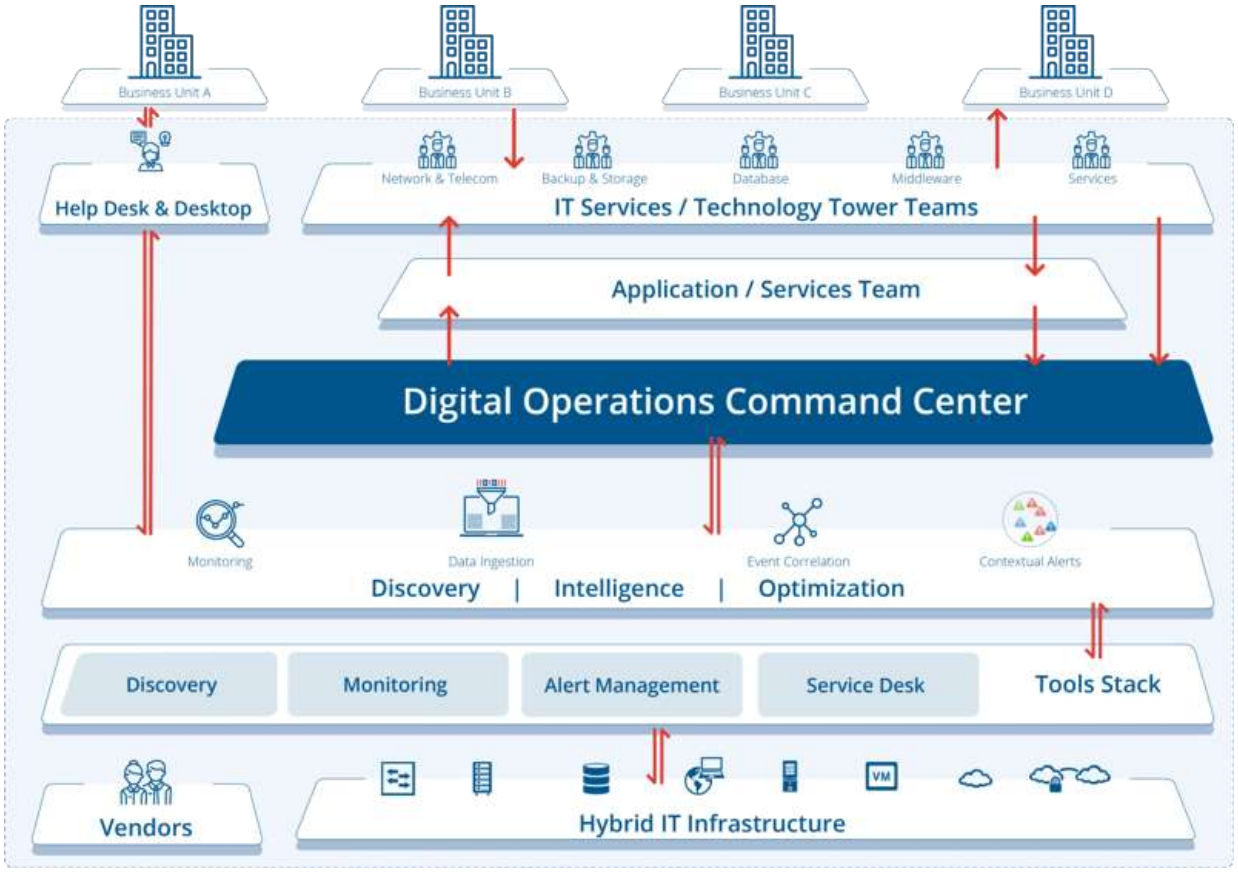


Fig. 1. Exemplu de COD

FISA DE PROIECT FANION

Titlu

Implementare Rețea fibră optică integrată la nivel de Municipiu Bistrița

Coordonator din partea consultantului

Bogdan CIOTLAUS

Rezumat

1. Scop

Scopul proiectului este design-ul parametrilor funcționali și tehnici pentru o rețea fibră optică subterană, integrată la nivelul municipiului Bistrița, caracterizată de eficiență, reziliență, scalabilitate și sustenabilitate și care să ofere o infrastructură de comunicații capabilă să susțină obiectivele și proiectele derivate din strategia de digitalizare a Primăriei Bistrița.

Proiectul va fi fundamentat pe analiza detaliată a situației curente la nivelul infrastructurii de comunicații a Primăriei Bistrița, a riscurilor sistemice, a categoriilor principale de nevoi dictate de digitalizare în domeniul infrastructurii IT.

2. Obiective

Obiectivele pe termen lung ale prezentului proiect sunt:

- Sistematizarea rețelei de comunicații digitale
- Creșterea disponibilității serviciilor instituției via comunicații eficiente
- Reducere dependență de furnizori de comunicații
- Asigurare sustenabilitate economică

Obiectivele pe termen scurt ale prezentului proiect sunt:

- Realizarea interconectării stabile și eficiente a locațiilor aflate în subordinea Primăriei Bistrița
- Creșterea disponibilității serviciilor digitale în toate locațiile aflate în subordinea Primăriei Bistrița
- Crearea premiselor de sistematizare parametri rețea conectivitate pentru toți operatorii regionali
- Asigurarea securității fizice a infrastructurii de comunicații
- Eficientizarea mentenabilității infrastructurii de comunicații

3. Beneficiari

Beneficiarii acestui proiect pot fi împărțiți în două categorii: beneficiari direcți și indirecți.

Beneficiarii direcți ai acestui proiect sunt managementul și angajații Primăriei Bistrița.

Beneficiarii indirecți sunt reprezentați de furnizorii terți și cetățenii din comunitate.

4. Rezultate așteptate

Rezultatele așteptate ale proiectului sunt:

- Identificare nevoilor de interconectare, a implicațiilor legate de infrastructura de comunicații
- Sistematizare infrastructurii de comunicații
- Creșterea disponibilității infrastructurii de comunicații și, implicit, a serviciilor digitale oferite cu ajutorul acesteia
- Asigurarea furnizării de servicii digitalizate către diverse instituții din subordinea Primăriei Bistrița și către cetățeni
- Crearea unor puncte de acces către serviciile Primăriei Bistrița care vor acționa ca nuclee de digitalizare

- Crearea de premise pentru operatorii economici să dezvolte servicii noi care să utilizeze drept punct de plecare infrastructura și/sau serviciile digitale ale Primăriei Bistrița

I. Context & Justificare

Probleme

Din analiza datelor preliminare, reiese că Primăria Bistrița are nevoie de o infrastructură de comunicații capabilă să interconecteze toate unitățile aflate în subordinea sa și toate punctele de acces prin care cetățenii sau organizațiile terțe intră în contact cu Primăria Bistrița, să implementeze o infrastructură de comunicații capabilă să ofere servicii digitalizate.

Situația prezentă a infrastructurii de comunicații prezintă carențe și riscuri semnificative pentru atingerea obiectivelor previzionate de digitalizarea sistemică a serviciilor Primăriei Bistrița. Menționăm în special:

- Lipsa sistematizării și standardizării
- Lipsa securizării fizice, operaționale și cibernetice
- Disponibilitate redusa sau inexistentă, în funcție de locație
- Dependență de furnizor de conectivitate și expunere semnificativă la volatilitate crescută a prețului serviciilor oferite de furnizorii de conectivitate actuali

Implementarea prezentului proiect se justifică prin necesitate de a elimina riscuri sistemice ale infrastructurii de comunicații, de a asigura un nivel de securitate și funcționalitate capabil să susțină multiple scenarii potențiale de digitalizare.

Oportunități

- Primăria Bistrița este în prezent angajată într-o serie de lucrări care presupun intervenții în subteranul teritoriul administrat
- Primăria Bistrița se poate prevala de contextul existent pentru a standardiza propria infrastructura de comunicații, a impune bune practici la nivel local și regional și a sincroniza eforturile tuturor actorilor implicați în aceste procese
- Primăria Bistrița poate pune în valoare noi tehnologii legate de rețele de comunicații pe bază de fibră optică caracterizate de o densitate și reziliență crescută

Soluții la nevoi identificate

- Identificarea și adoptarea de standarde adecvate la nivel tehnic, funcțional și management pentru infrastructura de comunicații
- Standardizarea abordărilor legate de implementarea rețelelor de comunicații
- Prioritizarea rețelelor subterane de tubulatură pentru fibră optică, capabile de extindere și utilizare partajată pentru multipli furnizori
- Standardizarea nodurilor de rețea în cadrul infrastructurii de comunicații
- Securizarea accesului fizic la rețeaua de fibră optică via acces securizat al căminelor și accesul operațional securizat cibernetic la nodurile de rețea
- Implementare sisteme de monitorizare în timp real, jurnalizare incidente și sistem de alertare programabil al tuturor componentelor esențiale de infrastructură IT la nivel de noduri de rețea

- Implementare programatică a redundanțelor în infrastructura de conectivitate la nivelul nodurilor de rețea în vederea eliminării punctelor unice de eroare (i.e. single point of failure) cu scopul de a crește reziliența și mentenabilitatea de ansamblu a infrastructurii de conectivitat
- Standardizare, integrare și centralizare comunicații critice pentru infrastructura IT
- Prioritizarea arhitecturilor modulare de tip „plug-and-play”

II. Obiective & Rezultate

Obiective termen lung

- Creșterea rezilienței serviciilor oferite de Primăria Bistrița prin îmbunătățirea rezilienței infrastructurii de comunicații: implementarea sistem subteran de tubulatură pentru rețea fibră optică, mecanisme de semnalizare a traseului rețelei pentru evitarea deteriorării accidentale la intervenții în subteran
- Creșterea disponibilității serviciilor oferite de Primăria Bistrița prin îmbunătățirea disponibilității infrastructurii de comunicații
- Securizarea fizică a rețelelor de fibră optică și a nodurilor de rețea din cadrul instituțiilor și/sau punctelor de lucru din subordinea Primăriei Bistrița Securitate fizica
- Creșterea mentenabilității rețelei de comunicații a Primăriei Bistrița
- Reducere dependenței de furnizori de conectivitate

Obiective termen scurt

- Interconectare localități și puncte de lucru ale Primăriei Bistrița într-o rețea de fibră optică
- Construirea unei infrastructuri capabilă să susțină o paletă largă de servicii digitalizate
- Sistematizare rețea conectivitate pentru toți operatorii regionali

Măsurarea & evaluarea obiectivelor

- Raport audit detaliat a situației curente, a riscurilor sistemice, a categoriilor principale de nevoi dictate de procesele de digitalizare în domeniul infrastructurii de comunicații, inclusiv identificarea traseelor optime pentru rețeaua care poate interconecta instituțiile din subordinea Primăriei Bistrița și analiza cost beneficiu structură nod rețea
- Grad de interconectare capabilă să asigure trafic de informații între instituțiile Primăriei și trafic de informații necesar furnizării de servicii digitalizate de către Primăria Bistrița
- Identificarea, securizarea și echiparea spațiilor fizice alocate nodurilor de rețea ale Primăriei Bistrița în vederea realizării unei infrastructuri de comunicații cu disponibilitate de 99,95%
- Infrastructură redundantă, conform standardelor TIA-942
- Rețea fibră optică & infrastructură comunicații scalabilă cu rezervă disponibilă de 30%
- Grad de monitorizare a nodurilor de rețea de minim 100%
- Simplificarea și eficientizarea mentenabilității infrastructurii de comunicații a primăriei Bistrița

Rezultate așteptate

- Identificarea nevoilor de interconectare, a implicațiilor legate de infrastructura de comunicații
- Sistematizarea infrastructurii de comunicații
- Creșterea disponibilității infrastructurii de comunicații și a serviciilor digitale oferite cu ajutorul acesteia; asigurarea furnizării de servicii digitalizate către diverse instituții din subordinea Primăriei Bistrița și către cetățeni
- Crearea unor puncte de acces către serviciile Primăriei Bistrița care vor acționa ca nuclee de digitalizare
- Crearea de premise pentru operatorii economici să dezvolte servicii noi care să utilizeze drept punct de plecare infrastructura și/sau serviciile digitale ale Primăriei Bistrița

III. Plan de implementare

Activitățile principale

- Studiu de fezabilitate care să cuprindă:
    - a) analiza detaliată a situației curente a infrastructurii de comunicații a Primăriei Bistrița (inclusiv rețeaua existentă), a infrastructurilor de suport, a sistemelor de management utilizate pentru gestionarea infrastructurii de comunicații (politici, proceduri, resurse umane, mecanisme de jurnalizare & raportare) și a vulnerabilităților infrastructurii de comunicații;
    - b) analiza scenariilor de digitalizare și a implicațiilor acestora asupra caracteristicilor infrastructurii de comunicații, a sistemelor de management ale acestora; prezentarea rezultatelor analizei sub formă de raport cost/beneficiu pentru facilitarea procesului decizional al instituției Primăriei în vederea selectarea modelului preferat (i.e. caracteristici rețea, caracteristici noduri rețea);
    - c) audit traseu, locații și modalități de implementare a rețelei de interconectare dorite;
    - d) analiză caracteristici tehnice și funcționale nod rețea tipic;
    - e) analiză autorizații necesare pentru executarea proiectului
- Investiții și execuție în vederea implementării proiectului tehnic:
    - a) creare rețea de interconectare
    - b) creare noduri rețea în locațiile stabilite
    - c) punere în funcțiune și testare
- Audit infrastructură comunicații & suport infrastructură comunicații și sisteme de management ulterior fazei de implementare
- Activități legate de valorificare a rețelei de intercomunicare

Responsabilități

Echipa responsabilă de proiect va fi formata din specialiști cu experiență în domeniul infrastructurilor de comunicații, rețelistică și infrastructură de suport rețele, a sistemelor de management ale acestor infrastructuri.

Primăria Bistrița va fi responsabila de supervizarea și coordonarea proiectului, asigurând o buna comunicare intre membrii echipei de proiect.

Durata proiectului

2-4 ani, în funcție de parametrii proiectului și prioritățile Primăriei Bistrița.

Nr	Activitate	Durata estimată
1	Studiu de fezabilitate	4 luni
2	Investiții și execuție în vederea implementării proiectului tehnic, pe componenta - Creare rețea de interconectare	36 luni
3	Investiții și execuție în vederea implementării proiectului tehnic, pe componenta - Creare noduri rețea în locațiile stabilite	4 luni
4	Investiții și execuție în vederea implementării proiectului tehnic, pe componenta - Punere în funcțiune și testare	2 luni
5	Audit infrastructură comunicații post-implementare	2 luni
6	Activități legate de valorificare a rețelei de intercomunicare	6 luni

V. Sustenabilitate & impact

Finanțarea & Construcția bugetului

Construcția și valoarea totală a bugetului proiectului va fi proiectată pentru a putea varia în funcție de opțiunile strategice ale instituției Primăriei Bistrița, a priorităților stabilite în cadrul proiectelor de digitalizare și a resurselor disponibile. Construcția bugetului va include următoarele categorii de costuri:

- Costuri legate de analiză, consultanță și audit
- Costuri legate de implementarea traselor de interconectare rețea
- Costuri legate de locația și caracteristicile spațiului / spațiilor fizice care vor găzdui nodurile de rețea
- Costuri legate de implementare a nodurilor de rețea
- Costuri legate de training și formare resurse umane
- Costuri legate de dezvoltarea de sisteme de management: politici, proceduri, protocoale, jurnalizare, raportare
- Costuri legate de valorificarea infrastructurii de comunicații

Nr.	Locație traseu rețea interconectare	Distanță estimată	Estimare cost implementare
1	Ghinda	10.000 m	86.519 €
2	Sărata	10.000 m	86.519 €
3	Sigmir	8.000 m	69.215 €
4	Slătinița	13.000 m	11.2475 €
5	Unirea	5.000 m	43.260 €
6	Viișoara	9.000 m	77.867 €
7	Clădiri Bistrița	25.000 m	216.298 €
	Total		**692.153 €**

Figură 1. Estimare prealabilă a bugetelor necesare implementării traseelor de interconectare fibră optică subterană pentru Primăria Bistrița

Estimare prealabilă a bugetului necesar achiziției de echipamente și realizării infrastructuri cu noduri de rețea tipice

Nr.	Categorie cost	Necesar	Estimare cost per unitate
1	Fortinet FortiSwitch-248E-POE	19	2288 €
2	SMT1500RMI2UC - UPS, 1kW, 240V, 4x IEC 60320 C13, APC	19	1278 €
3	ODF - 24 Porturi	19	162 €
4	Rack podea 22U 19'	19	406 €
5	Organizator cablu	19	20 €
6	PDU APC	19	162 €
	Total		**4316** €

În funcție de specificul și dimensiunea proiectului, bugetul total poate varia între 700.000 și 900.000 de Euro. Este important să se realizeze o estimare detaliată a costurilor și o alocare corespunzătoare a resurselor pentru a asigura

succesul proiectului și implementarea tuturor măsurilor necesare pentru protejarea, operarea eficientă și reziliența infrastructurii IT ca parte a strategiei instituționale de asigurarea a continuității activităților și recuperare în caz de dezastru.

Sustenabilitate

Sustenabilitatea proiectului va fi asigurată prin:

- Crearea unei infrastructuri de comunicații scalabilă și partajabilă, capabilă să deservească o paletă largă de servicii digitalizate oferite de către Primăria Bistrița cetățenilor și/sau altor instituții
- Proiectarea unei infrastructuri de comunicații eficiente din punct de vedere al consumului de resurse prin reducerea consumului de energie și creșterea gradului de monitorizare a proceselor interne și, în consecință, reducerea necesarului de resurse umane dedicate
- Crearea unui sistem de management transparent, capabil de monitorizare și jurnalizare al tuturor aspectelor infrastructurii de comunicații și capabil să producă decizii informate pentru investiții în tehnologii inteligente
- Implementarea unui program de educarea personalului în domeniul infrastructurii de comunicații, pentru a asigura o infrastructura viabilă, rezilientă și securizată.
- Identificarea modalităților de valorificare (și/sau stimulare dezvoltare economică) în condiții de transparență și securitate a infrastructurii de comunicații de către terți
- Asigurarea unei bune coordonări și comunicări între membrii echipei de proiect și angajații Primăriei Bistrița, pentru a menține nivelul ridicat de implicare.
- Sensibilizarea și educarea cetățenilor în ceea ce privește valoarea unei infrastructuri IT securizate, flexibile și eficiente pentru o instituție publică.

Impact social, economic.

Impactul social, economic și de mediu al proiectului va fi pozitiv și se va manifesta prin:

- Creșterea disponibilității infrastructurii de comunicații și a serviciilor digitale oferite cu ajutorul acesteia; asigurarea furnizării de servicii digitalizate către diverse instituții din subordinea Primăriei Bistrița și către cetățeni
- Creșterea încrederii cetățenilor în capacitatea instituțională a Primăriei Bistrița de a oferi servicii digitale și impact pozitiv la dezvoltarea socioeconomica a comunității locale
- Crearea unor puncte de acces către serviciile Primăriei Bistrița care vor acționa ca nuclee de digitalizare
- Crearea de premise pentru operatorii economici să dezvolte servicii noi care să utilizeze drept punct de plecare infrastructura și/sau serviciile digitale ale Primăriei Bistrița
- Reducerea costurilor și a timpului alocat pentru remedierea incidentelor legate de infrastructura de comunicații.
- Creșterea globală a flexibilității instituționale.

V. Anexe

Hărți

Fig. 1. Hartă estimativă trasee rețea de interconectare pentru locațiile principale aflate în subordinea Primăriei Bistrița

Diagrame

Fig.2. Diagrama model nod optic

FISA DE PROIECT FANION

Titlu

Implementare Sistem Integrat Informatic pentru Primăria Bistrița

Coordonator din partea consultantului

Bogdan CIOTLAUS

Rezumat

Scop

Scopul proiectului de față este analiza design-ului și a implicațiilor legate de implementarea unui sistem integrat informatic pentru Primăria Bistrița: o platformă digitală care centralizează și automatizează procesele, fluxurile de lucru și operațiunile specifice administrației publice locale

Scopul principal al unui sistem informatic integrat este să interconecteze diferitele aplicații și baze de date utilizate în cadrul instituției în vederea facilitării comunicării și colaborării între departamente, angajați, instituții sau organizații terțe și, esențial, cetățeni.

Fundamental, sistemul integrat informatic trebuie să susțină obiectivele și proiectele derivate din strategia de digitalizare a Primăriei Bistrița.

Proiectul va fi fundamentat pe analiza detaliată a situației curente la nivelul proceselor Primăriei Bistrița, a riscurilor sistemice, a categoriilor principale de nevoi dictate de digitalizare. În elaborarea proiectului va fi prioritizat principiul maximizării libertății instituției de a adopta o paletă largă de inițiative de digitalizare.

Obiective

Obiectivele pe termen scurt ale prezentului proiect sunt:

1. Definirea și crearea unei arhitecturi informatice integrate, scalabile și redundante, capabile să susțină o paletă cât largă de scenarii de digitalizare a instituției
2. Eficiență sporită & reducerea birocrației: automatizarea proceselor și operațiunilor, reducerea redundanței datelor și centralizarea informațiilor pentru a îmbunătăți eficiența în cadrul administrației publice locale; digitalizarea proceselor și fluxurilor de lucru pentru a reduce birocrația și a accelera gestionarea și procesarea documentelor, cererilor și autorizațiilor.
3. Gestionarea datelor într-un mod centralizat și securizat: stocarea și gestionarea datelor într-un mod centralizat, pentru a asigura protecția și securitatea informațiilor și a preveni pierderea de date și accesul neautorizat.
4. Îmbunătățirea comunicării și colaborării: interconectarea diferitelor departamente și funcționari pentru a îmbunătăți comunicarea și colaborarea între aceștia.
5. Accesibilitate crescută: implementarea unui sistem care să permită cetățenilor să acceseze și să solicite servicii publice online, simplificând interacțiunea cu administrația locală și îmbunătățind experiența utilizatorilor.

Obiectivele pe termen lung ale prezentului proiect sunt:

1. Transparență îmbunătățită: crearea unui sistem care să faciliteze accesul la informații și date în timp real pentru funcționari, conducând la o mai mare transparență în luarea deciziilor și gestionarea resurselor.
2. Optimizarea resurselor: dezvoltarea unui sistem care să permită o monitorizare eficientă a resurselor, facilitând planificarea și alocarea acestora într-un mod optim.
3. Suport pentru luarea deciziilor: crearea unui sistem care să ofere instrumente de analiză și raportare pentru a ajuta la luarea deciziilor informate și la evaluarea eficienței politicii și strategiilor locale.
4. Adaptabilitate și scalabilitate: implementarea unui sistem informatic integrat care să poată fi adaptat și extins pentru a răspunde nevoilor în continuă schimbare ale administrației publice locale și pentru a se adapta la evoluțiile tehnologice și legislative.
5. Reducerea costurilor: realizarea unui sistem care să automatizeze procesele și să eficientizeze operațiunile, contribuind la o reducere a costurilor administrative și la o utilizare mai eficientă a resurselor financiare și umane.

Beneficiari

Beneficiarii acestui proiect pot fi împărțiți în două categorii: beneficiari direcți și indirecți.
Beneficiari direcți:

- Administrația locală: primăria și departamentele sale vor beneficia direct de pe urma eficienței sporite, comunicării îmbunătățite și optimizării resurselor, care vor facilita luarea deciziilor și gestionarea serviciilor publice.
- Angajații primăriei: funcționarii și personalul administrației locale vor putea să își îndeplinească sarcinile mai eficient, având acces la informații centralizate și la un sistem care facilitează colaborarea între departamente.
- Furnizorii și partenerii locali: organizațiile și companiile care colaborează cu primăria, precum furnizorii de servicii și partenerii de proiect, vor beneficia de un sistem care îmbunătățește transparența și eficiența în relațiile cu administrația locală.

Beneficiari indirecți:

- Cetățenii localității: cetățenii vor avea acces la servicii publice mai eficiente, transparente și accesibile, precum și la informații actualizate despre activitatea administrației locale. Acest lucru va îmbunătăți calitatea vieții și va contribui la dezvoltarea comunității.
- Investitorii și mediul de afaceri: Mediul de afaceri local va beneficia de o primărie mai eficientă și transparentă, care poate atrage investiții și dezvoltare economică în zonă.
- Guvernul central și alte instituții publice: Implementarea unui sistem informatic integrat la nivelul primăriei poate contribui la îmbunătățirea relațiilor cu guvernul central și alte instituții publice, facilitând schimbul de informații și colaborarea între diferite niveluri ale administrației publice.
- Comunitatea de dezvoltare și implementare IT: Companiile și experții IT implicați în dezvoltarea și implementarea sistemului informatic integrat vor beneficia de experiență și expertiză în acest domeniu, care poate fi utilizată în alte proiecte similare.

Rezultate așteptate

Rezultatele așteptate ale implementării unui sistem informatic integrat pentru primărie includ:

- Eficiență crescută: îmbunătățirea proceselor prin automatizare și centralizare.
- Reducerea birocrației: accelerarea gestionării documentelor, cererilor și autorizațiilor.
- Securitatea datelor: gestionare centralizată și protejată a informațiilor.
- Comunicare și colaborare îmbunătățite: interconectare între departamente și angajați.
- Transparență sporită: acces facil la informații și date pentru funcționari.
- Accesibilitate crescută a serviciilor publice: servicii online ușor accesibile pentru cetățeni.
- Optimizarea resurselor: monitorizare eficientă a resurselor pentru planificare și alocare.
- Suport în luarea deciziilor: instrumente de analiză și raportare pentru decizii informate.
- Adaptabilitate și scalabilitate: sistemul se adaptează la nevoile în schimbare și evoluții tehnologice.
- Reducerea costurilor: reducerea cheltuielilor administrative și utilizarea eficientă a resurselor.

I. Context & Justificare

Primăria Bistrița are nevoie de un sistem informatic capabil să susțină o organizație digitalizată robust, caracterizat de: eficiență, integrare, scalabilitate, securitate, flexibilitate, transparență decizională, accesibilitate (atât în cadrul instituției & în afara instituției). Situația prezentă a sistemului informatic implementat în cadrul instituției Primăriei prezintă carențe și riscuri semnificative pe toate dimensiunile menționate și, în consecință, nu poate asigura capacitățile și funcționalitățile necesare pentru a susține majoritatea scenariilor de digitalizare robustă propuse.

Prin implementarea acestui proiect, se va crea o platformă centralizată care va îmbunătăți semnificativ modul în care administrația publică locală își gestionează activitatea și interacționează cu cetățenii. Un sistem informatic integrat va automatiza procesele și fluxurile de lucru, reducând birocrația și accelerând gestionarea documentelor și cererilor cetățenilor. Acest lucru va avea ca rezultat o eficiență crescută, o mai bună colaborare între departamente și un nivel sporit de transparență în luarea deciziilor.

În plus, implementarea unui astfel de sistem va permite cetățenilor să acceseze și să solicite servicii publice online, îmbunătățind astfel accesibilitatea și satisfacția față de serviciile oferite. Acest lucru va contribui la îmbunătățirea calității vieții pentru comunitate și la o mai mare implicare a cetățenilor în procesele locale de guvernare.

Implementarea sistemului informatic integrat va conduce, de asemenea, la optimizarea utilizării resurselor și reducerea costurilor administrative. În contextul constrângerilor bugetare și al nevoii de a aloca resursele în mod eficient, acest sistem va permite administrației să facă economii semnificative și să aloce resursele către alte proiecte și servicii esențiale pentru comunitate.

În concluzie, implementarea unui sistem informatic integrat în cadrul primăriei reprezintă o investiție strategică și necesară pentru a îmbunătăți eficiența, transparența și accesibilitatea administrației publice locale, asigurând în același timp o utilizare optimă a resurselor și o mai bună satisfacție a cetățenilor.

Probleme

Din analiza datelor preliminare rezultă carențe semnificative pe următoarele dimensiuni:

1. Redundanța datelor și informațiilor (impact: mediu) – manifestată în gestionarea ineficientă a datelor, informații redundante și duplicate în diferite departamente și sisteme.
2. Birocrație și procese ineficiente (impact: mare) - manifestată în proceduri birocratice îndelungate și la întârzieri în procesarea documentelor, cererilor și autorizațiilor, ceea ce afectează negativ satisfacția cetățenilor și eficiența administrației.
3. Comunicare și colaborare redusă între departamente (impact: mediu) – manifestate în comunicații și colaborare între diferitele departamente dificile și ineficiente, probleme în coordonarea și implementarea politicilor și strategiilor locale.
4. Acces limitat la informații și date (impact: mediu) – manifestată în acces limitat și neuniform la informații și date, adoptarea unor decizii mai puțin informate, transparență redusă în gestionarea resurselor și alocarea bugetului.
5. Dificultăți în monitorizarea și raportarea rezultatelor (impact: redus) – manifestate în dificultatea de a monitoriza și evalua eficiența și impactul proceselor, a politicilor și/sau programelor locale.
6. Servicii publice cu accesibilitate redusă (impact: mare) – manifestate în capacitate redusă a cetățenilor să acceseze și să solicite servicii publice online, deplasare fizică la primărie și timp pierdut, satisfacție redusă cu privire la activitatea instituție din partea cetățenilor.
7. Gestionare ineficientă a resurselor (impact: mediu) – manifestate în lipsă monitorizare eficientă a resurselor, dificultăți în planificarea și alocarea resurselor în mod optim.

8. Securitatea redusă a datelor și riscul de pierdere a datelor (impact: mediu) – manifestate în risc crescut de pierdere a datelor sau acces neautorizat la informații sensibile, colapsul încrederii cetățenilor.

9. Costuri administrative ridicate (impact: redus) – manifestate în lipsă automatizare procese, eficiență redusă a operațiunilor, costuri administrative ridicate, utilizare mai puțin eficientă a resurselor financiare și umane.

Oportunități

- Eficientizarea proceselor interne
- Îmbunătățirea comunicației și colaborării între departamente
- Accesibilitate crescută a serviciilor publice
- Transparență și luare de decizii informate
- Monitorizarea și evaluarea eficientă a programelor și proiectelor
- Gestionarea optimă a resurselor
- Securitatea și protecția datelor
- Reducerea costurilor administrative
- Adaptabilitate și scalabilitate (la schimbări demografice, tehnologice, legislative)
- Îmbunătățirea reputației și a imaginii primăriei

Soluții la nevoi identificate

Soluțiile identificate țin atât de domeniul software cât și hardware și sunt listate mai jos:

1. Un sistem de management al bazelor de date: Aceasta va stoca toate datele relevante pentru administrația locală, precum datele cadastrale, taxele locale, datele de identificare ale cetățenilor și alte informații esențiale. În contextul unei primării, un astfel de sistem trebuie să fie capabil să gestioneze o varietate de tipuri de date, inclusiv date cadastrale, taxe locale, date de identificare ale cetățenilor și alte informații esențiale.
2. Aplicații software pentru departamentele cheie: Acestea includ sisteme pentru gestionarea resurselor umane, finanțelor și contabilității, achizițiilor publice, infrastructurii, urbanismului și dezvoltării locale, și altele. Caracteristici generale necesare: modularitate, interoperabilitate, securitate nativă, ușurință în utilizare, diapazon de personalizare & configurare, capacitate de automatizare și optimizare procese, procese de raportare și analiză integrate, scalabilitate, accesibilitate și mobilitate, capacitate nativă de integrare cu alte sisteme, conformitate cu reglementări, standarde și bune practici locale și naționale.
3. Un sistem de gestiune a documentelor: Un astfel de sistem va permite stocarea, accesarea și gestionarea documentelor electronice, precum hârtii oficiale, cereri, formulare și rapoarte. În cazul unei primării, un DMS este utilizat pentru a gestiona documente precum hârtii oficiale, cereri, formulare, rapoarte și alte înregistrări administrative și trebuie să aibă următoarele caracteristici: import și captură de documente în diverse formate, capacitate de organizare flexibilă a documentelor (ierarhii, etichetare), stocare centralizată și securizată, control al versionării, mecanisme de colaborare și partajare, funcții pentru crearea și gestionarea de fluxuri de lucru, precum aprobări, revizuiri și semnături electronice, capacitate de a gestiona eficient arhivarea, facilități de interoperabilitate și integrare, funcții care să asigure accesibilitatea și mobilitatea, funcții de raportare și audit.
4. Un sistem de workflow și automatizare: Acesta va facilita procesele interne și va reduce timpul necesar pentru a rula și coordona diferite sarcini în cadrul administrației locale. Caracteristici importante: motor de workflow, proiectare și modelare de procese, integrare cu alte sisteme, monitorizare și raportare.
5. Un portal web pentru cetățeni: Portalul trebuie să ofere informații actualizate despre serviciile și programele oferite de primărie, precum și posibilitatea de a depune cereri, plăti taxe și accesa documente în format electronic. Caracteristici esențiale: interfață accesibilă și intuitivă, acces la resurse și informații, interactivitate în procese, accesibilitate (WCAG / Web Content Accessibility Guidelines), securitate și protecția datelor (e.g. în conformitate cu reglementări de tipul GDPR).
6. Soluții de comunicare și colaborare: Soluții software pentru a facilita comunicarea între angajații primăriei, inclusiv email, chat, videoconferințe, platforme de colaborare în timp real (e.g. Microsoft SharePoint, Google Workspace, Atlassian Confluence și Trello); toate fiind securizate de un sistem de autentificare de tip Single Sign On / SSO și criptarea informațiilor end-to end.
7. Soluții de securitate și protecția datelor: Soluții și măsuri adecvate pentru a asigura protecția și confidențialitatea datelor și a informațiilor stocate în cadrul sistemului. Pentru a asigura protecția și confidențialitatea datelor,

următoarele componente trebuie implementate: set politici, proceduri și standarde de securite, soluții de criptare a datelor (e.g AES-256 și TLS), soluții de autentificare și autorizare, detecție și protecția împotriva atacurilor cibernetice, soluții de backup redundant și recuperare a datelor.

8. Soluții care cresc interoperabilitatea: Abilitatea de a se integra și comunica cu alte sisteme software, cum ar fi cele ale agențiilor guvernamentale, autorităților locale și regionale și alți furnizori de servicii. Interoperabilitatea este esențială pentru un sistem informatic integrat într-o primărie, în special în contextul legislației europene și colaborării cu alte agenții guvernamentale, autorități locale și regionale și furnizori de servicii. Caracteristici esențiale: standarde și protocoale comune (XML, JSON, RDF și CSV pentru reprezentarea și schimbul de date, precum și HTTP, HTTPS, SOAP și REST pentru comunicarea între sisteme), conformitatea cu legislația și standardele europeane (EIF - European Interoperability Framework, Core Public Service Vocabulary Application Profile / CPSV-AP, ISA² Core Vocabularies sau European Interoperability Reference Architecture / EIRA), API-uri și servicii web (RESTful, GraphQL sau gRPC), sistem de management al identității și accesului (conforme standardelor SAML, OpenID Connect sau OAuth), middleware și adaptori (e.g. soluții de Enterprise Service Bus /ESB, Data Integration Tools), integrarea cu alte platforme și soluții (e.g. sisteme e-guvernare, platforme de achiziții publice, soluții de management al datelor cadastrale).
9. Scalabilitate și flexibilitate: Sistemul ar trebui să poată fi ușor adaptat și extins pentru a face față cerințelor viitoare și pentru a permite implementarea de noi funcționalități și servicii caracterizate de: utilizare microservicii, cloud computing, containerizare și orchestrare (e.g. Docker, Kubernetes), soluții de monitorizare și management al performanței, sistem de gestionare a schimbărilor, compatibilitate și interoperabilitate nativă (standarde și protocoale deschise și bine stabilite, precum RESTful APIs, JSON, XML și OAuth).

II. Obiective & Rezultate

Obiective termen scurt

1. Definirea și crearea unei arhitecturi informatice integrate, scalabile și redundante, capabile să susțină o paletă cât largă de scenarii de digitalizare a instituției
2. Eficiență sporită & reducerea birocrației: automatizarea proceselor și operațiunilor, reducerea redundanței datelor și centralizarea informațiilor pentru a îmbunătăți eficiența în cadrul administrației publice locale; digitalizarea proceselor și fluxurilor de lucru pentru a reduce birocrația și a accelera gestionarea și procesarea documentelor, cererilor și autorizațiilor.
3. Gestionarea datelor într-un mod centralizat și securizat: Stocarea și gestionarea datelor într-un mod centralizat, pentru a asigura protecția și securitatea informațiilor și a preveni pierderea de date și accesul neautorizat.
4. Îmbunătățirea comunicării și colaborării: Interconectarea diferitelor departamente și funcționari pentru a îmbunătăți comunicarea și colaborarea între aceștia.
5. Accesibilitate crescută: implementarea unui sistem care să permită cetățenilor să acceseze și să solicite servicii publice online, simplificând interacțiunea cu administrația locală și îmbunătățind experiența utilizatorilor.

Obiective termen lung

1. Transparență îmbunătățită: Crearea unui sistem care să faciliteze accesul la informații și date în timp real pentru funcționari, conducând la o mai mare transparență în luarea deciziilor și gestionarea resurselor.
2. Optimizarea resurselor: Dezvoltarea unui sistem care să permită o monitorizare eficientă a resurselor, facilitând planificarea și alocarea acestora într-un mod optim.
3. Suport pentru luarea deciziilor: Crearea unui sistem care să ofere instrumente de analiză și raportare pentru a ajuta la luarea deciziilor informate și la evaluarea eficienței politicii și strategiilor locale.
4. Adaptabilitate și scalabilitate: Implementarea unui sistem informatic integrat care să poată fi adaptat și extins pentru a răspunde nevoilor în continuă schimbare ale administrației publice locale și pentru a se adapta la evoluțiile tehnologice și legislative.
5. Reducerea costurilor: Realizarea unui sistem care să automatizeze procesele și să eficientizeze operațiunile, contribuind la o reducere a costurilor administrative și la o utilizare mai eficientă a resurselor financiare și umane.

Măsurarea & evaluarea obiectivelor

Măsurare obiective pe termen scurt

Nr.	Obiectiv	Modalități de evaluare
1	**Definirea și crearea unei arhitecturi informatice integrate, scalabile și redundante**	a) Documentația tehnică și arhitectura sistemului propusă
		b) Testarea și evaluarea performanței și redundanței sistemului în diferite scenarii de încărcare și în cazul unor incidente
		c) Capacitatea de a susține o gamă largă de aplicații și servicii
2	**Eficiență sporită & reducerea birocrației**	a) Procentul de procese și operațiuni automate
		b) Reducerea timpului mediu de procesare a documentelor, cererilor și autorizațiilor
		c) Reducerea erorilor și a redundanței datelor

3	**Gestionarea datelor într-un mod centralizat și securizat**	a) Procentul de date stocate și gestionate în sistemul centralizat
		b) Măsurarea și evaluarea securității informației și a nivelului de protecție a datelor personale
		c) Numărul de incidente de securitate înregistrate și rezolvate într-un anumit interval de timp
4	**Îmbunătățirea comunicării și colaborării**	a) Gradul de interconectare între departamente și funcționari / angajați
		b) Evaluarea eficienței comunicării și colaborării prin sondaje de opinie și feedback-ul angajaților
		c) Numărul de proiecte și sarcini realizate în echipă și în colaborare într-un anumit interval de timp, numărul de colaboratori implicați
5	**Accesibilitate crescută**	a) Numărul de servicii publice online disponibile pentru cetățeni
		b) Reducerea timpului necesar pentru a accesa și solicita servicii publice online
		c) Sondaje de opinie și feedback-ul cetățenilor privind accesibilitatea și experiența utilizatorilor

Măsurare obiective pe termen lung

Nr.	Obiectiv	Modalități de evaluare
1	**Transparență îmbunătățită**	a) Procentul de documente și informații accesibile publicului în format electronic din numărul total de documente accesibile
		b) Timpul mediu necesar pentru a obține informații sau date solicitate de cetățeni sau alte părți interesate
		c) Sondaje de opinie și feedback-ul cetățenilor privind accesibilitatea și transparența informațiilor
2	**Optimizarea resurselor**	a) Procentul de reducere a cheltuielilor administrative datorate utilizării eficiente a resurselor
		b) Gradul de îndeplinire a planurilor și proiectelor locale în cadrul resurselor alocate
		c) Rapoarte de monitorizare și evaluare a utilizării resurselor pe diferite proiecte și activități
3	**Suport pentru luarea deciziilor**	a) Numărul de rapoarte și analize realizate în baza datelor sistemului informatic integrat
		b) Gradul de îmbunătățire a procesului decizional în termen de scăderea timpului decizional și creșterea calității actului decizonal și de evaluare a eficienței politicilor și strategiilor locale
		c) Feedback-ul funcționarilor și a conducerii primăriei privind utilitatea instrumentelor de analiză și raportare
4	**Adaptabilitate și scalabilitate**	a) Capacitatea sistemului de a se adapta la modificări legislative sau tehnologice fără a necesita resurse semnificative sau timp îndelungat
		b) Ușurința cu care pot fi adăugate noi funcționalități sau extinse serviciile oferite de sistem

		c) Numărul de noi servicii și funcționalități implementate în sistem într-un anumit interval de timp
5	Reducerea costurilor	a) Procentul de reducere a costurilor administrative datorate implementării sistemului informatic integrat
		b) Reducerea timpului de procesare a cererilor și a sarcinilor administrative
		c) Economisirea resurselor financiare și umane care pot fi realocate pentru alte proiecte sau servicii publice

Rezultate așteptate

Rezultatele așteptate ale implementării unui sistem informatic integrat pentru primărie includ:

- Eficiență crescută: Automatizarea proceselor și operațiunilor, reducerea redundanței datelor și centralizarea informațiilor vor duce la o îmbunătățire semnificativă a eficienței în cadrul administrației publice locale.
- Reducerea birocrației: Digitalizarea proceselor și fluxurilor de lucru va duce la reducerea birocrației și la accelerarea gestionării și procesării documentelor, cererilor și autorizațiilor.
- Gestionarea centralizată și securizată a datelor: Stocarea și gestionarea datelor într-un mod centralizat va asigura protecția și securitatea informațiilor și va preveni pierderea de date și accesul neautorizat.
- Comunicare și colaborare îmbunătățite: Interconectarea diferitelor departamente și funcționari va îmbunătăți comunicarea și colaborarea între aceștia, facilitând coordonarea și luarea deciziilor.
- Transparență sporită: Accesul la informații și date în timp real pentru funcționari va conduce la o mai mare transparență în luarea deciziilor și gestionarea resurselor.
- Accesibilitate crescută a serviciilor publice: Implementarea unui sistem care să permită cetățenilor să acceseze și să solicite servicii publice online va simplifica interacțiunea cu administrația locală și va îmbunătăți experiența utilizatorilor.
- Optimizarea resurselor: Dezvoltarea unui sistem care să permită o monitorizare eficientă a resurselor va facilita planificarea și alocarea acestora într-un mod optim.
- Suport pentru luarea deciziilor: Sistemul va oferi instrumente de analiză și raportare pentru a ajuta la luarea deciziilor informate și la evaluarea eficienței politicii și strategiilor locale.
- Adaptabilitate și scalabilitate: Sistemul informatic integrat va putea fi adaptat și extins pentru a răspunde nevoilor în continuă schimbare ale administrației publice locale și pentru a se adapta la evoluțiile tehnologice și legislative.
- Reducerea costurilor: Implementarea sistemului va automatiza procesele și va eficientiza operațiunile, contribuind la o reducere a costurilor administrative și la o utilizare mai eficientă a resurselor financiare și umane.

III. Plan de implementare

Activitățile principale

- Realizarea unui audit tehnic și funcțional al sistemelor existente: analiza sistemelor și infrastructurii IT existente, identificarea punctelor tari și a punctelor slabe, precum și stabilirea cerințelor tehnice și funcționale pentru noul sistem.
- Crearea unei echipe de proiect multidisciplinare: echipa trebuie să includă reprezentanți din diferite departamente, precum IT, management, resurse umane, financiar, juridic și comunicare, precum și experți externi în domeniul tehnologiei informației și al transformării digitale.
- Definirea obiectivelor și a indicatorilor de performanță ai proiectului: dezvoltarea unei baze solide pentru a măsura progresul și succesul implementării sistemului informatic integrat.
- Selecția soluțiilor hardware și software: evaluarea și compararea diferitelor soluții disponibile pe piață, în funcție de cerințele identificate în auditul tehnic și funcțional; evaluarea interdependențelor reciproce între soluțiile de hardware și software în vederea eliminării incompatibilităților și/sau limitărilor create de acestea
- Achiziția soluțiilor hardware și software: evaluarea și compararea diferitelor soluții disponibile pe piață, în funcție de bugetul alocat proiectului, a condițiilor de livrare, service și suport pe durata ciclului de viață a produselor și serviciilor
- Dezvoltarea și personalizarea soluțiilor software: configurarea și personalizarea soluțiilor software achiziționate pentru a se potrivi nevoilor și proceselor specifice ale primăriei.
- Implementarea infrastructurii hardware și a soluțiilor software: instalarea și configurarea echipamentelor hardware și a soluțiilor software, inclusiv integrarea acestora cu sistemele existente.
- Migrarea datelor și a informațiilor existente: transferul și consolidarea datelor și informațiilor din sistemele vechi către noul sistem informatic integrat, precum și verificarea integrității și acurateței acestora.
- Testarea și validarea sistemului: verificarea funcționalității și a performanței noului sistem informatic integrat, precum și identificarea și remedierea eventualelor probleme și deficiențe.
- Pregătirea personalului și dezvoltarea competențelor: organizarea de sesiuni de instruire și workshop-uri pentru a familiariza personalul cu noul sistem și a dezvolta competențele necesare pentru utilizarea eficientă a acestuia.
- Lansarea și monitorizarea sistemului: punerea în funcțiune a noului sistem informatic integrat și monitorizarea performanței și eficienței acestuia în timp real, precum și ajustarea și îmbunătățirea continuă a acestuia pe baza feedback-ului și a nevoilor identificate.
- Evaluarea impactului și a rezultatelor proiectului: măsurarea și raportarea progresului și succesului proiectului în funcție de obiectivele și indicatorii de performanță stabiliți

Responsabilități

Echipa responsabilă de proiect va fi formata din specialiști cu experiență în domeniul IT, management, resurse umane, financiar, juridic și comunicare, precum și experți externi în domeniul tehnologiei informației și al transformării digitale.

Primăria Bistrița va fi responsabila de supervizarea și coordonarea proiectului, asigurând o buna comunicare intre membrii echipei de proiect.

Durata proiectului

Durata estimată de implementare a proiectului se ridică la 16 -20 luni.

Nr	Activitate	Durată estimată (săpt.)
1	Realizarea unui audit tehnic și funcțional al sistemelor existente: analiza sistemelor și infrastructurii IT existente, identificarea punctelor tari și a punctelor slabe, precum și stabilirea cerințelor tehnice și funcționale pentru noul sistem.	4
2	Crearea unei echipe de proiect multidisciplinare: echipa trebuie să includă reprezentanți din diferite departamente, precum IT, management, resurse umane, financiar, juridic și comunicare, precum și experți externi în domeniul tehnologiei informației și al transformării digitale.	3
3	Definirea obiectivelor și a indicatorilor de performanță ai proiectului: dezvoltarea unei baze solide pentru a măsura progresul și succesul implementării sistemului informatic integrat.	3
4	Selecția soluțiilor hardware și software: evaluarea și compararea diferitelor soluții disponibile pe piață, în funcție de cerințele identificate în auditul tehnic și funcțional; evaluarea interdependențelor reciproce între soluțiile de hardware și software în vederea eliminării incompatibilităților și/sau limitărilor create de acestea	6
5	Achiziția soluțiilor hardware și software: evaluarea și compararea diferitelor soluții disponibile pe piață, în funcție de bugetul alocat proiectului, a condițiilor de livrare, service și suport pe durata ciclului de viață a produselor și serviciilor	10
6	Dezvoltarea și personalizarea soluțiilor software: configurarea și personalizarea soluțiilor software achiziționate pentru a se potrivi nevoilor și proceselor specifice ale primăriei.	20
7	Implementarea infrastructurii hardware și a soluțiilor software: instalarea și configurarea echipamentelor hardware și a soluțiilor software, inclusiv integrarea acestora cu sistemele existente.	20
8	Migrarea datelor și a informațiilor existente: transferul și consolidarea datelor și informațiilor din sistemele vechi către noul sistem informatic integrat, precum și verificarea integrității și acurateței acestora.	10
9	Testarea și validarea sistemului: verificarea funcționalității și a performanței noului sistem informatic integrat, precum și identificarea și remedierea eventualelor probleme și deficiențe.	4
10	Pregătirea personalului și dezvoltarea competențelor: organizarea de sesiuni de instruire și workshop-uri pentru a familiariza personalul cu noul sistem și a dezvolta competențele necesare pentru utilizarea eficientă a acestuia.	9
11	Lansarea și monitorizarea sistemului: punerea în funcțiune a noului sistem informatic integrat și monitorizarea performanței și eficienței acestuia în timp real, precum și ajustarea și îmbunătățirea continuă a acestuia pe baza feedback-ului și a nevoilor identificate.	2
12	Evaluarea impactului și a rezultatelor proiectului: măsurarea și raportarea progresului și succesului proiectului în funcție de obiectivele și indicatorii de performanță stabiliți	2
	TOTAL	93

IV. Sustenabilitate & impact

Finanțarea & Construcția bugetului

Construcția și valoarea totală a bugetului proiectului va fi proiectată pentru a putea varia în funcție de opțiunile strategice ale instituției Primăriei Bistrița, a priorităților proiectelor de digitalizare și a resurselor disponibile. Construcția bugetului va include următoarele categorii de costuri:

- Costuri legate de analiză, consultanță și audit
- Costuri legate de achiziția soluțiilor hardware
- Costuri legate de achiziția soluțiilor software
- Costuri legate de dezvoltarea și personalizarea soluțiilor
- Costuri legate instalarea și configurarea echipamentelor hardware
- Costuri legate de migrarea datelor
- Costuri legate de training și formare resurse umane

În funcție de specificul și dimensiunea proiectului, bugetul total poate varia între 850.000 și 1.500.000 EUR. Este important să se realizeze o estimare detaliată a costurilor și o alocare corespunzătoare a resurselor pentru a asigura succesul proiectului și implementarea tuturor măsurilor necesare pentru protejarea, operarea eficientă și reziliența sistemului integrat informatic.

Sustenabilitate

Sustenabilitatea proiectului va fi asigurată prin:

- Stabilirea unui plan de întreținere și actualizare continuă a sistemului: Dezvoltarea unui plan care să prevadă actualizări regulate ale software-ului și hardware-ului, pentru a menține securitatea și eficiența sistemului pe termen lung.
- Asigurarea finanțării pe termen lung: Identificarea unor surse stabile de finanțare pentru implementarea, întreținerea și dezvoltarea continuă a sistemului, inclusiv fonduri guvernamentale, fonduri europene sau alte surse de finanțare.
- Formarea și dezvoltarea personalului: Organizarea de cursuri de formare și dezvoltare profesională pentru personalul primăriei, pentru a asigura o utilizare eficientă și sustenabilă a sistemului.
- Implementarea unui sistem de monitorizare și evaluare: Monitorizarea și evaluarea performanței sistemului în mod regulat, pentru a identifica posibile probleme și a asigura eficiența acestuia pe termen lung.
- Încheierea unor contracte de suport tehnic și mentenanță cu furnizorii de software și hardware: Aceste contracte vor asigura suportul tehnic necesar pentru remedierea eventualelor probleme și pentru menținerea sistemului într-o stare de funcționare optimă.
- Dezvoltarea de parteneriate cu alte instituții și organizații: Stabilirea unor parteneriate cu alte primării, instituții guvernamentale, universități și organizații pentru a împărtăși bune practici și resurse în domeniul sistemelor informatice integrate.
- Implementarea unei strategii de comunicare și diseminare a informațiilor: Dezvoltarea și punerea în aplicare a unei strategii de comunicare pentru a informa cetățenii și alte părți interesate despre beneficiile și rezultatele sistemului, pentru a crește gradul de acceptare și utilizare.
- Stabilirea unor proceduri și politici de securitate a datelor și a informațiilor: Implementarea unor măsuri de protecție adecvate pentru a asigura securitatea și confidențialitatea datelor și informațiilor stocate în cadrul sistemului.
- Documentarea și standardizarea proceselor și procedurilor: Elaborarea unor documente care să descrie în detaliu procesele și procedurile asociate cu sistemul informatic, pentru a facilita gestionarea, dezvoltarea și întreținerea acestuia pe termen lung.

Impact social, economic, mediu

Impactul social, economic și de mediu al proiectului va fi pozitiv și se va manifesta prin:

Impact social:

- Accesibilitate sporită: Implementarea unui sistem informatic integrat va facilita accesul cetățenilor la serviciile oferite de primărie, inclusiv informații și formulare online. Astfel, se va îmbunătăți comunicarea și interacțiunea dintre cetățeni și administrația locală.
- Transparență și responsabilitate: Un astfel de sistem va permite o mai bună monitorizare și control al activităților desfășurate în cadrul primăriei, contribuind la transparența și responsabilizarea instituției.
- Eficientizarea proceselor interne: Personalul primăriei va beneficia de un mediu de lucru mai eficient și organizat, ceea ce va duce la creșterea productivității și îmbunătățirea serviciilor oferite.

Impact economic:

- Reducerea costurilor administrative: Prin digitalizarea proceselor și serviciilor, primăria va economisi resurse financiare și umane, reducând costurile administrative.
- Creșterea veniturilor: O mai bună gestionare a resurselor și optimizarea colectării taxelor și impozitelor vor duce la creșterea veniturilor locale.
- Atracția de investiții: O administrație locală eficientă și transparentă este mai atractivă pentru investitori, ceea ce poate contribui la dezvoltarea economică a comunității.

Impact de mediu:

- Reducerea consumului de hârtie: Digitalizarea documentelor și a proceselor de lucru va duce la o scădere semnificativă a consumului de hârtie, ceea ce va avea un impact pozitiv asupra mediului.
- Reducerea emisiilor de carbon: Implementarea unui sistem informatic integrat va reduce necesitatea deplasărilor cetățenilor și a personalului primăriei pentru a accesa și furniza anumite servicii, contribuind astfel la diminuarea emisiilor de carbon.
- Promovarea practicilor sustenabile: Un sistem informatic eficient poate ajuta la monitorizarea și gestionarea mai bună a resurselor naturale și a infrastructurilor, promovând astfel dezvoltarea durabilă în cadrul comunității.

V. Anexe

Diagrama simplificată a unei arhitecturi care respectă interoperabilitatea: