

Beneficiar: COMUNA GORGOTA , județul Prahova, sat Gorgota, str. Principală , nr.70,
Ordonator principal de credite: COMUNA GORGOTA ,
Elaboratorul studiului de fezabilitate: TRUST BGE CONF S.R.L.

Nr. 2/09.04.2025

PROIECT TEHNIC pentru proiectele care au exclusiv componente specifice tehnologiei
informațiilor și comunicațiilor (TIC)
Digitalizarea în Administrațiile Publice-com.Gorgota, jud.Prahova

Denumirea Beneficiarului:	Comuna Gorgota
Numele reprezentantului legal:	Primar Dumitru Ionuț-Nicolae
Sediu:	Com. Gorgota, str. Principală nr. 70, jud. Prahova
CIF:	2845354
Telefon/Fax/Mobil:	0244474511; 0722514823
Adresă de e-mail:	primar@primariagorgota.ro
Locația de implementare a proiectului:	Primăria Comunei Gorgota, com. Gorgota, str. Principală, nr. 70, jud. Prahova

1. OBIECTIVELE PROIECTULUI

De ce este importantă digitalizarea?

- **Eficiență:** Automatizarea proceselor reduce timpul și costurile asociate cu activitățile administrative.
- **Transparență:** Accesul la informații publice devine mai facil și mai rapid, crescând gradul de încredere al cetățenilor în instituții.
- **Accesibilitate:** Serviciile publice pot fi accesate de oriunde și oricând, eliminând barierele geografice și temporale.
- **Interacțiune îmbunătățită:** Cetățenii pot interacționa cu instituțiile publice într-un mod mai intuitiv și mai personalizat.
- **Competitivitate:** Digitalizarea contribuie la creșterea competitivității economice, facilitând dezvoltarea localității.

Scopul principal al proiectului de digitalizare este de a realiza un Sistem Informatic Integrat și Interoperabil pentru Digitalizarea Proceselor în cadrul Primăriei comunei GORGOTA, în vederea valorificării avantajelor digitalizării, în beneficiul cetățenilor, al operatorilor economici și al autorităților publice, prin investiții în dezvoltarea infrastructurii, serviciilor și echipamentelor IT relevante și necesare la nivelul comunei GORGOTA, județ Prahova și necesitatea retrodigitalizării a multiple documente disponibile doar în format fizic din cadrul Primăriei comunei GORGOTA.

Prin digitalizare, se urmărește:

- Simplificarea interacțiunii dintre cetățeni și administrație: Oferirea de servicii online, reducerea birocrăției și a timpului de așteptare, accesibilitate sporită la informații.
- Îmbunătățirea transparenței și a accesului la informație: Publicarea datelor publice, facilitarea participării cetățenilor la procesul decizional.
- Creșterea eficienței instituționale: Automatizarea proceselor interne, optimizarea fluxurilor de lucru, reducerea costurilor.
- Dezvoltarea economiei locale: Atragerea de investiții, crearea de noi locuri de muncă în sectorul IT.

În vederea implementării acestui proiect de digitalizare avem în vedere parcurgerea următoarelor etape:

- Analiza nevoilor: Identificarea deficiențelor existente și a potențialului de îmbunătățire.
- Proiectarea soluției: Elaborarea unei arhitecturi IT, selectarea tehnologiilor și a furnizorilor.
- Implementarea: Instalarea echipamentelor, configurarea software-ului, migrarea datelor.
- Testarea și punerea în funcțiune: Verificarea funcționalității sistemului, instruirea personalului.
- Întreținerea și dezvoltarea: Asigurarea suportului tehnic, actualizarea sistemului.

Pentru atingerea obiectivelor am analizat exemple de bune practici în domeniul digitalizării administrației publice, cum ar fi:

1. Danemarca - Focus pe utilizator

- Co-creare cu cetățenii: Serviciile online sunt concepute în colaborare cu cetățenii, asigurându-se că acestea corespund nevoilor reale ale utilizatorilor.
- Limbaj simplu și intuitiv: Interfețele serviciilor online sunt simple și ușor de utilizat, chiar și pentru persoanele cu cunoștințe limitate de tehnologie.

2. Finlanda - Transparență și deschidere

- Date publice deschise: O cantitate mare de date publice sunt disponibile în format deschis, facilitând inovarea și dezvoltarea de noi servicii.
- Platforme de participare civică: Cetățenii sunt încurajați să participe la procesul decizional prin intermediul platformelor online de consultare.

Lecții învățate, provocări și obiective propuse:

- Importanța unei viziuni strategice: Digitalizarea trebuie să fie parte integrantă dintr-o strategie mai amplă de dezvoltare a administrației publice locale.
- Colaborarea între instituții: Succesul digitalizării depinde de o bună coordonare între diferitele niveluri de administrație și între diferitele instituții.
- Investiții în infrastructură IT: Este necesară o infrastructură IT modernă și sigură pentru a susține serviciile digitale.
- Formarea personalului: Funcționarii publici trebuie să fie pregătiți pentru a utiliza noile tehnologii și a oferi suport cetățenilor.
- Securitatea datelor: Protejarea datelor cu caracter personal este o prioritate absolută.

Beneficiile digitalizării pentru cetățeni

- Servicii publice online: Acces facil la o gamă largă de servicii, de la obținerea de documente până la plata taxelor și impozitelor.
- Interacțiune personalizată: Comunicare directă cu instituțiile publice prin intermediul unor canale digitale.
- Transparență și responsabilitate: Acces la informații publice relevante și posibilitatea de a formula reclamații.
- Reducerea birocrăției: Simplificarea procedurilor administrative și eliminarea duplicatelor.

În concluzie, digitalizarea administrației publice locale este un proces continuu, care aduce beneficii atât pentru cetățeni, cât și pentru instituții (locale, regionale și nu numai). Prin adoptarea unor bune practici și prin învățarea din experiența altor țări, România poate avansa semnificativ pe calea transformării digitale.

Obiective specifice:

- Creșterea cu un număr de 5 softuri aferente serviciilor publice digitalizate în interesul cetățenilor.
- Creșterea utilizării a sistemelor/serviciilor digitale de către angajați la 85%.
- Creșterea eficienței în furnizarea de servicii publice la 40%

La stabilirea obiectivelor specifice, s-a ținut cont de următoarele aspecte:

- Nevoile cetățenilor: Obiectivele trebuie să se alinieze cu nevoile și așteptările cetățenilor.
- Contextul local: Obiectivele trebuie să fie adaptate la specificul fiecărei instituții și al comunității pe care o servește.
- Resursele disponibile: Obiectivele trebuie să fie realizabile în funcție de resursele financiare, umane și tehnologice disponibile.
- Indicatori de performanță: astfel cum au fost definiți în cadrul prezentului proiect și care permit măsurarea progresului.

Prin acest proiect se urmărește:

- Crearea unei **platforme integrate** care să permită interoperabilitatea aplicațiilor existente și gestionarea centralizată a datelor;
- **Digitalizarea completă** a proceselor interne și retrodigitalizarea arhivei fizice;
- Implementarea unor **soluții moderne de securitate cibernetică** pentru protejarea datelor;
- Asigurarea unui acces facil și transparent la informații pentru cetățeni și mediul de afaceri;
- **Formarea personalului** pentru utilizarea eficientă a noilor sisteme.

Proiectul de digitalizare a administrației publice din Comuna Gorgota, județul Prahova, are ca obiectiv principal modernizarea infrastructurii IT și integrarea soluțiilor digitale pentru a eficientiza serviciile publice oferite cetățenilor și pentru a îmbunătăți transparența și accesibilitatea acestora. Auditul de maturitate digitală a evidențiat faptul că nivelul actual al digitalizării în administrația locală este incipient, ceea ce face necesară o intervenție substanțială pentru transformarea proceselor administrative într-un mediu digital modern, securizat și integrat.

Digitalizarea administrației publice nu reprezintă doar o modernizare tehnologică, ci și o reformă fundamentală a modului în care autoritățile interacționează cu cetățenii. Prin implementarea unor soluții

digitale avansate, Comuna Gorgota va putea să ofere servicii mai eficiente, să reducă timpul de procesare a solicitărilor și să îmbunătățească accesul populației la informații și servicii esențiale. De asemenea, proiectul vizează îmbunătățirea securității cibernetice și conformitatea cu reglementările privind protecția datelor, asigurând astfel un mediu digital sigur pentru toate părțile implicate.

➤ **Modernizarea infrastructurii IT**

Pentru a putea implementa soluțiile digitale necesare, infrastructura IT existentă trebuie să fie actualizată și extinsă. În acest sens, proiectul include achiziția de echipamente hardware și software moderne, care vor asigura performanță, scalabilitate și eficiență energetică. Echipamentele IT propuse includ 15 stații de lucru performante pentru angajații primăriei, servere de înaltă disponibilitate pentru stocarea și procesarea datelor, soluții de rețelistică avansate, precum și echipamente de securitate cibernetică pentru protecția infrastructurii digitale.

Instalarea și configurarea acestor echipamente vor fi realizate în conformitate cu cele mai bune practici în domeniul IT, asigurând compatibilitatea și interoperabilitatea acestora cu soluțiile software ce urmează a fi implementate. De asemenea, se va pune un accent deosebit pe utilizarea tehnologiilor eficiente energetic, care să reducă consumul de electricitate și impactul asupra mediului.

➤ **Soluții software pentru eficientizarea proceselor administrative**

Implementarea unor soluții software integrate este esențială pentru digitalizarea administrației publice. În acest sens, proiectul prevede achiziția și dezvoltarea unor aplicații care să faciliteze gestionarea documentelor, automatizarea proceselor administrative și îmbunătățirea comunicării cu cetățenii.

Una dintre prioritățile proiectului este implementarea unui sistem de gestiune a documentelor, care să permită arhivarea electronică, accesul facil la informații și eliminarea treptată a documentelor fizice. Acest sistem va permite integrarea cu alte baze de date existente și va facilita partajarea documentelor între departamente și instituții.

Totodată, vor fi dezvoltate aplicații pentru gestionarea taxelor și impozitelor locale, care să permită cetățenilor să efectueze plăți online și să acceseze istoricul obligațiilor fiscale. De asemenea, se va implementa un sistem de programări online pentru diverse servicii publice, reducând astfel aglomerația la ghișee și optimizând timpul de lucru al funcționarilor.

În plus, se va dezvolta o platformă de e-guvernare care să ofere acces la servicii publice digitale, permițând cetățenilor să depună cereri și petiții online, să urmărească stadiul acestora și să primească notificări în timp real. Această platformă va integra funcționalități de consultare publică și participare civică, permițând locuitorilor comunei să se implice activ în procesul decizional.

➤ **Implementarea tehnologiilor IoT și AI**

O componentă inovatoare a proiectului o reprezintă integrarea tehnologiilor IoT (Internet of Things) și AI (Inteligență Artificială) pentru îmbunătățirea serviciilor publice.

Prin utilizarea senzorilor IoT, administrația locală va putea monitoriza în timp real diverse aspecte ale comunității, precum calitatea aerului, nivelul de zgomot sau condițiile meteorologice. Aceste date vor fi afișate pe platforme digitale accesibile publicului, permițând cetățenilor să fie informați în timp util despre factorii de mediu care îi pot afecta.

În plus, tehnologiile AI vor fi utilizate pentru optimizarea proceselor administrative și îmbunătățirea interacțiunii cu cetățenii. De exemplu, implementarea unui chatbot bazat pe AI va permite utilizatorilor să obțină rapid informații despre serviciile publice disponibile, să primească asistență pentru completarea formularelor online și să obțină răspunsuri la întrebările frecvente.

➤ **Securitate cibernetică și protecția datelor**

Având în vedere creșterea numărului de atacuri cibernetice asupra instituțiilor publice, proiectul include măsuri riguroase pentru securizarea infrastructurii digitale. Printre acestea se numără implementarea de soluții avansate de protecție a rețelelor, criptarea datelor sensibile și aplicarea unor politici stricte de acces la informații.

Vor fi achiziționate și instalate firewall-uri de ultimă generație, sisteme de detecție și prevenire a intruziunilor, precum și soluții de backup automatizat pentru protejarea datelor împotriva pierderilor accidentale sau atacurilor de tip ransomware. De asemenea, angajații primăriei vor beneficia de sesiuni de instruire privind securitatea cibernetică, pentru a preveni eventualele breșe de securitate cauzate de erori umane.

În conformitate cu regulamentul GDPR și cu cerințele legislației naționale privind protecția datelor, toate soluțiile software implementate vor include funcționalități de anonimizare și control al accesului la informații, asigurând astfel confidențialitatea datelor cetățenilor.

➤ **Extinderea infrastructurii IT și conectivitate**

Pentru a susține digitalizarea administrației publice, se vor realiza investiții în infrastructura IT, inclusiv în extinderea rețelelor de fibră optică și modernizarea sistemelor de alimentare cu energie electrică. Aceste măsuri vor permite asigurarea unei conectivități stabile și rapide, necesare pentru funcționarea optimă a aplicațiilor digitale și pentru accesul online la serviciile publice.

În plus, se va analiza posibilitatea implementării unor puncte de acces Wi-Fi gratuit în zonele publice din comună, pentru a facilita accesul locuitorilor la internet și la resursele digitale puse la dispoziție de administrația locală.

2. ANALIZA SOLUȚIEI DIGITALE EXISTENTE LA NIVELUL BENEFICIARULUI

Sistemul informatic al Primăriei Gorgota este compus dintr-o serie de echipamente hardware, inclusiv stații de lucru, imprimante și routere, alături de o infrastructură software formată din aplicații de gestiune a documentelor, registre electronice și alte soluții digitale menite să sprijine activitatea instituției.

Dintre acestea, reamintim:

- 23 de Computere utilizate în diferite departamente ale Administrației Locale;
- Un Sistem de supraveghere video exterior;
- 9 Imprimante;
- 2 Access Router-e pentru conexiunea de internet a Primăriei;
- 2 Router-e pentru accesul intern la documente între utilizatori.

Ex. Softuri:

1. Aplicație impozite și taxe, neintegrabilă și perimată din punct de vedere tehnic și operațional;

2. Aplicație pentru contabilitate, neintegrabilă și perimată din punct de vedere tehnic și operațional;
3. Aplicație Registrul agricol, neintegrabilă și perimată din punct de vedere tehnic și operațional;
4. Site-web.

Cu toate acestea, nivelul de digitalizare al instituției este considerat incipient, ceea ce indică faptul că procesele digitale sunt realizate sporadic, fără a urma o strategie clară de transformare digitală. Lipsa unei strategii de digitalizare bine definite are ca efect o utilizare inefficientă a resurselor existente, ceea ce limitează capacitatea primăriei de a oferi servicii moderne cetățenilor.

Un aspect esențial al analizei soluției digitale existente este reprezentat de utilizarea tehnologiei pentru furnizarea de servicii către cetățeni. Deși Primăria Gorgota deține un website oficial și utilizează platforma Regista pentru gestiunea documentelor, utilizarea acesteia de către cetățeni este redusă. Un procent scăzut al populației accesează serviciile digitale oferite de instituție, ceea ce subliniază nevoia de promovare și instruire atât a angajaților, cât și a cetățenilor pentru a facilita adoptarea acestor soluții. Lipsa unui sistem eficient de informare a publicului contribuie la acest nivel redus de adoptare, iar educarea utilizatorilor finali, precum și dezvoltarea unei platforme de transparență al documentelor emise de Consiliul Local ar putea fi un prim pas spre creșterea interacțiunii digitale.

Un punct important al analizei este lipsa unui departament IT intern. Administrarea echipamentelor și a soluțiilor software este realizată prin contracte cu terți, ceea ce poate afecta timpul de reacție și eficiența rezolvării problemelor tehnice. De asemenea, lipsa unei strategii clare de securitate cibernetică este o deficiență majoră, instituția neavând implementate soluții de protecție avansate precum firewall-uri, EDR/XDR sau alte aplicații de securitate menite să prevină atacurile informatice. Un alt aspect esențial este lipsa unor proceduri de recuperare a datelor în cazul unui incident cibernetic sau a unui incident fizic (incendiu, calamități, vandalism, efracție, forță majoră etc.), ceea ce ar putea expune instituția la pierderi semnificative de informații critice.

Accesibilitatea serviciilor digitale reprezintă un alt punct slab al soluției existente. Deși platforma Regista oferă posibilitatea depunerii online a petițiilor, programării serviciilor și gestiunii documentelor, numărul utilizatorilor efectivi este scăzut. Acest lucru poate fi cauzat de lipsa unei campanii de informare a cetățenilor, dar și de nivelul redus de competențe digitale din comunitate. Un alt impediment este lipsa unei interfețe intuitive și adaptate nevoilor utilizatorilor, ceea ce reduce semnificativ atractivitatea utilizării acestor servicii. Implementarea unor funcționalități interactive și personalizate ar putea atrage un număr mai mare de utilizatori.

Pe de altă parte, există și aspecte pozitive în cadrul infrastructurii digitale existente. Conectivitatea internetului este asigurată printr-o conexiune de fibră optică de 100MB/s, furnizată de Orange, ceea ce permite desfășurarea activităților în condiții optime. De asemenea, utilizarea soluțiilor de cloud computing, prin contractele cu Regista Digital SA și SOBIS SOLUTIONS SRL, oferă o anumită flexibilitate în gestionarea documentelor și arhivarea electronică a acestora. Cu toate acestea, lipsa unei arhive electronice complet implementate este o problemă care poate genera dificultăți în regăsirea și gestionarea documentelor istorice. Dezvoltarea unui sistem de arhivare digitală avansat ar contribui semnificativ la eficiența administrativă a instituției.

Un alt element de analiză este gradul de integrare al soluțiilor informatice existente cu alte sisteme publice. Lipsa interoperabilității cu instituții precum ANAF, ghișeul.ro sau RO-eID limitează eficiența serviciilor digitale și impune necesitatea dezvoltării unor soluții care să permită schimbul de date între diferite platforme guvernamentale. De asemenea, utilizarea inteligenței artificiale sau a tehnologiilor IoT este inexistentă, ceea ce ar putea reprezenta o direcție de dezvoltare viitoare pentru optimizarea serviciilor publice. Integrarea unor soluții bazate pe AI ar putea contribui la automatizarea proceselor administrative și la creșterea eficienței generale a instituției.

Așadar, soluția digitală existentă la nivelul Primăriei Comunei Gorgota prezintă numeroase puncte slabe care trebuie adresate pentru a asigura o digitalizare eficientă și funcțională. Implementarea unor soluții integrate, interoperabile și securizate, alături de o strategie clară de instruire a personalului și promovare a serviciilor digitale către cetățeni, sunt esențiale pentru creșterea nivelului de maturitate digitală al instituției. Investițiile în echipamente IT de generație nouă, dezvoltarea unor aplicații mobile intuitive și extinderea arhivei electronice sunt pași necesari în acest proces de transformare digitală.

3. CERINTE PRIVIND SOLUTIA TEHNICA

3.1. Cerinte generale

Scopul principal al investiției este dezvoltarea și implementarea unui Sistem Informatic Integrat și Interoperabil pentru Digitalizarea Proceselor în cadrul Primăriei comunei GORGOTA, în vederea valorificării avantajelor digitalizării, în beneficiul cetățenilor, al operatorilor economici și al autorităților publice, prin investiții în dezvoltarea infrastructurii, serviciilor și echipamentelor IT relevante și necesare la nivelul comunei GORGOTA, județ Prahova și necesitatea retrodigitalizării a multiple documente disponibile doar în format fizic din cadrul Primăriei comunei GORGOTA.

Sistemele trebuie să răspundă nevoilor tehnice ale autorității, să fie accesibile și exploatabile în mod intuitiv, astfel încât specialiștii și cetățenii să fie motivați să le utilizeze în scopul de raportare, respectiv informare.

În mod particular, Sistemul Informatic Integrat și Interoperabil va trebui să funcționeze ca un instrument de gestionare a informațiilor (Dashboard/Raportare) care primește și analizează date din bazele de date existente în scopul de a putea defini/iniția rapoarte, statistici și previziuni. Acesta reprezintă componenta cea mai complexă din cadrul investiției.

Rezultatele și impactul pozitiv al tuturor aplicațiilor propuse în cadrul acestui Studiu de Fezabilitate sunt:

- Reducerea birocrăției în procesele administrative;
- Îmbunătățire a transparenței și a accesului la informații publice;
- Eficiență sporită în procesele administrative;
- Reducerea erorilor în procesele administrative;
- Creșterea eficienței în furnizarea de servicii publice;
- Reducerea timpului necesar pentru procesare a cererilor administrative.

Autoritatea contractantă optează pentru **Opțiunea 1 din SF: Implementarea unui Sistem Informatic**

Integrat și Interoperabil Mixt bazat pe microservicii. Alternativa aceasta vizează o abordare modulară, în care fiecare componentă a sistemului este tratată ca un microserviciu independent. Aceasta permite o mai bună scalabilitate și flexibilitate, facilitând actualizările și integrarea de noi servicii fără a perturba funcționarea sistemelor existente. Microserviciile permit o personalizare extinsă și o adaptare ușoară la nevoile specifice ale administrației și ale utilizatorilor.

■ Ambele opțiuni sunt fundamentate pe principiul că eficiența administrativă și satisfacția cetățenilor constituie obiective critice. Fiecare opțiune reprezintă un pas către o administrație publică modernă, transparentă și eficientă, capabilă să răspundă prompt și precis nevoilor comunității.

■ Pentru a completa peisajul tehnologic și pentru a răspunde cerințelor comunității, fiecare opțiune include dezvoltarea unor softuri (ex. **Cadastru**), care vor funcționa ca o platformă centrală de acces la informații și servicii. Acestea vor promova transparența și va încuraja participarea publică, oferind cetățenilor și afacerilor posibilitatea de a interacționa direct cu datele puse la dispoziție de către administrația publică.

■ Aceste inițiative tehnologice sunt doar un segment al unei viziuni mai ample, care include și alte aplicații precum **Inventarierea patrimoniului** și procesul de **Retrodigitalizare**, fiecare contribuind semnificativ la îmbunătățirea accesului la informații și la eficientizarea proceselor administrative. Însumând, aceste elemente conturează o strategie comprehensivă de digitalizare, menită să aducă administrația publică din comuna GORGOTA mai aproape de cetățeni și de mediul de afaceri, printr-o utilizare inovatoare a tehnologiei.

- Achiziția și implementarea unui **Sistem Informatic Integrat** bazat pe tehnologii moderne, capabil să gestioneze eficient documentele și fluxurile informaționale;
- **Integrarea aplicațiilor existente** prin standardizarea formatelor de date și asigurarea compatibilității;
- Crearea unui portal online destinat interacțiunii cu cetățenii pentru depunerea și urmărirea cererilor, accesarea informațiilor publice și efectuarea plăților online;
- **Consolidarea infrastructurii IT** prin achiziția de servere, echipamente și soluții software performante;
- Dezvoltarea unei **politici de securitate cibernetică** robuste, în conformitate cu legislația națională și europeană.

Opțiunea 1 - Implementarea unui Sistem Informatic Integrat și Interoperabil Mixt bazat pe microservicii

Utilizarea arhitecturii bazate pe microservicii oferă un cadru solid pentru această inițiativă ambițioasă. În cazul de față, fiecare dintre sistemele externe se propune să fie integrat printr-un microserviciu dedicat. Fiecare sistem extern va avea propriul său microserviciu dedicat pentru a gestiona integrarea și maparea datelor într-un mod centralizat. Acest lucru va reduce complexitatea și va facilita gestionarea separată a fiecărui flux de date.

Fiecare microserviciu poate fi dezvoltat și actualizat independent, fără a afecta funcționalitatea celorlalte. Acest lucru permite dezvoltarea de noi servicii fără a perturba întregul sistem. Un alt aspect

pentru utilizarea microserviciilor este că resursele pot fi alocate în mod eficient fiecărui sistem extern în funcție de nevoile sale.

Microserviciile se planifică să comunice între ele prin intermediul API-urilor și protocolului HTTP.

O altă funcționalitate importantă este implementarea unui micro serviciu care va permite importul de date în sistemul integrat utilizând fișierele. Un astfel de funcționalitate va extinde considerabil potențialul sistemului și va rezolva problema cu datele care nu fac parte din sistemele externe deja implementate dar sunt păstrate în anumite formate digitale. Ca format de import de date pot servi următoarele tipuri de fișiere CSV (Comma-Separated Values), JSON (JavaScript Object Notation), XML (eXtensible Markup Language), Excel (XLSX). Aceste date sunt apoi standardizate și integrate în sistem pentru a fi analizate și raportate. Datele primite trec prin procese de transformare, mapare și validare pentru a asigura coerența și calitatea datelor. Ca și în opțiunea anterioară, se va implementa un sistem de securitate robust pentru a proteja accesul la date și pentru a asigura confidențialitatea și integritatea informațiilor.

Avantaje:

Scalabilitate și Redundanță;

Flexibilitate;

Un micro serviciu eronat nu va distruge neapărat întregul sistem. Ar afecta doar o anumită zonă.

Integrare/ Implementare continuă;

Flexibilitate tehnologică.

Beneficii:

Flexibilitatea sistemului permite adaptarea rapidă la schimbările din sursele externe sau în cerințele de raportare;

Centralizarea datelor;

Toate datele sunt colectate și stocate într-un singur loc, facilitând analiza și raportarea.

Bază de date centralizată;

Datele transformate sunt stocate într-o bază de date centralizată, care asigură accesul rapid și eficient la informații. Aceasta va permite analize complexe și raportare personalizată.

Scalabilitate;

Arhitectura permite adăugarea de resurse pentru a face față creșterii volumului de date.

Dezavantaje:

Complexitate inițială;

Proiectarea și implementarea unui astfel de sistem pot fi inițial complexe și necesită resurse considerabile.

Costuri inițiale ridicate;

Investiții semnificative pot fi necesare pentru dezvoltarea și implementarea inițială a sistemului și pentru formarea echipei.

Timpul îndelungat de implementare.

Digitalizarea administrației publice reprezintă un pas esențial în modernizarea serviciilor oferite cetățenilor și în îmbunătățirea eficienței operaționale a instituțiilor publice. În acest context, soluția tehnică

propusă pentru digitalizarea comunei Gorgota trebuie să fie concepută pentru a răspunde unui set complex de cerințe, care să asigure nu doar funcționalități avansate, ci și conformitatea cu standardele europene, securitatea datelor și sustenabilitatea pe termen lung. Scopul principal al soluției este de a transforma modul în care administrația locală interacționează cu cetățenii, oferind servicii publice digitale accesibile, sigure și eficiente.

Soluția tehnică trebuie să fie scalabilă și modulară, permițând o implementare flexibilă pe faze și adaptarea la nevoile specifice ale comunei Gorgota. Aceasta trebuie să permită extinderea ulterioară a funcționalităților, fără a necesita investiții masive suplimentare. Modularitatea sistemului este esențială pentru a asigura integrarea ușoară cu alte sisteme existente sau viitoare, precum și pentru a permite o gestionare eficientă a resurselor și a proceselor administrative.

Conformitatea cu standardele europene reprezintă un pilon esențial în proiectarea și implementarea oricărei soluții tehnice destinate administrației publice, mai ales într-un context de digitalizare finanțată prin fonduri europene. Această conformitate nu este doar o obligație legală, ci și o garanție a eficienței, securității și sustenabilității pe termen lung a sistemelor implementate. Pentru comuna Gorgota, respectarea acestor standarde asigură integrarea armonioasă în ecosistemul digital european, facilitând accesul la resurse financiare, colaborarea interinstituțională și creșterea încrederii cetățenilor în serviciile publice digitale.

➤ Securitatea Datelor și Regulamentul General privind Protecția Datelor (GDPR)

GDPR-ul (Regulamentul UE 2016/679) stabilește cadrul juridic pentru protejarea datelor cu caracter personal în întreg spațiul European. Pentru soluția tehnică propusă, acest regulament impune implementarea unor măsuri tehnice și organizatorice riguroase:

- Criptarea și Anonimizarea: Toate datele sensibile (e.g., informații personale ale cetățenilor, documente oficiale) trebuie criptate atât în stocare, cât și în transmisie. Anonimizarea datelor este obligatorie în cazurile în care prelucrarea nu necesită identificarea persoanelor.
- Gestionarea Accesului: Sistemul trebuie să utilizeze un model de control al accesului bazat pe roluri (Role-Based Access Control – RBAC), limitând accesul la date doar pentru personalul autorizat. Logurile de activitate trebuie să înregistreze toate interacțiunile cu datele, permițând auditul și detectarea incidentelor.
- Drepturile Subiectului de Date: Soluția trebuie să permită exercitarea drepturilor GDPR, cum ar fi dreptul la ștergere, portabilitatea datelor sau rectificarea informațiilor, prin interfețe de înregistrare a solicitărilor în portalul e-Cetățean.
- Evaluarea Impactului și Consimțământul: Orice procesare de date trebuie precedată de o evaluare a impactului asupra protecției datelor (Data Protection Impact Assessment – DPIA), iar consimțământul cetățenilor trebuie obținut explicit și documentat.

Nerespectarea GDPR-ului poate duce la amenzi severe (până la 4% din cifra de afaceri globală, pentru întreprinderi, sau 20 de milioane de euro, pentru instituțiile publice) și la pierderea încrederii publice. Prin urmare, soluția trebuie să integreze instrumente de monitorizare continuă a conformității, precum module de detectare a breșelor de securitate și notificare automată a autorităților în caz de încălcare.

➤ Accesibilitatea Digitală și Directiva UE 2016/2102

Directiva UE 2016/2102 impune instituțiilor publice să asigure accesibilitatea integrală a website-urilor și aplicațiilor mobile pentru persoanele cu dizabilități. Pentru comuna Gorgota, aceasta înseamnă că portalul e-Cetățean, chatbot-ul AI și orice altă interfață digitală trebuie să respecte standardele WCAG 2.1 (Web Content Accessibility Guidelines) la nivel AA. Acestea includ:

- Navigare Adaptivă: Interfețele trebuie să fie compatibile cu dispozitive asistive (e.g., cititoare de ecran, dispozitive Braille) și să permită navigarea doar prin tastatură.
- Design Incluziv: Elementele grafice trebuie să aibă contrasturi suficiente (raport de minimum 4.5:1), iar textele să fie redimensionabile fără a afecta layout-ul. Videoclipurile trebuie să includă subtitrare și descrieri audio.
- Structură Semantică: Utilizarea corectă a HTML5 (e.g., etichete <header>, <nav>, <article>) și a atributelor ARIA (Accessible Rich Internet Applications) pentru a facilita înțelegerea conținutului de către dispozitivele asistive.
- Testare Continuă: Accesibilitatea trebuie verificată periodic prin tool-uri automate (e.g., WAVE, Axe) și teste manuale efectuate de utilizatori cu dizabilități.

Accesibilitatea nu este doar o cerință legală, ci și o oportunitate de a include toți cetățenii în procesul de digitalizare. Prin urmare, soluția trebuie să fie proiectată cu un mindset incluziv din faza de concepție (prin abordarea „Design for All”), evitând costurile ulterioare ale remedierii problemelor de accesibilitate.

➤ Interoperabilitate și Cadrul ISA² (Interoperability Solutions for European Public Administrations)

Cadrul ISA² promovează interoperabilitatea sistemelor informatice ale administrațiilor publice europene, asigurând schimbul eficient de date și colaborarea transfrontalieră. Pentru comuna Gorgota, acest aspect se materializează prin:

- Utilizarea Standardelor Deschise: Soluția trebuie să adopte formate de date deschise (e.g., XML, JSON) și protocoale standardizate (e.g., REST API, OAuth 2.0), evitând dependența de tehnologii proprietare.
- Alinierea la Cadrul European de Interoperabilitate (EIF): Acesta impune structurarea sistemelor în patru niveluri de interoperabilitate:
 - Legal: Respectarea reglementărilor privind schimbul de date între entități (e.g., Regulamentul eIDAS pentru identitatea digitală).
 - Organizațional: Definirea proceselor comune de colaborare între instituții.
 - Semantic: Utilizarea de vocabulare controlate și ontologii (e.g., taxonomii EU pentru categorii de documente).
 - Tehnic: Integrarea cu platforme europene precum CEF (Connecting Europe Facility) sau PEPPOL (Pan-European Public Procurement Online).
- Compatibilitate cu Sistemele Naționale: Soluția trebuie să se alinieze și cu standardele naționale (e.g., formatul METS pentru arhivarea electronică în România) și să permită integrarea cu sisteme precum Ghidul de Interoperabilitate al Guvernului Român.

De exemplu, portalul e-Cetățean ar putea folosi API-urile europene pentru a valida automat identitățile digitale (prin eIDAS) sau pentru a trimite notificări transfrontaliere. În plus, arhivarea digitală a documentelor istorice trebuie să respecte standardul OAIS (Open Archival Information System), asigurând conservarea pe termen lung și accesul universal.

➤ Alinierea Componentelor Hardware și Software

Conformitatea nu se limitează la software. Ea implică și selectarea de hardware certificat și aprovizionat în conformitate cu reglementările UE:

- Hardware: Echipamentele (e.g., servere Dell, UPS NetYS) trebuie să respecte directivele UE privind eficiența energetică (ErP Directive) și gestionarea deșeurilor electronice (WEEE Directive). De asemenea, trebuie să fie compatibile cu standardele de securitate fizică (e.g., rack-uri cu încuietori fizice cu cheie).
- Software: Licențele software (e.g., DMS) trebuie să permită auditul codului sursă și actualizări periodice pentru a răspunde la noile vulnerabilități. Componentele open-source trebuie verificate pentru conformitate cu licențele EU (e.g., EUPL – European Union Public Licence).

Actualizările periodice și monitorizarea continuă a conformității sunt esențiale. De exemplu, un sistem de management al vulnerabilităților (Vulnerability Management System) poate detecta componentele învechite și recomanda patch-uri conforme cu reglementările UE.

O provocare majoră este menținerea conformității într-un mediu tehnologic dinamic, unde standardele evoluează constant. Pentru a atenua acest risc, soluția trebuie să includă:

- Proceduri de Audit Regulate: Evaluări semestriale efectuate de experți externi pentru a verifica alinierea la GDPR, WCAG și ISA².
- Colaborare cu Furnizori Certificați: Parteneriate cu companii care dețin certificate europene (e.g., ISO/IEC 27001 pentru securitate, EN 301 549 pentru accesibilitate).
- Training Specializat: Programe de formare pentru personalul tehnic și administrativ privind noile reglementări și instrumentele de conformitate.

Interoperabilitatea este un alt pilon fundamental al soluției tehnice. Sistemul trebuie să permită integrarea cu alte platforme și sisteme utilizate de administrația publică, cum ar fi sistemele de registru, arhiva electronică sau sistemele de gestionare a documentelor. Suportul pentru standarde deschise (Open Standards) și formate de date compatibile este esențial pentru a facilita schimbul de informații între diferite sisteme și pentru a asigura o colaborare eficientă între instituții.

Securitatea și protecția datelor sunt aspecte de maximă importanță în proiectarea soluției tehnice. Sistemul trebuie să includă măsuri robuste de securitate, cum ar fi criptarea datelor sensibile, gestionarea accesului pe bază de roluri și auditul activităților, precum și autentificare în doi factori, îndeosebi utilizatorilor cu rol de administrator sau ce au acces la informații confidențiale / ce intră sub regulamentul GDPR. De asemenea, trebuie să fie implementate măsuri de protecție împotriva atacurilor cibernetice, conform celor mai recente standarde de securitate IT, pentru a asigura integritatea și confidențialitatea datelor, atât în interiorul Sistemului, cât și în comunicarea bidirecțională dintre Soluția IT și Internet.

Performanța și disponibilitatea sistemului constituie fundamentele esențiale pentru o funcționare optimă și fără întreruperi a infrastructurii digitale utilizate în cadrul administrației publice sau al oricărui alt domeniu care depinde de tehnologii informatice avansate. Asigurarea unor timpi de răspuns scăzuți și a unei disponibilități ridicate reprezintă cerințe critice pentru a garanta accesul continuu la servicii digitale, astfel încât utilizatorii să poată beneficia de procese eficiente, rapide și sigure.

Un sistem informatic performant trebuie să fie capabil să gestioneze simultan multiple cereri fără a compromite viteza de procesare sau stabilitatea platformei. Acest lucru implică utilizarea unor infrastructuri hardware și software optimizate, capabile să susțină un volum mare de operațiuni într-un interval scurt de timp. Arhitectura sistemului trebuie proiectată astfel încât să asigure un echilibru între resursele disponibile și cerințele operaționale, evitând astfel blocajele sau supraîncărcările care ar putea afecta fluxul de lucru. Prin utilizarea unor tehnologii de ultimă generație, precum servere de înaltă performanță, soluții de stocare scalabile și rețele rapide, sistemul poate funcționa în parametri optimi și poate răspunde cerințelor impuse de utilizatori fără întârzieri semnificative.

Disponibilitatea ridicată a sistemului, definită printr-un prag minim de 99,9% pe an, este un aspect esențial care asigură accesul constant la date și servicii. Aceasta presupune implementarea unor măsuri de protecție care să prevină perioadele de nefuncționare neplanificate și să permită intervenții rapide în cazul unor defecțiuni. În acest sens, redundanța infrastructurii joacă un rol crucial. Prin replicarea componentelor esențiale și distribuirea sarcinilor între mai multe resurse, sistemul devine capabil să continue activitatea chiar și în situația în care apar erori la nivelul unor echipamente sau aplicații specifice. Astfel, utilizatorii finali nu sunt afectați de eventuale disfuncționalități, iar continuitatea serviciilor este menținută la un nivel optim.

Un aspect fundamental în asigurarea disponibilității și fiabilității sistemului îl constituie implementarea unor mecanisme avansate de backup și recuperare a datelor. Acestea trebuie să fie integrate în arhitectura soluției, astfel încât orice pierdere accidentală de informații sau corupere a fișierelor să poată fi remediată în cel mai scurt timp posibil. Realizarea de copii de siguranță la intervale regulate, pe suporturi de stocare sigure și distribuite în locații diferite, reprezintă o strategie eficientă pentru protecția datelor critice. Totodată, trebuie adoptate soluții de restaurare rapidă, care să permită recuperarea integrală a informațiilor și reluarea activității fără pierderi semnificative de date sau timp.

În situațiile neprevăzute, precum atacurile cibernetice, defecțiunile hardware sau erorile umane, sistemul trebuie să dispună de proceduri clare de intervenție și restaurare. Acestea includ atât măsuri proactive de prevenție, cât și strategii reactive pentru remedierea rapidă a incidentelor. Monitorizarea constantă a performanței și analizarea în timp real a stării sistemului contribuie la identificarea timpurie a posibilelor probleme și la luarea măsurilor necesare pentru a preveni impactul negativ asupra utilizatorilor. În plus, testarea periodică a procedurilor de recuperare a datelor și simularea unor scenarii de urgență asigură faptul că soluțiile implementate sunt eficiente și pot fi aplicate cu succes în condiții reale.

Un alt element esențial care contribuie la menținerea performanței și disponibilității sistemului este optimizarea fluxurilor de lucru și a resurselor. Distribuirea echilibrată a sarcinilor de procesare între servere și utilizarea unor algoritmi avansați de gestionare a resurselor ajută la evitarea supraîncărcării și la

menținerea unui nivel optim de performanță. În același timp, adoptarea unor tehnologii de scalabilitate permite ajustarea capacității sistemului în funcție de nevoile curente, fără a compromite funcționalitatea acestuia.

Atingerea obiectivelor privind performanța și disponibilitatea sistemului necesită o abordare multidimensională care include utilizarea tehnologiilor avansate, implementarea unor mecanisme robuste de protecție și recuperare a datelor, monitorizarea constantă și optimizarea resurselor. Prin asigurarea unor timpi de răspuns reduși și a unei disponibilități ridicate, soluția implementată va garanta funcționarea continuă a serviciilor digitale și va contribui la crearea unui mediu digital sigur, eficient și fiabil pentru utilizatori.

Suportul tehnic și mentenanța reprezintă elemente fundamentale în asigurarea funcționării optime și continue a unei soluții tehnice moderne, mai ales într-un context administrativ în care eficiența și disponibilitatea sistemelor informatice sunt esențiale pentru desfășurarea activităților zilnice. Implementarea unui plan de suport tehnic pe termen lung, cu o perioadă minimă de cinci ani și posibilitatea de prelungire, garantează sustenabilitatea investiției și menținerea performanței la standardele necesare. Acest aspect este crucial pentru evitarea disfuncționalităților și asigurarea unei tranziții fluide între actualizările tehnologice, astfel încât utilizatorii să beneficieze constant de un mediu digital stabil și sigur.

Un serviciu de suport tehnic eficient trebuie să fie structurat astfel încât să răspundă rapid și adecvat la orice problemă apărută, indiferent de complexitatea acesteia. În cazul incidentelor critice, unde funcționalitatea sistemului este grav afectată și există riscul de întrerupere a activităților administrative, timpul de răspuns nu trebuie să depășească patru ore. Această cerință este esențială pentru minimizarea impactului negativ asupra proceselor interne și pentru restabilirea rapidă a operațiunilor. De aceea, un sistem de ticketing bine organizat, combinat cu monitorizare proactivă și intervenție rapidă, poate asigura o gestionare eficientă a solicitărilor și prevenirea unor probleme recurente.

Pe lângă suportul reactiv, este necesară și o strategie de mentenanță preventivă, care să includă actualizări periodice ale software-ului, optimizări de performanță și testări regulate ale infrastructurii IT. Această abordare reduce riscul apariției unor defecțiuni neprevăzute și permite identificarea timpurie a potențialelor vulnerabilități. De asemenea, mentenanța corectivă trebuie să fie bine definită, astfel încât să poată remedia rapid orice problemă apărută, cu intervenții precise și eficiente. Planurile de mentenanță trebuie să includă atât măsuri pentru actualizarea și optimizarea soluției, cât și mecanisme pentru gestionarea incidentelor critice în mod transparent și eficient.

Pentru ca suportul tehnic să fie cât mai eficace, este esențial ca acesta să fie oferit de specialiști bine pregătiți, cu expertiză în gestionarea infrastructurilor IT complexe și capacitatea de a diagnostica rapid problemele. Comunicarea eficientă între echipa de suport și utilizatorii sistemului contribuie la reducerea timpului de remediere și la creșterea satisfacției acestora. O documentație tehnică detaliată și accesibilă, împreună cu sesiuni periodice de instruire pentru personalul administrativ, pot îmbunătăți considerabil procesul de utilizare și întreținere a soluției.

Un alt aspect esențial al suportului tehnic este monitorizarea continuă a sistemului, care permite detectarea și soluționarea problemelor înainte ca acestea să afecteze funcționalitatea generală.

Implementarea unor soluții avansate de monitorizare poate asigura o supraveghere permanentă a infrastructurii și o intervenție proactivă în cazul detectării unor anomalii. Prin aceasta, se poate preveni apariția unor probleme grave și se poate reduce semnificativ necesitatea intervențiilor corective majore.

În contextul unei soluții tehnice implementate în administrația publică, suportul tehnic trebuie să fie adaptat nevoilor specifice ale instituției și să ofere atât asistență de bază, cât și intervenții specializate pentru gestionarea aspectelor mai complexe. Serviciul trebuie să fie disponibil prin multiple canale de comunicare, inclusiv telefon, e-mail și platforme dedicate de ticketing, asigurând astfel o accesibilitate ridicată pentru utilizatori. Flexibilitatea acestui suport este esențială, permițând adaptarea la cerințele în schimbare și asigurând că soluția tehnică rămâne eficientă pe termen lung.

Suportul tehnic și mentenanța joacă un rol esențial în succesul unei soluții digitale, asigurând disponibilitatea constantă a sistemului, optimizarea continuă a performanței și gestionarea eficientă a incidentelor. O strategie bine definită în acest sens nu doar că reduce riscurile operaționale, dar contribuie și la creșterea încrederii utilizatorilor în soluția implementată. Prin stabilirea unor proceduri clare de intervenție, a unui timp de răspuns optim și a unor mecanisme eficiente de prevenire a defectărilor, suportul tehnic devine un pilon de bază în garantarea unei infrastructuri digitale sigure și funcționale.

În cadrul unei administrații publice modernizate prin digitalizare, documentația și formarea utilizatorilor reprezintă piloni esențiali ai succesului implementării unei soluții tehnice. Oricât de avansată ar fi infrastructura implementată, valoarea sa este determinată în mare măsură de capacitatea personalului de a o utiliza eficient și de a o întreține în conformitate cu cele mai bune practici. Prin urmare, furnizarea unei documentații tehnice detaliate, alături de sesiuni de formare specializate, este indispensabilă pentru optimizarea fluxurilor de lucru și pentru creșterea eficienței operaționale în administrația locală. De asemenea, suportul este disponibil pentru fiecare modul în parte, de tip Knowledgebase, ușor accesibil pentru utilizator.

Documentația tehnică a soluției trebuie să fie completă, clară și bine organizată, astfel încât să permită utilizatorilor să înțeleagă toate aspectele funcționale și tehnice ale sistemului. Aceasta trebuie să includă manuale de utilizare detaliate, care să explice într-un limbaj accesibil modul de operare al platformei, ghiduri de implementare care să descrie configurațiile inițiale și procedurile necesare pentru integrarea cu alte sisteme existente, precum și proceduri de operare pentru gestionarea eficientă a aplicațiilor în activitatea curentă. Un astfel de set de documente este esențial nu doar pentru utilizarea optimă a soluției, ci și pentru asigurarea unei tranziții line în cazul schimbărilor de personal sau a extinderii funcționalităților sistemului în viitor.

O administrație publică digitalizată trebuie să asigure că fiecare utilizator este familiarizat cu soluțiile informatice implementate. De aceea, sesiuni de formare bine structurate sunt necesare pentru a instrui atât personalul administrativ, cât și pe cel tehnic, astfel încât aceștia să poată utiliza sistemul în mod eficient și să fie capabili să gestioneze eventualele probleme minore fără a necesita intervenția constantă a echipelor de suport. În acest sens, formarea trebuie să fie personalizată în funcție de rolurile și responsabilitățile fiecărui grup de utilizatori, acoperind atât aspectele generale ale utilizării sistemului, cât și funcționalități specifice pentru fiecare departament în parte.

Procesul de instruire trebuie să fie unul continuu, nu doar un eveniment singular desfășurat în momentul implementării soluției. În acest sens, sunt necesare sesiuni periodice de actualizare, mai ales în contextul în care soluțiile digitale sunt în permanentă evoluție și necesită adaptare constantă la noi cerințe și provocări. Organizarea unor sesiuni de formare la intervale regulate va contribui la menținerea unui nivel ridicat de competență tehnică în rândul angajaților, reducând astfel dependența de suportul extern și optimizând modul în care soluția este utilizată zilnic.

Pentru a maximiza beneficiile digitalizării, instruirea trebuie să fie susținută de materiale didactice interactive, cum ar fi tutoriale video, studii de caz și sesiuni de practică aplicată. Aceste metode permit angajaților să înțeleagă mai bine procesele și să își însușească rapid noile cunoștințe, facilitând astfel o adoptare eficientă a sistemului. În plus, feedback-ul utilizatorilor trebuie să fie luat în considerare pentru a adapta programul de instruire în funcție de dificultățile întâmpinate în practică, asigurând astfel o învățare continuă și eficientă.

Un alt aspect important al documentației și formării este asigurarea unui sistem de suport accesibil, care să permită utilizatorilor să obțină rapid informațiile necesare în cazul în care întâmpină dificultăți. În acest sens, trebuie dezvoltate platforme de asistență care să includă baze de cunoștințe actualizate și posibilitatea de a contacta specialiști pentru clarificări suplimentare. O astfel de abordare sprijină utilizatorii în procesul de adaptare și crește nivelul de autonomie în utilizarea sistemului, reducând în același timp necesitatea unor intervenții frecvente din partea echipei tehnice.

Sustenabilitatea și optimizarea costurilor de operare sunt factori esențiali în proiectarea și implementarea unei soluții tehnice destinate administrației publice. O soluție digitală performantă nu trebuie să se limiteze doar la îndeplinirea cerințelor actuale, ci trebuie să fie concepută astfel încât să permită funcționarea eficientă și economică pe termen lung. Acest obiectiv poate fi atins prin utilizarea unor tehnologii moderne, capabile să reducă semnificativ consumul de resurse și să limiteze necesitatea intervențiilor costisitoare de mentenanță și actualizare.

Reducerea costurilor de operare și mentenanță reprezintă un aspect crucial pentru sustenabilitatea unei soluții informatice, mai ales în contextul administrației publice, unde eficiența bugetară este o prioritate constantă. Alegerea unor infrastructuri scalabile și eficiente energetic, alături de utilizarea unor tehnologii optimizate pentru reducerea consumului de resurse, permite minimizarea cheltuielilor recurente asociate utilizării și întreținerii sistemului. Implementarea unor mecanisme avansate de monitorizare a resurselor informatice, cum ar fi gestionarea inteligentă a consumului de energie și utilizarea optimă a capacităților de stocare, asigură un control mai eficient asupra costurilor operaționale și o mai bună alocare a resurselor disponibile.

În vederea optimizării costurilor, soluțiile tehnice moderne trebuie să fie proiectate astfel încât să reducă dependența de infrastructura fizică extinsă și să permită utilizarea unor servicii bazate pe cloud computing, acolo unde este posibil. Migrarea către soluții de tip cloud sau hibrid poate oferi beneficii semnificative în ceea ce privește reducerea costurilor asociate echipamentelor hardware, extinderea facilă a capacităților sistemului și eliminarea necesității unor investiții constante în infrastructură fizică. Totodată, prin adoptarea unor tehnologii care permit automatizarea proceselor administrative și reducerea sarcinilor

repetitive, administrațiile locale pot optimiza fluxurile de lucru și pot reduce semnificativ costurile de operare.

Un alt aspect fundamental al sustenabilității unei soluții tehnice este flexibilitatea sa în raport cu cerințele legislative și administrative aflate în continuă schimbare. Sistemele informatice utilizate în administrația publică trebuie să fie capabile să se adapteze rapid la modificările impuse de reglementările legale, fără a necesita investiții semnificative pentru actualizare. Acest lucru poate fi realizat prin adoptarea unei arhitecturi modulare, care să permită integrarea rapidă a noilor funcționalități și ajustarea proceselor existente fără perturbări majore asupra activității instituționale. Totodată, utilizarea unor standarde deschise și a unor protocoale interoperabile asigură compatibilitatea cu alte sisteme utilizate la nivel guvernamental, facilitând schimbul de date și reducând costurile asociate integrării acestora.

Soluția tehnică trebuie, de asemenea, să fie proiectată pentru a minimiza impactul asupra mediului și pentru a susține un model de dezvoltare sustenabil. Reducerea consumului de energie și utilizarea unor tehnologii prietenoase cu mediul pot contribui nu doar la reducerea costurilor, ci și la alinierea administrației publice la obiectivele de protecție a mediului și de eficiență energetică. De exemplu, implementarea unor sisteme de răcire optimizate pentru centrele de date, utilizarea hardware-ului cu un consum redus de energie și adoptarea unor politici de gestionare eficientă a resurselor pot genera economii semnificative pe termen lung și pot contribui la reducerea amprente de carbon a instituției.

În contextul digitalizării administrației publice, menținerea unui echilibru între costurile inițiale de implementare și economiile pe termen lung reprezintă o provocare esențială. Investițiile realizate în faza inițială trebuie să fie justificate printr-o reducere progresivă a costurilor de operare, printr-o eficientizare a activităților curente și printr-o creștere a accesibilității și fiabilității serviciilor oferite cetățenilor. În acest sens, este esențială efectuarea unor analize de impact și rentabilitate care să permită identificarea celor mai eficiente soluții din punct de vedere economic și operațional.

2.2. Prevederi de Securitate

Noul **Sistem Informatic Integrat și Interoperabil** va trebui să asigure o interconectare perfectă între toate aplicațiile existente în cadrul Primăriei, fără a necesita modificări semnificative ale acestora. API-ul dezvoltat va juca un rol de bază în realizarea acestei interoperabilități.

Centralizarea datelor;

Sistemul va trebui să centralizeze datele din diverse aplicații și să le coreleze pentru a oferi o imagine de ansamblu coerentă și comprehensivă asupra activităților și proceselor din cadrul Primăriei.

Securitate și confidențialitate;

Implementarea unui sistem robust de securitate va fi de importanță majoră pentru protejarea datelor sensibile și a informațiilor cetățenilor. Accesul la date trebuie să fie controlat, iar transmiterea informațiilor să fie securizată pentru a evita posibilele vulnerabilități.

Flexibilitate și scalabilitate;

Sistemul va trebui să fie flexibil pentru a permite adăugarea ulterioară de noi module sau aplicații fără a afecta funcționalitatea generală. De asemenea, acesta trebuie să fie scalabil pentru a face față creșterii

volumului de date și numărului de utilizatori.

Reziliență și backup;

Sistemul va trebui să includă strategii de backup și recuperare a datelor pentru a minimiza pierderile în caz de evenimente neprevăzute.

Usabilitate și formare;

Interfața sistemului trebuie să fie intuitivă și ușor de utilizat, asigurând astfel o adaptare rapidă de către personalul instituțional. De asemenea, se impune formarea personalului pentru utilizarea eficientă a sistemului.

Analiză și raportare avansată;

Sistemul va trebui să ofere instrumente puternice pentru analiza datelor și generarea de rapoarte detaliate. Capacitatea de a identifica tendințele, de a genera rapoarte cu un singur clic și de a reprezenta vizual informațiile vor fi necesare pentru luarea deciziilor informate.

Compatibilitate tehnologică;

Noul Sistem Informatic Integrat trebuie să fie compatibil cu tehnologiile existente și să permită integrarea cu viitoare inovații tehnologice.

Costuri și buget;

Evaluarea costurilor asociate implementării, dezvoltării API-ului și operării sistemului va fi vitală pentru asigurarea fezabilității opțiunii.

Aceste cerințe generale reprezintă o temelie solidă pentru proiectarea și dezvoltarea primei opțiuni și vor servi drept ghid pentru identificarea beneficiilor și riscurilor asociate acestei abordări în secțiunile ulterioare ale studiului de fezabilitate.

Prevederi de securitate:

Securitatea informațiilor este primordială pentru protejarea informațiilor sensibile și a resurselor informatice ale Primăriei. Prevederile de securitate sunt concepute pentru a crea un mediu sigur și controlat, în care datele și procesele sunt protejate împotriva accesului neautorizat, pierderii sau distrugerii. Ele stabilesc standarde clare privind gestionarea parolelor, accesul la rețele și sisteme, monitorizarea activității, criptarea datelor și multe altele.

După analiza Politicii și Regulamentului de Securitate IT din cadrul Primăriei comunei GORGOTA, aprobat prin dispoziția primarului, a fost constatat că acest regulament îndeplinește toate prevederile necesare pentru asigurarea securității și confidențialității informațiilor și resurselor informatice utilizate în cadrul instituției. Nu s-a simțit necesitatea de a replica prevederile de securitate din Politică și Regulamentul de Securitate în studiul de fezabilitate.

Este important de subliniat că această Politică și Regulament de Securitate trebuie aplicate și asupra Sistemului Informatic Integrat. Acest lucru implică respectarea tuturor prevederilor privind securitatea, managementul datelor și controlul accesului la informații, astfel încât să se asigure o funcționare corespunzătoare și să se minimizeze riscurile de securitate pentru toate componentele Sistemului Informatic Integrat.

Prin includerea acestor politici și reguli de securitate, se demonstrează angajamentul față de standardele de

securitate și confidențialitate și se asigură că SII propus în acest studiu de fezabilitate va fi gestionat în conformitate cu cele mai bune practici de securitate.

Recuperarea datelor în caz de incident:

Recuperarea datelor în caz de incident este un aspect critic al strategiei de securitate a informațiilor. Primăria comunei GORGOTA, utilizează cu succes tehnologia de backup bazată pe dispozitive de stocare pentru a asigura protecția și disponibilitatea datelor lor. În acest context, argumentăm că această tehnologie ar trebui extinsă și implementată pentru Sistemul Informatic Integrat propus în studiul de fezabilitate.

Datorită fiabilității, redundanței, funcționalității de backup automat și planificat, securității și eficienței în utilizare, tehnologia de backup bazată pe dispozitive de stocare a demonstrat eficacitatea sa în cadrul Primăriei comunei GORGOTA. Extinderea acestei tehnologii pentru Sistemul Informatic Integrat și Interoperabil va asigura că și acest sistem beneficiază de cele mai bune practici în materie de recuperare a datelor în caz de incident. Astfel, se va minimiza riscul de pierdere a informațiilor critice și se va spori securitatea și continuitatea operațiunilor primăriei.

Implementarea tehnologiei de backup pentru Sistemul Informatic Integrat și Interoperabil, ar reprezenta o măsură esențială în asigurarea protejării datelor și a funcționării fără întreruperi a acestui sistem vital.

Această decizie nu numai că protejează datele, dar demonstrează și angajamentul pentru securitatea informațiilor și pentru furnizarea de servicii eficiente și de încredere pentru cetățeni și comunitate.

Securitatea datelor cu caracter personal

Manipularea datelor cu caracter personal în cadrul Sistemului Informatic Integrat și Interoperabil se va realiza exclusiv în conformitate cu legislația în vigoare, inclusiv regulile referitoare la proiectarea sistemelor informatice care gestionează astfel de date. Aceste reguli includ:

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Ordinul Avocatului Poporului nr. 52/18.04.2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.

Aceste regulamente vor fi strict respectate pentru a asigura protecția adecvată a datelor cu caracter personal în cadrul sistemului informatic.

În contextul transformării digitale a administrației publice, asigurarea unui mediu digital sigur și fiabil reprezintă o condiție esențială pentru buna desfășurare a activităților instituționale. Prevederile de securitate sunt concepute pentru a proteja infrastructura informatică, datele și serviciile digitale împotriva amenințărilor cibernetice, accesului neautorizat și pierderilor accidentale de informații. Această documentație își propune să ofere un cadru comprehensiv de măsuri și proceduri, care, prin aplicarea lor consecventă, vor contribui la menținerea unui nivel înalt de securitate și la asigurarea continuității operaționale în cadrul administrației publice digitalizate.

Sistemele informatice utilizate în administrația publică sunt supuse unui număr semnificativ de riscuri, atât din partea atacurilor cibernetice, cât și a defecțiunilor tehnice sau a erorilor umane. Din acest motiv, este imperativ ca soluțiile implementate să fie dotate cu măsuri de protecție avansate, care să asigure confidențialitatea, integritatea și disponibilitatea informațiilor. Prin adoptarea unui set de prevederi de

securitate bine structurat, instituția își poate reduce vulnerabilitățile și poate preveni incidentele care ar putea afecta negativ activitatea și încrederea cetățenilor în serviciile publice.

Un aspect central al prevederilor de securitate îl constituie protecția rețelilor și a sistemelor informatice. Întrucât infrastructura IT reprezintă coloana vertebrală a oricărei administrații digitalizate, accesul neautorizat la aceasta poate avea consecințe grave. Pentru a preveni astfel de situații, se impune utilizarea unor tehnologii de filtrare și monitorizare a traficului de rețea, care să permită identificarea și blocarea imediată a oricăror tentative de intruziune. Aceste tehnologii sunt concepute pentru a detecta activități suspecte și pentru a interveni prompt, astfel încât sistemul să nu fie compromis. De asemenea, implementarea unor politici stricte de acces, bazate pe autentificare robustă, este esențială pentru a garanta că doar persoanele autorizate pot intra în sistem. Măsurile de segregare a rețelilor interne, împreună cu izolarea componentelor critice, contribuie la reducerea riscului de propagare a eventualelor breșe de securitate, asigurând astfel o barieră eficientă între diferitele segmente ale infrastructurii IT.

Protejarea datelor cu caracter personal și a informațiilor sensibile reprezintă o prioritate absolută în cadrul oricărei strategii de securitate. Conform cerințelor Regulamentului General privind Protecția Datelor (GDPR), toate datele gestionate de administrația publică trebuie să fie criptate atât în tranzit, cât și în repaus. Această abordare previne accesul neautorizat la informații și asigură integritatea datelor chiar și în cazul unui incident de securitate. În plus, politicile de anonimizare și pseudonimizare a datelor contribuie la minimizarea riscurilor asociate scurgerilor de informații, transformând datele sensibile în formate care nu pot fi asociate direct cu identitatea persoanelor vizate. Astfel, chiar dacă datele sunt compromise, impactul asupra drepturilor și libertăților cetățenilor este redus la minimum.

Pentru a asigura continuitatea operațională și pentru a minimiza efectele negative ale unor eventuale incidente, este imperativă implementarea unor mecanisme robuste de backup și recuperare a datelor. Mecanismele de backup trebuie să fie automate și să opereze la intervale regulate, astfel încât toate informațiile critice să fie salvate în timp real sau aproape de aceasta. Soluțiile de stocare a copiilor de siguranță trebuie să fie distribuite în locații fizice diferite, astfel încât, în cazul unui dezastru sau a unui atac cibernetic de amploare, datele să poată fi recuperate rapid și complet. În plus, procedurile de recuperare a datelor trebuie testate periodic pentru a se asigura că planurile de continuitate sunt eficiente și că timpul de restaurare a sistemelor este minim. Această abordare nu doar că protejează informațiile, dar și menține încrederea utilizatorilor în capacitatea instituției de a-și desfășura activitatea în condiții optime, chiar și în situații de criză.

Securizarea aplicațiilor și a serviciilor digitale constituie un alt element esențial în cadrul prevederilor de securitate. Întrucât majoritatea operațiunilor se bazează pe aplicații software, este vital ca acestea să fie proiectate și actualizate continuu pentru a face față noilor amenințări. Utilizarea unor metode de autentificare multifactorială, care combină mai multe elemente de securitate, asigură că accesul la aplicații este restricționat și monitorizat. În același timp, actualizările periodice ale software-ului și aplicarea patch-urilor de securitate sunt măsuri critice pentru prevenirea exploatarea vulnerabilităților. O administrare eficientă a actualizărilor implică, de asemenea, monitorizarea constantă a sistemului, astfel încât orice semn

de anomalie să fie detectat și remediat prompt. Aceste procese sunt esențiale pentru menținerea integrității și performanței aplicațiilor, contribuind astfel la asigurarea unui mediu digital stabil și securizat.

În paralel cu măsurile tehnice, factorul uman reprezintă un pilon de bază în strategia de securitate. Personalul administrativ și tehnic trebuie să fie conștient de riscurile cibernetice și să fie instruit în mod regulat cu privire la bunele practici în domeniul securității informatice. Sesiunile de instruire și simulările de atacuri cibernetice sunt esențiale pentru a pregăti angajații să recunoască și să reacționeze adecvat în cazul unui incident. În plus, crearea unei culturi organizaționale orientate spre securitate poate reduce semnificativ riscul erorilor umane, care adesea reprezintă puncte vulnerabile în sistemele informatice. Prin dezvoltarea unor politici interne clare și prin implementarea unor proceduri de raportare a incidentelor, instituția poate asigura că orice potențială amenințare este gestionată în mod corespunzător și că lecțiile învățate sunt integrate în strategia de securitate viitoare.

O altă componentă crucială a prevederilor de securitate este reprezentată de evaluările periodice și de auditările interne. Aceste procese de verificare sunt menite să identifice punctele slabe ale sistemului și să recomande măsuri corective înainte ca acestea să devină probleme majore. Evaluările de securitate, realizate de echipe interne sau de auditori externi, oferă o imagine clară asupra stării sistemului și permit ajustarea continuă a politicilor de securitate. Prin aplicarea unor standarde recunoscute la nivel internațional, instituția poate demonstra conformitatea cu normele de securitate și poate obține certificări care atestă calitatea măsurilor implementate. Această abordare nu doar că îmbunătățește protecția sistemelor informatice, dar contribuie și la consolidarea încrederii cetățenilor și a altor părți interesate în capacitatea administrației de a gestiona în siguranță datele și informațiile critice.

Pe lângă măsurile tehnice și de organizare, este esențial ca soluția de securitate să fie flexibilă și adaptabilă, astfel încât să răspundă eficient la evoluția constantă a amenințărilor cibernetice. Mediul digital se schimbă rapid, iar atacatorii își actualizează metodele de infiltrare într-un ritm alert. În acest context, strategia de securitate trebuie să fie dinamică și să includă mecanisme de actualizare continuă, care să permită integrarea celor mai noi tehnologii și proceduri de protecție. Aceasta presupune, de asemenea, colaborarea strânsă cu furnizorii de soluții IT și cu experții în securitate, pentru a putea beneficia de inovațiile din domeniu și pentru a se adapta la schimbările legislative și tehnologice. Flexibilitatea sistemului de securitate este un factor cheie în menținerea unei protecții robuste pe termen lung, permițând administrației publice să își ajusteze rapid strategiile în funcție de noile riscuri identificate.

Integrarea tehnologiilor emergente joacă un rol important în întărirea prevederilor de securitate. De exemplu, utilizarea inteligenței artificiale în monitorizarea activității rețelelor poate permite identificarea timpurie a anomaliilor și a comportamentelor suspecte, înainte ca acestea să evolueze în incidente majore. Algoritmii avansați pot analiza volume mari de date în timp real, detectând patternuri care indică posibile atacuri și alertând echipa de securitate pentru a interveni prompt. Astfel de tehnologii nu numai că sporesc capacitatea de răspuns la incidente, dar contribuie și la prevenirea apariției acestora, oferind un nivel suplimentar de protecție.

Un alt aspect esențial în strategia de securitate este gestionarea incidentelor și a situațiilor de urgență. Chiar cu toate măsurile preventive aplicate, este posibil să apară situații neprevăzute care necesită

o intervenție rapidă și eficientă. Pentru a răspunde acestor situații, este necesar ca instituția să dispună de un plan de răspuns la incidente bine definit, care să stabilească responsabilitățile și pașii de urmat în cazul unui atac cibernetic sau al unei defecțiuni majore. Acest plan trebuie să fie integrat în cultura organizațională, astfel încât fiecare membru al echipei să știe exact ce acțiuni să întreprindă în momentul în care apare o problemă. Un management eficient al incidentelor presupune, de asemenea, comunicarea transparentă atât internă, cât și externă, pentru a minimiza impactul asupra activității și pentru a asigura o rezolvare rapidă a situațiilor critice.

În mediul administrativ, unde datele personale și informațiile sensibile sunt gestionate zilnic, implementarea unor măsuri stricte de securitate nu este doar o cerință tehnică, ci și una de responsabilitate socială. Instituția trebuie să demonstreze angajamentul său față de protecția drepturilor cetățenilor, asigurându-se că datele acestora sunt tratate cu cel mai mare grad de confidențialitate și că accesul la informațiile sensibile este controlat riguros. Această abordare nu doar că protejează datele, dar consolidează și imaginea administrației ca entitate modernă, transparentă și responsabilă. În plus, prin respectarea normelor internaționale de protecție a datelor și a standardelor de securitate, instituția se aliniază la practicile de referință din domeniul IT, ceea ce poate facilita, pe termen lung, integrarea cu alte sisteme guvernamentale și colaborarea la nivel național și european.

În final, implementarea prevederilor de securitate reprezintă o investiție strategică în viitorul administrației publice digitalizate. Prin adoptarea unui set cuprinzător de măsuri, care acoperă aspecte de protecție a rețelelor, a datelor, a aplicațiilor și a factorului uman, instituția se poate asigura că mediul digital în care operează este robust, sigur și adaptabil la noile provocări. Astfel, se creează un cadru de securitate care nu doar previne incidentele, ci și permite o reacție rapidă și coordonată în cazul în care acestea apar. Această abordare holistică este esențială pentru menținerea unui nivel ridicat de încredere din partea utilizatorilor și pentru asigurarea continuității operaționale, contribuind astfel la realizarea obiectivelor de digitalizare și modernizare ale administrației publice.

Prevederile de securitate, în concluzie, propuse în acest proiect, constituie un pilon esențial în cadrul oricărei strategii de digitalizare. Prin adoptarea unor tehnologii avansate, politici stricte de control și măsuri de protecție integrate, administrația publică poate asigura un mediu digital sigur și eficient, capabil să susțină activitățile instituționale și să protejeze datele cetățenilor. Această abordare nu doar că optimizează funcționarea sistemelor informatice, ci contribuie și la dezvoltarea unui ecosistem digital fiabil, în care inovația și tehnologia sunt utilizate pentru a îmbunătăți serviciile publice și pentru a promova transparența, responsabilitatea și protecția informațiilor. Într-o eră în care securitatea cibernetică devine tot mai crucială, investiția în prevederi de securitate adecvate reprezintă o condiție sine qua non pentru succesul oricărui proiect de digitalizare. Prin urmare, instituțiile publice, precum Primăria Comunei Gorgota, trebuie să considere implementarea acestor măsuri ca pe un element strategic, care va asigura nu doar protecția datelor, ci și stabilitatea și fiabilitatea întregii infrastructuri digitale pe termen lung.

3. DESCRIEREA TEHNICA A PROIECTULUI

Implementarea unei soluții de digitalizare în administrația publică presupune adoptarea unei infrastructuri moderne și eficiente, capabile să asigure gestionarea optimă a activităților instituționale și îmbunătățirea interacțiunii cu cetățenii. Proiectul vizează dezvoltarea unui sistem informatic integrat, cu un grad ridicat de securitate, performanță și disponibilitate, care să permită administrarea electronică a documentelor, automatizarea proceselor interne și furnizarea de servicii publice digitale accesibile.

Arhitectura sistemului este concepută pe o infrastructură distribuită, bazată pe tehnologii cloud și servere locale, pentru a asigura atât flexibilitate în gestionarea resurselor, cât și securitatea datelor. Aceasta va permite scalabilitatea soluției, permițând integrarea ulterioară a unor noi module sau aplicații, fără a afecta performanța generală a sistemului. Serverele utilizate vor fi echipate cu soluții avansate de redundanță și backup automatizat, astfel încât să fie prevenită pierderea datelor în cazul unor defecțiuni tehnice. În plus, utilizarea unor rețele de mare viteză și a unor soluții avansate de echilibrare a traficului va permite optimizarea fluxurilor de date și reducerea timpilor de răspuns.

Un aspect fundamental al proiectului este **gestionarea documentelor și automatizarea proceselor administrative**. Soluția tehnică include un sistem de management al documentelor (DMS), care permite arhivarea digitală, clasificarea și accesarea rapidă a informațiilor. Acest sistem va integra fluxuri de lucru automatizate, reducând semnificativ timpul necesar procesării documentelor și facilitând colaborarea între departamente. Totodată, platforma va dispune de un modul de registratură electronică, care va permite depunerea și procesarea cererilor online, eliminând necesitatea interacțiunilor fizice cu administrația.

Pentru **creșterea eficienței și îmbunătățirea relației cu cetățenii**, proiectul va include implementarea unui portal online dedicat serviciilor publice digitale. Acesta va oferi funcționalități precum depunerea electronică a documentelor, programări online, solicitări de informații și consultări publice. Portalul va fi optimizat pentru accesibilitate și va fi compatibil cu dispozitive mobile, asigurând astfel o experiență digitală intuitivă pentru utilizatori. De asemenea, se va implementa un chatbot bazat pe inteligență artificială, capabil să răspundă automat întrebărilor cetățenilor și să îi ghideze în utilizarea serviciilor disponibile.

Un alt element esențial al proiectului este **securitatea cibernetică**, având în vedere importanța protejării datelor și prevenirea accesului neautorizat la informații sensibile. Sistemul informatic va include soluții avansate de protecție a rețelelor, precum firewall-uri de ultimă generație, sisteme de detecție și prevenire a intruziunilor (IDS/IPS) și criptare end-to-end a comunicațiilor. Autentificarea utilizatorilor se va face prin metode multifactoriale, prevenind astfel accesul neautorizat la sistem. În plus, se vor aplica măsuri stricte de gestionare a drepturilor de acces, asigurând astfel că fiecare utilizator are acces doar la informațiile relevante pentru activitatea sa.

Pentru **asigurarea continuității operaționale**, proiectul prevede implementarea unor mecanisme avansate de backup și recuperare a datelor. Copiile de siguranță vor fi realizate periodic și vor fi stocate atât local, cât și în centre de date externe securizate. În cazul unor defecțiuni majore sau atacuri cibernetice, sistemul va permite restaurarea rapidă a datelor, minimizând astfel impactul asupra activității administrației publice.

În vederea **sustenabilității pe termen lung**, soluția va fi proiectată astfel încât să reducă la minimum costurile de operare și mentenanță. Optimizarea consumului de resurse, utilizarea unor tehnologii eficiente energetic și adoptarea unor politici de administrare inteligentă a infrastructurii IT vor contribui la menținerea unor cheltuieli reduse pe durata de utilizare a sistemului. În plus, flexibilitatea arhitecturii software va permite adaptarea soluției la modificările legislative sau la noile cerințe ale administrației, fără a necesita intervenții costisitoare.

Un aspect fundamental al implementării proiectului îl constituie **formarea personalului administrativ și tehnic**, pentru a asigura utilizarea optimă a noii soluții digitale. În acest sens, se vor organiza sesiuni de instruire, care vor include atât prezentarea funcționalităților sistemului, cât și exerciții practice de utilizare. Documentația tehnică va fi detaliată și va include manuale de utilizare, ghiduri de implementare și proceduri de operare, astfel încât utilizatorii să poată gestiona eficient platforma fără a depinde constant de suport tehnic extern.

3.1. Cerințele funcționale ale sistemului

Cerințele funcționale ale sistemului reprezintă un set de specificații tehnice și operaționale care definesc modul în care soluția de digitalizare trebuie să funcționeze pentru a satisface nevoile comunei Gorgota. Aceste cerințe sunt esențiale pentru asigurarea eficienței, accesibilității și interoperabilității sistemului, precum și pentru îndeplinirea obiectivelor proiectului finanțat prin fonduri europene. În cele ce urmează, vom analiza în detaliu fiecare componentă funcțională, evidențiind avantajele și cerințele specifice, într-un mod formal și adecvat unui proiect tehnic TIC.

Opțiunea tehnică este implementarea unui Sistem Informatic Integrat Mixt bazat pe microservicii (Opțiunea 1), pe o arhitectură hardware în cadrul Primăriei comunei GORGOTA, care să permită integrarea datelor din diferite sisteme existente în cadrul Primăriei comunei GORGOTA.

Totodată, se vor utiliza serviciile de Cloud în scopul realizării activității de predicții pentru Sistemul Informatic Integrat și Interoperabil.

Această alegere va fi justificată prin prezentarea următoarelor argumente:

- Argumentul 1 - Flexibilitate tehnică prin microservicii;

Unul dintre principalele avantaje ale Opțiunii 1, bazate pe microservicii, este flexibilitatea tehnologică pe care o oferă. Prin dezvoltarea de microservicii pentru fiecare sistem extern, se permite dezvoltarea și actualizarea independentă a acestora. Acest lucru înseamnă că, în cazul în care un sistem extern trebuie să fie actualizat sau adaptat la schimbări, acest lucru poate fi realizat fără a afecta restul componentelor. Acest nivel de flexibilitate este esențial într-un mediu în continuă schimbare.

- Argumentul 2 - Extinderea capacității de import de date;

Opțiunea 1 include, de asemenea, implementarea unui microserviciu pentru importul de date din fișiere (CSV, JSON, XML, Excel). Aceasta extinde semnificativ capacitatea sistemului de a procesa date din surse variate. Prin această funcționalitate, sistemul devine mai versatil și poate gestiona date provenite din surse invariabile sau neașteptate, care nu sunt integrate prin microserviciile dedicate.

- Argumentul 3 - Separarea responsabilităților și redundanță cu microservicii;

Arhitectura bazată pe microservicii, din Opțiunea 1, oferă o clară separare a responsabilităților. Fiecare sistem extern este integrat printr-un microserviciu dedicat pentru integrare și mapare. Această separare nu doar că simplifică gestionarea și întreținerea sistemului, ci oferă și un nivel mărit de redundanță. Dacă un microserviciu întâmpină probleme sau necesită actualizări, celelalte microservicii pot continua să funcționeze fără a afecta întregul sistem.

- Argumentul 4 - Integrare eficientă și coerentă a datelor cu microservicii;

Microserviciile din Opțiunea 1 contribuie la centralizarea datelor. Datele din sistemele externe, fie ele integrate prin microservicii dedicate sau importate din fișiere, sunt colectate și stocate într-o bază de date centralizată. Aceasta asigură accesul rapid și eficient la informații pentru analize complexe și raportare personalizată. Prin procesele de transformare, mapare și validare a datelor, se garantează coerența și calitatea datelor, ceea ce este esențial pentru luarea deciziilor informate.

Prin urmare, pentru instituțiile care caută o soluție robustă și agilă pentru gestionarea și raportarea datelor, Opțiunea 1 reprezintă o alegere prudentă.

3.2. Arhitectura funcțională a sistemului

Arhitectura funcțională a sistemului descrie modul în care componentele software și hardware sunt organizate și interacționează pentru a asigura funcționalitățile necesare în implementarea unei soluții de digitalizare a administrației publice. Această arhitectură este proiectată pentru a oferi o infrastructură scalabilă, sigură și eficientă, capabilă să susțină gestionarea documentelor, automatizarea proceselor administrative, oferirea de servicii publice digitale și asigurarea securității datelor. În cele ce urmează, vom detalia principalele componente funcționale ale sistemului, precum și modul în care acestea vor fi hostate sau amplasate în cadrul Primăriei, într-un mod formal și adecvat unui proiect tehnic TIC.

3.2.1. Amplasarea și Hostarea Soluțiilor în Primărie

Implementarea unui mediu hibrid care combină infrastructura locală a Primăriei cu servicii cloud reprezintă o soluție modernă pentru gestionarea eficientă a resurselor IT. Această abordare este motivată de necesitatea echilibrării flexibilității, scalabilității, securității și costurilor operaționale. Un mediu hibrid permite instituțiilor publice să adopte cele mai bune practici din domeniul tehnologiei informației, menținând controlul asupra datelor critice. În plus, mediul hibrid oferă posibilitatea integrării unor tehnologii emergente, precum inteligența artificială, analiza big data și Internet of Things (IoT), ceea ce contribuie la îmbunătățirea serviciilor publice și la eficientizarea proceselor administrative. De asemenea, această soluție sprijină tranziția către o administrație digitală modernă, permițând accesibilitate îmbunătățită pentru cetățeni și reducerea timpului necesar pentru procesarea documentelor și solicitărilor.

Sistemul hibrid propus este alcătuit din două componente principale:

1. **Infrastructura locală (on-premises)** - Centrele de date și serverele deținute și administrate de Primărie, care asigură control deplin asupra datelor și a aplicațiilor critice.
2. **Serviciile cloud** - Resurse virtualizate oferite de furnizori cloud (publici, privați sau hibrizi), utilizate pentru scalabilitate, stocare, backup, procesare de date și aplicații accesibile online.

Arhitectura include un sistem de interconectare securizat, permițind transferul de date în mod eficient și sigur între infrastructura locală și cloud.

Dintre avantajele mediului hibrid, amintim:

- **Flexibilitate**

Un mediu hibrid permite Primăriei să utilizeze resursele IT într-un mod dinamic, mutând sarcinile de lucru în cloud sau în infrastructura locală, în funcție de necesitate. De exemplu, procesele cu cerințe ridicate de calcul pot fi transferate în cloud pentru a evita supraîncărcarea serverelor interne. În plus, acest model oferă flexibilitate în integrarea de noi aplicații și servicii digitale, fără a necesita modificări majore ale infrastructurii existente.

- **Scalabilitate**

Resursele cloud oferă posibilitatea extinderii rapide a capacității de procesare și stocare, fără a necesita investiții majore într-o infrastructură locală suplimentară. Aceasta este esențială pentru gestionarea creșterii volumului de date și a nevoilor de procesare în perioadele de solicitare maximă (de exemplu, depunerea declarațiilor fiscale). Scalabilitatea mediului hibrid permite și adaptarea rapidă la noi cerințe legislative sau schimbări în volumul de lucru al administrației publice.

- **Securitatea și control al datelor**

Prin păstrarea datelor sensibile în infrastructura locală, Primăria poate respecta reglementările privind protecția datelor și confidențialitatea informațiilor. Serviciile cloud sunt utilizate pentru date mai puțin critice sau pentru soluții care necesară accesibilitate extinsă, cum ar fi portalurile online pentru cetățeni. Mecanismele de autentificare multi-factor, criptarea datelor și monitorizarea continuă a activităților IT contribuie la consolidarea securității generale a infrastructurii.

- **Continuitatea operațională și recuperare în caz de dezastru**

Prin utilizarea unui mediu hibrid, Primăria poate implementa strategii eficiente de recuperare în caz de dezastru (Disaster Recovery), replicând datele critice în cloud pentru a preveni pierderile cauzate de avarii hardware sau atacuri cibernetice. Totodată, sistemele de backup automate și soluțiile de failover asigură continuitatea operațională, reducând riscurile asociate incidentelor IT.

- **Optimizarea costurilor**

Costurile sunt optimizate prin utilizarea eficientă a resurselor disponibile. Infrastructura locală este utilizată pentru sarcini constante, în timp ce cloud-ul este folosit pentru cerințe variabile, reducând astfel investițiile în echipamente fizice. În plus, modelul de plată „pay-as-you-go” permite ajustarea cheltuielilor în funcție de necesități, evitând supradimensionarea infrastructurii locale.

**APLICATIE DE
MANAGEMENT A
DOCUMENTELOR -1
buc.**

1. Cerinte generale:

- Sistemul trebuie să fie un sistem cu o arhitectură scalabilă pentru a permite adăugarea de noi utilizatori și noi documente cu păstrarea performanțelor de utilizare;
- Sistemul trebuie să funcționeze atât pe sisteme de tip Linux (RedHat, CentOS și alte distribuții) cât și sisteme de tip Windows Server;
- Sistemul trebuie să permită achiziția On-premises și Software as a Services;
- Sistemul trebuie să asigure integrare cu LDAP / Active Directory /OID;
- Sistemul trebuie să permită funcționarea mixtă atât cu utilizatori de aplicație (user și parolă), cât și cu utilizatori de Active Directory sau altele;
- Sistemul trebuie să permită conectarea prin SSO;
- Să expună servicii full REST pentru integrare cu alte sisteme interne;
- Sistemul trebuie să asigure administrare facilă bazată pe Organigrama, Utilizatori, Grupuri, Roluri;
- Sistemul trebuie să permită restricționarea accesului la anumite meniuri și funcționalități în funcție de drepturile și permisiunile fiecărui utilizator. Astfel, utilizatorii vor avea acces doar la acele secțiuni și funcționalități ale sistemului care sunt relevante pentru rolul și responsabilitățile lor, asigurând o utilizare securizată și conformă cu politica organizației;
- Să permită setarea de politici de expirare și reguli de complexitate ale parolelor;
- Sistemul trebuie să aibă un meniu dedicat de Password Policies, de unde să permită reguli de parole precum: lungime minimă, lungime maximă, număr minim de caractere, număr minim de majuscule, număr minim de cifre, număr minim de caractere speciale, regulă de permitere a numelui de utilizator în parolă, timp de resetare a parolei, număr maxim de modificări pe zi, durată minimă între modificările parolei;
- Comunicații securizate utilizând SSL / HTTPS;
- Sistemul oferit nu trebuie să necesite instalare pe stațiile locale, el trebuie să funcționeze pe toate browserele moderne: Chrome, Firefox, Mozilla etc;
- Sistemul nu trebuie să aibă limitări de extensie a documentelor păstrate în arhiva electronică;
- Sistemul trebuie să fie disponibil în mai multe limbi de circulație internațională (Română și Engleză) și ușor de tradus în orice altă limbă solicitată;
- Din rațiuni de securitate, utilizatorii trebuie să fie deconectați automat din sistem după o perioadă în care acesta nu mai este utilizat;
- Sistemul trebuie să păstreze logul detaliat la fiecare modificare efectuată asupra fiecărei tabelă din baza de date și pentru fiecare coloană;
- Protecție automată la fraude, încercări de descărcare / spam. Blocarea accesului la sistem de la anumite IP-uri considerate riscante;
- Soluția trebuie să permită proceduri de backup și recuperare în caz de dezastru;
- Platforma va dispune de un sistem de metadate care se vor asocia fișierelor, sistem care se va putea customiza din cadrul interfeței web;
- Ofertantul trebuie să furnizeze o propunere de hardware și software pentru instalarea aplicației în premisele beneficiarului;
- Sistemul trebuie să fie responsive, adaptându-se automat la diferite dimensiuni de ecran și dispozitive (desktop, tabletă, mobil), pentru a asigura o experiență de utilizare optimă indiferent de platformă.

2. Cerințe funcționale:

2.1. Configurarea și Gestionarea Nomenclatoarelor și Librăriilor de Documente:

- Sistemul propus trebuie să permită configurarea nomenclatorului arhivistic, inclusiv stabilirea termenului de păstrare și a departamentului responsabil pentru fiecare tip de document din cadrul acestuia;
- Sistemul trebuie să permită configurarea nomenclatoarelor pentru destinatari interni, precum și externi;
- Sistemul trebuie să permită definirea facilă a unui număr nelimitat de librării/folders de documente organizate ierarhic, pe o structură familiară utilizatorilor - tip Windows Explorer;

- Fiecare librărie de documente (folder) să aibă drepturi ușor gestionabile, similar cu Windows Explorer: grup, citire, scriere.
- Fiecare librărie să poată afișa tabelar, pe lângă informațiile standard, și diferite alte metadata specifice pentru a ajuta la identificarea și căutarea rapidă a unui document în librărie;
- Sistemul trebuie să permită salvarea de vizualizări personalizate ale unei librării și a filtrelor alocate în aceasta, cu posibilitatea de a le adăuga într-o zonă de favorite;
- Sistemul trebuie să permită definirea și alocarea de tag-uri/etichete multiple la nivel de document, cu posibilitatea de regăsire a acestora într-o librărie dedicată tag-urilor/etichete utilizate;
- Aplicația trebuie să dispună de un meniu dedicat pentru suport, prin care utilizatorii pot trimite tichete direct către producător pentru asistență și suport.
- Aplicația trebuie să permită utilizatorului să își personalizeze profilul și să includă cel puțin următoarele opțiuni: Temă de vizualizare (Light/Dark); Limba (minim Română, Engleză); Fus orar; Formatul de dată (DD-MM-YYYY; YYYY-MM-DD); Formatul numerelor (cu/fără zecimale; separator de mii: „,“, „,“, „,“ sau „,“).
- Aplicația trebuie să pună la dispoziție un manual de utilizare, care poate fi accesat direct din platformă.
- Drepturile de securitate și permisiunile trebuie să fie special proiectate astfel încât să permită controlul accesului utilizatorilor la documente și tipul drepturilor de acces;
- Trebuie să permită alocarea unui proprietar de document, care poate fi schimbat din cadrul interfeței web;

2.2. Încărcarea și Manipularea Documentelor:

- Sistemul trebuie să permită încărcarea de documente cu drag&drop sau selecție din Windows Explorer;
- Sistemul trebuie să permită încărcarea de documente prin import (via API/citire căsuță de e-mail/hot-folder/sFTP);
- Sistemul trebuie să permită vizualizarea direct din interfață a fișierelor de tip .pdf, .doc/.docx, .html, .jpeg, .png, .xml, .xls/.xlsx;
- Sistemul trebuie să afișeze un thumbnail cu prima pagină a documentelor de tip .pdf, .doc/.docx, .jpeg, .png;
- Sistemul trebuie să permită schimbarea modului de vizualizare la nivel de librărie între listă și thumbnail/grid;
- Sistemul trebuie să permită vizualizarea accesibilității fiecărui fișier într-un tabel dedicat în cadrul librăriei;
- Sistemul trebuie să permită alocarea mai multor tipuri de documente unui singur obiect (de exemplu, pentru un fișier PDF care conține un contract și o anexă, sistemul să permită alocarea a două tipuri de documente distincte și metadatale specifice acestora);
- Sistemul trebuie să permită scanarea documentelor direct din browser, având posibilitatea de conectare cu stația de scanare și posibilitatea de salvare în librărie a documentului scanat. La nevoie, să permită alocarea unui număr de registratură direct la momentul salvării în librărie;
- Soluția oferită trebuie să aibă posibilitatea de configurare a unui „vizualizare personalizata de coloane/custom view” la nivel de librărie, cu posibilitatea de configurare de tip public (utilizabil de toți utilizatorii) sau privat (vizibil doar pentru utilizatorul care l-a creat);
- Soluția trebuie să permită crearea de șabloane în format WORD direct din aplicație;
- Soluția trebuie să permită generarea de șabloane în formatele Word, Excel și RTF;
- Soluția trebuie să permită clasificarea șabloanelor prin crearea de categorii;
- Soluția trebuie să permită activarea și dezactivarea șabloanelor din aplicație;
- Soluția trebuie să permită încărcarea șabloanelor de pe stația locală în formatele Word, Excel și RTF, și adaptarea lor direct în aplicație;
- Soluția trebuie să permită utilizarea șabloanelor active doar de către utilizatorii cu drepturi specifice;
- Soluția trebuie să permită generarea unui document pe baza unui șablon activ, cu asocierea automată a atributelor completate în zonele dedicate din șablon;

- Soluția trebuie să permită stabilirea formatului de generare a documentelor, cu formatele minime acceptate: Word, Excel, PDF și RTF;
- Soluția trebuie să permită editarea directă a documentelor generate din șabloane în formatele editabile, cum ar fi Word și Excel, direct din aplicație;

2.3. Gestionarea și Securitatea Documentelor:

- Sistemul informatic oferit trebuie să aibă capacitatea de luare în evidență a documentelor din domeniul de interes, îi atribuie un identificator unic, să permită alocarea metadatelor;
- Drepturile de securitate și permisiunile trebuie să fie special proiectate astfel încât să permită controlul accesului utilizatorilor la documente și tipul drepturilor de acces;
- Soluția trebuie să ofere mecanisme de securitate bazate pe grupuri, roluri, utilizatori și funcții din organigramă;
- Nu trebuie să existe limitări privind numărul de grupuri ce pot fi definite la nivelul depozitului de documente;
- Soluția trebuie să permită sincronizarea automată între grupurile funcționale din arhiva electronică și grupurile de utilizatori definite în sistemul de Active Directory;
- Soluția trebuie să poată oferi acces către mai multe arhive individuale pentru același utilizator și să ofere posibilitatea desemnării relației pe care o are fiecare utilizator în raport cu celelalte arhive gestionate, inclusiv rolul general pe care acel utilizator îl are pentru fiecare astfel de arhivă (administrator sau utilizator normal);
- Soluția trebuie să ofere posibilitatea organizării utilizatorilor în grupuri. Un utilizator poate face parte din unul sau mai multe grupuri, iar permisiunile de securitate trebuie să fie asociate cu grupurile de utilizatori (aplicându-se tuturor utilizatorilor membri ai acelui grup la momentul controlului accesului);
- Soluția trebuie să permită stabilirea nivelului de autorizare pe care utilizatorul îl are alocat în cadrul arhivei, cel puțin: citire, scriere, complet, vizualizare doar fișa documentului fără posibilitate de vizualizare a conținutului, cu recursivitate sau nu;
- Să permită accesul la vizualizarea fișei documentelor, dar fără acces la conținutul efectiv al documentului;
- Utilizatorii trebuie să poată avea acces la documentele din arhivele electronice în conformitate cu rolul asociat acestora și cu drepturile de acces înregistrate de către administratorul arhivei;
- Sistemul trebuie să permită alocarea de anexe în mod bilateral, atât pentru anexe principale, cât și pentru anexe secundare;
- Soluția trebuie să ofere utilizatorilor posibilitatea de a accesa un tur ghidat al funcționalităților bibliotecii virtuale printr-un buton dedicat;
- Soluția trebuie să permită reluarea turului ghidat oricând, fără limitări, prin apăsarea butonului dedicat;
- Soluția trebuie să indice utilizatorilor funcționalitățile cheie, butoanele și ariile relevante din arhiva electronică în timpul turului ghidat;
- Soluția trebuie să ofere explicații detaliate pentru fiecare funcționalitate esențială sau buton indicat în cadrul turului ghidat;

2.4. Funcționalități de Căutare și Raportare:

- Aplicația va dispune de un motor performant de căutare a documentelor în arhivă după unul sau mai multe criterii simultan. Accesul la documente se va realiza securizat utilizând permisiuni prestabilite pentru diferite roluri atribuite utilizatorilor;
- Motorul de căutare avansată va avea minim următoarele opțiuni:
 - Posibilitatea de căutare în foldere sau în foldere specifice;
 - Posibilitatea de căutare în subfoldere;
 - Posibilitatea de căutare după metadata cu variabile multiple;
 - Posibilitatea de căutare cu operatori logici (<, >, <=, >=, Range, Like/Contains, =, etc.);
 - Posibilitatea de căutare doar pentru anumite extensii;

- Posibilitatea de căutare după tip document
- Posibilitatea de filtrare și salvare a filtrelor direct din rezultatul căutării, cu posibilitatea de adăugare la favorite a căutărilor;
- Posibilitatea de interacțiune cu rezultatele căutării (edit, view, anexare, etc)
- Posibilitatea de export a rezultatului căutării în Excel/CSV;
- Posibilitatea de căutare după cuvinte obligatorii sau cuvinte opționale, dar și cuvinte excluse;
- Posibilitatea de restricționare a căutărilor doar pentru anumite documente;
- Posibilitatea de căutare globală în sistem;
- Posibilitate de salvare a cautarilor la favorite.

2.5. Editare și Colaborare pe Documente:

- Sistemul trebuie să permită editarea atât simplă, cât și colaborativă, direct în interfața web a sistemului;
- Sistemul trebuie să permită lucrul colaborativ și posibilitatea de editare a următoarelor extensii de fișiere: .xlsx, .doc, .ppt, .txt, .xml;
- Sistemul trebuie să permită salvarea de versiuni noi ale fișierelor atunci când sunt efectuate modificări de către unul sau mai mulți utilizatori;
- Sistemul trebuie să permită lucrul colaborativ/editarea unui document .doc pentru un număr estimativ de 5-10 persoane simultan;
- Sistemul trebuie să permită salvarea automată după un interval de timp în cazul în care sunt efectuate modificări pe document de către unul sau mai mulți utilizatori și niciunul dintre ei nu a efectuat încă operațiunea de salvare;
- Sistemul trebuie să permită vizualizarea în timp real de către alți utilizatori care nu au drept de modificare a documentelor, dar au posibilitatea de vizualizare a conținutului;
- Sistemul trebuie să permită direct în interfața web funcționalitățile standard conform extensiilor, după cum urmează:
 - Pentru editarea fișierelor în format .doc, sistemul trebuie să permită minim următoarele: schimbarea fontului, posibilitatea de aliniere, posibilitatea de bold, posibilitatea de copy-paste, posibilitatea de paragraf, posibilitatea de undo-redo, posibilitatea de titlu, posibilitatea de track-changes, posibilitatea de inserare tabele, posibilitatea de comentarii, posibilitatea de paginare, posibilitatea de insert header-footer, etc.;
 - Pentru editarea fișierelor în format .xlsx, sistemul trebuie să permită minim următoarele: posibilitatea de adăugare de sheet-uri noi, posibilități de calcul (adunare, scădere, împărțire, înmulțire), posibilitatea de pivot, posibilitatea de borders, posibilitatea de schimbare a fontului, posibilitatea de schimbare a culorilor de fundal, posibilitatea de insert-remove rows, posibilitatea de sum, average, min, max, count, posibilitatea de chart, posibilitatea de undo-redo, etc.;
 - Pentru editarea fișierelor în format .ppt, sistemul trebuie să permită minim următoarele: posibilitatea de adăugare de text box, posibilitatea de adăugare-ștergere slide-uri, posibilitatea de layout-uri standard cu 2 sau mai multe blocuri de date pe un slide, posibilitatea de introducere de forme (shapes), posibilitate de introducere imagini, posibilitate de schimbare fonds , posibilitate de schimbare fill color si line color, posibilitate de undo-redo, etc;
 - Pentru editarea fișierelor în format .txt și .xml, sistemul trebuie să permită minim următoarele: posibilitatea de aliniere, posibilitatea de bold, posibilitatea de copy-paste, posibilitatea de undo-redo, etc;
- Sistemul trebuie să permită vizualizarea conținutului pentru fișierele .zip (conținutul poate fi compus din foldere și fișiere cu extensii precum .pdf, .xml, .doc, .txt, .ppt);
- Sistemul trebuie să afișeze conținutul fișierelor cu extensie .zip fără a fi necesar să dezarhivezi fișierul .zip și fără a fi necesar să părăsești inter.
- Să permită definirea de „liste filtrate” de documente, vizibile pentru utilizator ca niște foldere, prin specificarea parametrilor utilizați la filtrare;

	• Trebuie să permită îmbinarea documentelor în format .pdf din cadrul aceleiași librării; acest proces de îmbinare .pdf trebuie să ruleze în fundal fără a influența activitatea utilizatorilor, iar când documentul îmbinat este realizat, utilizatorul va fi notificat în aplicație; • Sistemul trebuie să permită utilizatorilor să divizeze un document PDF într-unul sau mai multe documente separate, selectând paginile dorite pentru fiecare document nou generat; • Sistemul să poată bloca descărcarea anumitor sau a tuturor fișierelor din platformă, consultarea acestora urmând a fi făcută doar în cadrul platformei; • Să permită versionarea documentelor existente în librăriile definite; • Descărcarea documentelor să se întâmple background fără a influența activitatea utilizatorilor; • Sistemul trebuie să permită partajarea documentelor prin generarea unui hyperlink unic, accesibil partenerilor externi; • Sistemul trebuie să permită protejarea hyperlink-ului cu o parolă generată conform politicilor interne de securitate. Parola trebuie să fie modificabilă de către utilizator dacă este necesar; • Sistemul trebuie să permită setarea unei date de expirare pentru hyperlink. După expirare, accesul la hyperlink trebuie să fie blocat automat; • Sistemul trebuie să permită acordarea accesului de editare asupra documentului partajat, cu opțiunea de salvare a modificărilor; • Sistemul trebuie să permită adăugarea unei versiuni noi a documentului direct de pe stația locală, actualizând link-ul partajat fără a-l regenera; • Sistemul trebuie să permită semnarea documentului prin metode simple, inclusiv: ○ Semnătură cu pen digital; ○ Inserarea unei imagini predefinite (semnătură scanată); ○ Adăugarea textului semnăturii; • Sistemul trebuie să permită trimiterea hyperlink-ului direct pe email-ul partenerilor externi, incluzând un mesaj personalizat; • Sistemul trebuie să afișeze opțiunile de partajare într-un panou dedicat în detaliile documentului, incluzând: ○ Generare hyperlink; ○ Protecție cu parolă; ○ Setare dată expirare; ○ Acces de editare; ○ Acces la semnarea documentelor (pen digital, imagine, text) ○ Acces de atasare anexe la documentele partajate; ○ Trimitere prin email. • Sistemul trebuie să permită vizualizarea detaliilor hyperlink-ului generat, incluzând data expirării, parola asociată și istoricul modificărilor; • Sistemul trebuie să afișeze pentru utilizatorii externi o interfață simplă, care să includă: ○ Vizualizarea documentului partajat. ○ Opțiunile disponibile (descărcare, editare, semnare, upload versiune nouă). ○ Mesajul și contactul trimis de către utilizatorul intern. • Sistemul trebuie să aibă un meniu dedicat pentru utilizatori, în care aceștia să poată vizualiza și modifica hyperlink-urile emise de ei. Modificările posibile includ: ○ Dezactivarea unui hyperlink („Unshare”). ○ Generarea unei parole noi pentru hyperlink. ○ Eliminarea documentelor asociate hyperlink-ului. • Sistemul trebuie să aibă un meniu dedicat pentru administratori, în care aceștia să poată vizualiza toate hyperlink-urile emise în sistem și
--	---

	să efectueze aceleași acțiuni disponibile utilizatorilor: ○ Dezactivarea unui hyperlink („Unshare”). ○ Generarea unei parole noi. ○ Eliminarea documentelor asociate hyperlink-ului. • Sistemul trebuie să permită transformarea fișierelor de tip Word în format PDF, facilitând astfel gestionarea și distribuirea documentelor într-un format standardizat și securizat; • Sistemul trebuie să permită semnătura electronică simplă/avansată direct în aplicație; • Sistemul trebuie să permită semnarea documentelor în format .pdf folosind pen digital, mouse, adăugare de text sau imagine; • Sistemul trebuie să permită semnătura electronică simplă/avansată direct în aplicație; • Pentru semnătura simplă/avansată, sistemul oferit trebuie să permită următoarele: ○ Selectarea ariei în care dorești să introduci semnătura; ○ Selectarea tipului de semnătură: pen digital/mouse, imagine de pe stația locală, text; ○ Posibilitatea de a semna în mai multe locuri pe document fără a fi nevoie să refaci semnătura realizată cu pen digital/mouse, imagine de pe stația locală, text; ○ Criterii de audit: numele utilizatorului care a realizat semnarea, data (zi-lună-an) și ora (ora-minut-secundă). • Sistemul trebuie să permită semnarea documentelor utilizând un token fizic, asigurând astfel securitatea și autenticitatea documentelor semnate; • Sistemul trebuie să ofere posibilitatea de integrare cu un furnizor de semnătură calificată, dacă este cazul, pentru a asigura conformitatea cu reglementările legale și standardele de securitate; • Sistemul trebuie să permită duplicarea sau clonarea unui fișier existent, inclusiv toate metadatele asociate, pentru a ușura gestionarea documentelor similare sau recurente; • Sistemul trebuie să permită setarea unor clasificări automate, prin care să poată sugera tipul de document corespunzător unui fișier, pe baza conținutului acestuia, îmbunătățind astfel eficiența și acuratețea procesului de organizare a documentelor; • Sistemul trebuie să permită extragerea textului din conținutul fișierelor în format .pdf, word, excel, ppt, jpeg, png și să permită cautarea după cuvinte din conținutul acestora; • Sistemul nu trebuie să permită ștergerea permanentă a datelor din aplicație în mod direct, chiar dacă utilizatorul are drepturi de ștergere. În schimb, fișierele șterse trebuie să fie păstrate într-o zonă dedicată, destinată fișierelor șterse. Din această zonă, fișierele pot fi restaurate împreună cu toate elementele asociate, cum ar fi tipul de document, metadate, versiuni anterioare, etc., asigurând astfel integritatea și recuperabilitatea informațiilor; • Sistemul trebuie să permită ștergerea fișierelor din zona dedicată fișierelor șterse doar printr-o procedură automată. Această procedură poate fi configurată să se declanșeze după o anumită perioadă de timp, fie manual, fie automat, asigurând astfel gestionarea controlată și conformă a fișierelor eliminate. • Sistemul trebuie să includă o opțiune pentru partajarea către extern cu posibilitatea de creare a unui utilizator dedicat. În acest caz: ○ Link-ul partajat trebuie să redirecționeze utilizatorul extern către un formular de creare cont. ○ Formularul trebuie să solicite completarea câmpurilor minime necesare: Nume, Prenume și Adresă de e-mail. • Sistemul trebuie să creeze automat un cont pentru utilizatorul extern, pe baza informațiilor furnizate, și să: ○ Trimită un e-mail automat cu parola temporară și un link pentru conectarea în aplicație. ○ Permită utilizatorului să modifice parola după prima autentificare. • Sistemul trebuie să afișeze pentru utilizatorii externi autentificați o secțiune dedicată, „Shared with Me”, care să conțină:
--	--

- Toate documentele partajate către acel utilizator extern.
- Istoricul documentelor partajate, inclusiv cele deja vizualizate.
- Orice documente noi partajate, afișate în ordine cronologică.
- Sistemul trebuie să permită utilizatorilor externi să acceseze documentele partajate oricând, prin autentificarea în aplicație, fără a fi necesară regenerația hyperlink-ului.
- Sistemul trebuie să mențină sincronizarea continuă între documentele partajate și secțiunea „Shared with Me”, astfel încât utilizatorii externi să vadă întotdeauna cele mai recente actualizări.

2.6. Cerințe privind funcționalități de Notificare pentru Documente

- Sistemul trebuie să permită configurarea notificărilor automate printr-un meniu dedicat , accesibil în secțiunea de setări ale sistemului doar de utilizatorii autorizați;
- Sistemul trebuie să permită utilizatorilor autorizați să creeze, editeze, activeze/inactiveze și să șteargă notificări dintr-o listă centralizată. Lista trebuie să includă minim următoarele informații: Data Creării, Numele Notificării, Creatorul și Status (Activ/Inactiv) ;
- Sistemul trebuie să permită deschidă o pagină dedicată configurării notificărilor;
- Sistemul trebuie să permită configurarea notificărilor, incluzând minim următoarele cerințe generale:
 - Definirea unui nume descriptiv
 - Selectarea unei perioade de aplicabilitate configurabile
 - Alegerea unei opțiuni de resetare automată (săptămânal, lunar, trimestrial, anual)
 - Asocierea notificărilor cu tipuri specifice de documente și metadate
 - Adăugarea de metavariabile disponibile, cu afișarea următoarelor informații: tipul metavariabilei, valoarea implicită, opțiunile posibile și formatul de afișare
- Sistemul trebuie să permită configurarea de reguli pentru notificări, incluzând minim următoarele:
 - Comparare valori (<, >, =, <=, >=)
 - Validarea completării metavariabilelor
 - Filtrarea opțiunilor pentru metavariabile de tip dropdown
 - Setarea pragurilor pentru valori cumulative ale documentelor
 - Configurarea notificărilor recurente pentru starea documentelor și termenele limită
 - Notificarea la expirarea termenelor de retenție
 - Mutarea automată a documentelor în arhivă după expirarea perioadei de retenție
- Sistemul trebuie să permită trimiterea notificărilor utilizatorilor prin:
 - Email și/sau notificări în aplicație
 - Folosind mesaje personalizabile în funcție de regulile definite, aceste mesaje sunt configurate de către utilizatorul autorizat, direct din interfață
 - Selecția utilizatorilor, grupurilor sau membrilor specifici care vor primi notificările
- Sistemul trebuie să declanșeze notificări pe baza următoarelor evenimente:
 - Importul documentelor cu metadate asociate din alte sisteme
 - Completarea sau editarea metadatelor
 - Încărcarea manuală a documentelor
 - Execuția cron-job-urilor (lucrări programate) configurate periodic

- Sistemul trebuie să păstreze un log detaliat al notificărilor trimise, incluzând minim următoarele:
 - ID-ul notificării
 - Data și ora trimerii
 - Numele utilizatorului sau grupului notificat
 - Numele notificării
 - Lista documentelor asociate notificării
 - Utilizatorii care au fostificați
- Sistemul trebuie să permită vizualizarea și exportarea log-urilor de notificări în excel sau csv.

3. Cerințe funcționale specifice Registraturii

3.1. Înregistrarea și Gestionarea Documentelor:

- Modulul de registratură trebuie să permită înregistrarea detaliată a informațiilor privind corespondența, incluzând intrările, ieșirile și documentele de uz intern;
- Sistemul trebuie să includă câmpuri obligatorii precum Număr de înregistrare, Data primirii/înregistrării, Ora primirii/înregistrării, asigurând astfel completitudinea informațiilor;
- Sistemul trebuie să permită definirea și personalizarea câmpurilor pentru fiecare tip de registru, inclusiv a metadatelor precum seria numerică și alte caracteristici esențiale pentru gestionarea documentelor;
- Sistemul trebuie să gestioneze alocarea numerelor unice de înregistrare pentru documente folosind un sistem de numerotare centralizat, care să permită resetarea acestora la începutul fiecărui an calendaristic;
- Sistemul trebuie să împiedice modificarea numerelor de înregistrare alocate documentelor și să permită crearea și gestionarea registrelor de numere secvențiale definite de administratorul soluției;
- Sistemul trebuie să permită minim următoarele specificații pentru tipul „Intrare”:
 - Tip de înregistrare: intern/extern/uz intern
 - Registrator responsabil: automat utilizatorul conectat / user-ul de domeniu sau alt utilizator/grup
 - Forma de prezentare (plic, colet, etc.)
 - Categorie documente
 - Conținut document (câmp editabil)
 - Emitentul
 - Destinatar (entitate): utilizator sau departament intern
 - Observații suplimentare (câmp editabil)
 - Soluția trebuie să permită definirea de câmpuri suplimentare specifice tipului de registratură.
- Sistemul trebuie să permită minim următoarele specificații pentru tipul „Ieșire”:
 - Posibilitatea de legare cu numărul de intrare
 - Numele persoanei care înregistrează: automat utilizatorul conectat / user-ul de domeniu
 - Forma de prezentare (document, colet, plic, etc.)
 - Emitentul
 - Destinatarul
 - Observații suplimentare
 - Soluția trebuie să permită definirea de câmpuri suplimentare specifice tipului de registratură.

- Modulul de registratură trebuie să permită înregistrarea detaliată a informațiilor privind corespondența, incluzând intrările, ieșirile și documentele de uz intern;

3.2. Personalizarea și Configurarea Registrelor și Monitorizarea:

- Sistemul trebuie să permită configurarea și personalizarea registrelor direct din interfața web, permițând utilizatorilor să adauge câmpuri și atribute specifice fiecărui registru;
- Utilizatorii trebuie să poată specifica atributele registrului, inclusiv tipul, numele, tipurile de documente asociate, și formatul numărului de registru (cu opțiunea de a adăuga sufixe sau prefixe, termen de resetare, etc);
- Sistemul trebuie să permită configurarea atributelor și metadatelor specifice fiecărui registru, asigurând astfel o gestionare eficientă și adaptată la nevoile organizației;
- Sistemul trebuie să permită definirea de registre personalizate, oferind posibilitatea de a adăuga și personaliza câmpuri și atribute specifice, în funcție de particularitățile fiecărui registru;
- La nivel de registru, sistemul trebuie să permită configurarea de atribute și metadata specifice, inclusiv seria numerică și alte caracteristici esențiale pentru gestionarea eficientă a documentelor în cadrul registrului;
- Sistemul trebuie să permită trimiterea de notificări privind transmiterea corespondenței, cu opțiunea de aprobare sau respingere, atât prin notificări în aplicație, cât și prin e-mail;
- Sistemul trebuie să permită utilizatorilor să seteze nivelul de confidențialitate al documentelor, asigurând astfel protecția datelor sensibile;
- Sistemul trebuie să permită configurarea de drepturi specifice pentru registrele clasificate ca „top secret”, restricționând accesul doar la utilizatorii autorizați;
- Sistemul trebuie să permită configurarea registrelor direct din interfața web, inclusiv definirea și personalizarea câmpurilor specifice fiecărui registru, pentru a facilita gestionarea documentelor;
- Sistemul trebuie să permită setarea de câmpuri obligatorii necesare pentru alocarea unui număr de registru, asigurând completitudinea și corectitudinea datelor înregistrate;
- Sistemul trebuie să permită adăugarea de câmpuri specifice și pentru înregistrările de tip „uz intern”. Aceste câmpuri personalizate vor putea fi configurate în funcție de nevoile interne ale organizației și vor fi disponibile doar pentru acest tip specific de înregistrări;
- Sistemul trebuie să ofere funcționalități de căutare avansate la nivel de registratură, permițând utilizatorilor să efectueze căutări după orice câmp sau coloană din registru;
- Sistemul trebuie să permită setarea unui timp de răspuns specific pentru fiecare înregistrare în registru, asigurând astfel gestionarea eficientă a termenelor limită;
- Sistemul trebuie să permită setarea unei priorități pentru fiecare înregistrare în registru, facilitând organizarea și procesarea documentelor în funcție de urgență;
- Sistemul trebuie să ofere funcționalități de raportare a înregistrărilor care se apropie de termenul de răspuns, permițând utilizatorilor să ia măsuri proactive pentru a respecta termenele stabilite;
- Sistemul trebuie să permită înregistrarea numerelor alocate de instituțiile emitente și să asigure atribuirea documentelor asociate documentului ce urmează a fi înregistrat, facilitând astfel o evidență clară și completă;
- Sistemul trebuie să gestioneze alocarea numerelor unice de înregistrare pentru documente, utilizând un sistem de numerotare centralizat (serie numerica) la nivelul întregii companii, pentru a asigura uniformitatea și integritatea înregistrărilor;
- Sistemul trebuie să permită resetarea numerelor de înregistrare la începutul fiecărui an calendaristic, menținând astfel organizarea și claritatea numerotării documentelor;

	• Sistemul trebuie să împiedice modificarea numerelor de înregistrare alocate documentelor de către orice utilizator, asigurând astfel integritatea și securitatea datelor; • Sistemul trebuie să permită crearea și gestionarea de registre de numere definite de către administratorul soluției; • Sistemul trebuie să permită crearea și gestionarea registrelor de numere, care vor fi definite și administrate de către administratorul soluției, oferind astfel flexibilitate în organizarea înregistrărilor; • Sistemul trebuie să permită crearea de tipuri de registre care să gestioneze serii de numere secvențiale, asigurând o structură coerentă și ușor de urmărit a numerotării documentelor; • Sistemul trebuie să permită utilizatorilor ca, la definirea unui registru, să poată specifica cel puțin următoarele atribute: ○ Tip registru ○ Nume registru ○ Tipuri de documente asociate registrului - selectate din nomenclatorul aferent ○ Formatul numărului de registru, care trebuie să permită adăugare de sufix/prefix • Sistemul trebuie să ofere posibilitatea urmăririi stării documentului, a responsabililor care acționează pe document și a tuturor acțiunilor efectuate asupra documentului de fiecare entitate în parte; • Sistemul trebuie să permită trimiterea unei notificări prin e-mail la finalizarea fluxului de registratură, atât către destinatarii interni, cât și către destinatarii externi. Această notificare va conține detalii relevante despre documentul sau înregistrarea finalizată, asigurând astfel o comunicare eficientă și promptă cu toți destinatarii implicați; • Sistemul trebuie să permită înregistrarea de documente de intrare, de ieșire sau informative, oricare dintre acestea putând fi transmise către unul sau mai mulți destinatari; • Trebuie să permită ca, atunci când se creează răspuns la un document printr-un alt document, să se genereze o relație între documentele respective. Relația dintre cele două documente trebuie să fie bidirecțională; • Să permită ca relațiile între documente să fie păstrate în tot ciclul de viață al documentelor respective; • Trebuie să gestioneze nomenclatoare pentru: ○ Tip de documente ○ Emitenți și destinatari externi ○ Emitenți și destinatari interni ○ Secretariate/puncte de registratură • Sistemul trebuie să permită utilizatorilor aplicației să creeze și să actualizeze direct nomenclatorul de destinatari externi, oferind astfel flexibilitate și accesibilitate în gestionarea acestor date; • Sistemul trebuie să permită actualizarea nomenclatorului de destinatari interni exclusiv de către utilizatorii cu rol de administrator al aplicației, asigurând astfel controlul și securitatea datelor interne; • Sistemul trebuie să permită adăugarea de conținut unui document atât prin scanare, cât și prin încărcare dintr-un fișier existent pe stația de lucru, facilitând astfel integrarea eficientă a documentelor înregistrate; • Sistemul trebuie să permită limitarea vizualizării înregistrărilor din registru la numerele alocate de către un utilizator, asigurând astfel confidențialitatea și gestionarea securizată a datelor; • Funcționalități de raportare: ○ Raport după Destinatar cu posibilitatea de setare a unui interval de timp ○ Raport după Emitent cu posibilitatea de setare a unui interval de timp ○ Raport privind toate numerele de înregistrare emise pentru un interval de timp
--	--

	○ Raport cu număr total de documente înregistrate în ultima lună, împărțite pe tipuri de documente • Sistemul trebuie să permită generarea de rapoarte registru, pentru fiecare registru în parte; • Raportul registru poate fi exportat sub forma unui document de tip Excel si PDF.
	4. Cerinte functionale specifice fluxurilor de management document 4.1. Funcționalități generale ale modului de flux de lucru • Modulul de flux de lucru trebuie să asigure circulația documentelor pe trasee ierarhice sau definite de autorul documentului, cu posibilitatea aprobării sau respingerii acestora, distribuirea și circulația informațiilor și a documentelor interne în cadrul organizației; • Aplicația trebuie să includă atât instrumentele necesare pentru dezvoltare, cât și mediul de rulare, permițând astfel proiectarea, execuția și monitorizarea fluxurilor de documente într-un mod integrat și eficient; 4.2. Funcționalități specifice fluxului de lucru 4.2.1. Gestionarea fluxurilor de lucru: • Modulul trebuie să permită administratorilor de procese să utilizeze grupuri și roluri pentru definirea fluxurilor de lucru, facilitând organizarea și atribuirea sarcinilor; • Administratorii de procese trebuie să poată implementa orice tip de acțiune înainte sau după orice etapă a fluxului de lucru, oferind flexibilitate în gestionarea proceselor; • Posibilitatea de a defini și valida metadate ca fiind obligatorii într-o anumită etapă a fluxului de lucru, asigurând completitudinea și corectitudinea datelor; • Modulul trebuie să permită programarea escaladării automate a pașilor din fluxul de lucru dacă nu există un răspuns într-un anumit număr de zile, asigurând respectarea termenelor limită; • Administratorii trebuie să poată exporta definiția fluxurilor de lucru în format de tip imagine (canvas workflow) pentru prezentare și avizare; • Sistemul trebuie să permită redirectionarea automată a sarcinilor în cazul în care un utilizator și-a delegat sarcinile, garantând gestionarea corespunzătoare a tuturor sarcinilor; • Administratorii trebuie să aibă opțiunea de a opri sau revoca un flux de lucru în curs, oferind control complet asupra proceselor active; • Sistemul trebuie să permită administrarea de delegații pentru utilizatorii aflați în concediu medical sau de odihnă, asigurând continuitatea sarcinilor; 4.2.2. Notificări și comunicare: • Sistemul trebuie să permită notificarea utilizatorilor prin mesaje implicite la inițializarea fluxului de lucru și la fiecare acțiune în cadrul unui pas. • Utilizatorii trebuie să fie informați prin e-mail despre o nouă sarcină primită într-un flux de lucru; • Sistemul trebuie să permită notificarea utilizatorilor prin e-mail despre sarcini de efectuat sau neefectuate, cu posibilitatea de a deschide sarcinile direct din e-mail (redirecționare către aplicație); • Utilizatorii trebuie să poată adăuga comentarii la finalizarea unei sarcini din fluxul de lucru; 4.2.3. Definirea și personalizarea fluxurilor de lucru: • Autorii de procese trebuie să poată proiecta fluxuri de lucru cu sarcini singulare sau sarcini paralele și să definească condițiile de terminare

	pentru activitățile paralele; • Sistemul trebuie să permită definirea de comenzi condiționale în cadrul fluxurilor de lucru (de exemplu, facturi care depășesc o anumită sumă să fie aprobate de o persoană specifică); • Posibilitatea de a defini variabile pentru fluxurile de lucru, precum și lansarea unui flux de lucru fără a necesita un obiect/document atașat; • Autorii de procese trebuie să poată alocă drepturi de executare și să definească tipurile de documente permise pentru fiecare flux de lucru; • Sistemul trebuie să permită programarea unui timp de expirare pentru un flux de lucru; 4.3. Gestionarea documentelor în fluxul de lucru 4.3.1. Editarea și manipularea documentelor: • Utilizatorii trebuie să poată edita documentele din cadrul fluxului de lucru și să mute automat fișierul într-un dosar preselectat după finalizarea unei etape a fluxului; • În cazul respingerii documentului, utilizatorii trebuie să poată selecta etapa la care se va întoarce documentul (etapa anterioară sau o altă etapă); • Utilizatorii trebuie să aibă posibilitatea de a selecta persoana dintr-un grup de lucru pentru a evita trimiterea documentului întregului grup; • Sistemul trebuie să permită asocierea de documente la nivel de flux, cu vizualizare prin link-uri către librăriile din arhivă; • Sistemul trebuie să permită stabilirea acțiunilor de aprobare și respingere sub denumiri personalizate; 4.3.2. Monitorizare și raportare: • Sistemul trebuie să permită generarea unui istoric al fluxurilor de lucru pentru utilizatori individuali și întreaga organizație; • Trebuie să fie posibilă monitorizarea fluxurilor de lucru active și generarea de alerte și notificări pentru acestea, în special pentru fluxurile care nu sunt executate în termenul stabilit; • Sistemul trebuie să permită definirea de termene limită de execuție atât la nivel de flux, cât și la nivel de pas; 4.3.3. Transformarea documentelor și semnături: • Platforma trebuie să permită ilustrarea grafică a fluxului de lucru, cu evidențierea pașilor curenți; • Platforma trebuie să permită stabilirea unei reguli de semnare a documentelor într-un anumit pas al fluxului; Platforma trebuie să permită transformarea documentelor dintr-o extensie în alta, minim din Word în PDF;
PORTAL CETATEAN-1 buc.	1. Portalul trebuie să fie un sistem scalabil, capabil să gestioneze un număr mare de utilizatori și cereri fără a afecta performanța. Arhitectura sa trebuie să permită adăugarea facilă de noi module și extinderea funcționalităților. 2. Sistemul trebuie să funcționeze exclusiv online, fără necesitatea instalării pe stațiile locale ale utilizatorilor, și să fie compatibil cu toate browserele moderne, inclusiv Chrome, Firefox, Edge și Safari. 3. Portalul trebuie să suporte mai multe limbi de circulație internațională, având disponibilă cel puțin limba română și engleză, cu posibilitatea de traducere în alte limbi. 4. Sistemul trebuie să permită integrarea cu funcționalități precum RoEID, plăți online, Smart Locker și alte opțiuni relevante. 5. Sistemul trebuie să permită conectarea în platformă prin intermediul unui user și a unei parole, cu autentificare securizată. 6. Sistemul trebuie să permită adăugarea facilă de noi cereri în cazul în care apar tipuri suplimentare de solicitări administrative sau servicii. 7. Sistemul trebuie să permită modificarea facilă a cererilor existente, oferind flexibilitate pentru actualizarea sau adaptarea acestora la noile cerințe. 8. Sistemul trebuie să permită adăugarea cererilor pentru alte persoane, în cazul în care utilizatorul deține documentele care atestă dreptul de a face

	acest lucru. În astfel de cazuri, sistemul trebuie să solicite completarea unor câmpuri obligatorii cu informațiile necesare și încărcarea documentelor justificative în platformă. 9. Sistemul trebuie să permită adăugarea cererilor specifice atât pentru persoane fizice, cât și pentru persoane juridice, asigurând o personalizare corespunzătoare pentru fiecare tip de utilizator. 10. Sistemul trebuie să permită crearea conturilor atât pentru persoane fizice, cât și pentru persoane juridice. Utilizatorii trebuie să poată alege tipul contului în funcție de statutul lor, cu formulare specifice fiecărei categorii. 11. Sistemul trebuie să permită gestionarea cererilor specifice persoanelor fizice. Utilizatorii care creează un cont de persoană fizică trebuie să poată completa și trimite formulare adaptate nevoilor lor. 1. Sistemul trebuie să permită gestionarea cererilor specifice persoanelor juridice. Utilizatorii cu conturi de persoană juridică trebuie să aibă acces la formulare personalizate pentru organizațiile lor. 2. Sistemul trebuie să aibă opțiunea de a gestiona cereri în așteptare. Cererile trimise trebuie să aibă un status clar, indicând etapa procesului în care se află. 3. Sistemul trebuie să permită vizualizarea cererilor finalizate, astfel încât utilizatorii să poată accesa istoricul acestora în orice moment. 4. Sistemul trebuie să permită vizualizarea statusului cererilor efectuate de către cetățean către primărie. Utilizatorii trebuie să primească actualizări în timp real despre progresul cererilor lor. 5. Sistemul trebuie să permită trimiterea cererilor completate de către cetățean pe un flux de lucru în back-office-ul aferent. Fiecare cerere trebuie să urmeze un traseu clar definit, implicând departamentele relevante. 6. Sistemul trebuie să asigure o conectare facilă pentru utilizatori, dar să ofere și un nivel ridicat de securitate, având în vedere caracterul sensibil al documentelor personale procesate. 7. Sistemul trebuie să includă mecanisme de backup automat, care să asigure păstrarea în siguranță a datelor și restaurarea acestora în caz de necesitate. 8. Sistemul trebuie să permită adăugarea de sesizări, oferind cetățenilor posibilitatea de a raporta probleme, reclamații sau alte aspecte de interes public. 9. Sistemul trebuie să permită multiple opțiuni pentru sesizări, acoperind toate categoriile existente, cum ar fi infrastructura, mediu sau servicii comunitare. 10. Sistemul trebuie să permită filtrarea sesizărilor, astfel încât utilizatorii și administratorii să poată identifica rapid categoria de interes sau sesizările prioritare. 11. Sistemul trebuie să permită personalizarea interfeței pentru utilizatori, oferind opțiuni precum tema limba preferată. 12. Sistemul trebuie să permită adăugarea programărilor, oferind cetățenilor posibilitatea de a planifica întâlniri sau accesul la servicii administrative. 13. Sistemul trebuie să permită adăugarea de multiple opțiuni pentru programări, adaptabile la tipurile de servicii disponibile și la cerințele administrației. 14. Sistemul trebuie să permită vizualizarea intervalelor orare disponibile și selectarea acestora de către utilizatori, pentru a facilita o programare eficientă. 15. Sistemul trebuie să permită blocarea automată a intervalelor orare și a zilelor deja ocupate, prevenind astfel suprapunerea programărilor. 16. Sistemul trebuie să permită gestionarea zilelor libere, sărbătorilor legale și altor indisponibilități, pentru a evita confuzia în rândul cetățenilor și suprasolicitarea administrației. 17. Sistemul trebuie să fie construit pe o arhitectură modulară, care să permită adăugarea ulterioară de noi funcționalități fără a afecta stabilitatea platformei existente. Fiecare modul trebuie să funcționeze independent, cu posibilitatea de integrare cu modulele existente prin API-uri securizate.
--	---

	18. Portalul trebuie să permită configurarea unei interfețe multilingve, adaptabilă automat în funcție de preferințele utilizatorului sau de locația sa geografică. 19. Sistemul trebuie să asigure disponibilitatea continuă, garantând un uptime de cel puțin 99.5%. În cazul unor întreruperi planificate sau accidentale, utilizatorii trebuie să fie notificați în prealabil, iar mesajele afișate să includă estimări privind durata indisponibilității. 20. Sistemul trebuie să permită gestionarea cererilor prin fluxuri de lucru configurabile, care să includă etape predefinite, responsabili și termene limită configurabile. Fluxurile trebuie să permită escaladarea automată în cazul întârzierilor. 21. Portalul trebuie să includă funcționalități de notificare automată pentru utilizatori și administratori, informând despre evenimente importante precum termene limită, modificări de status ale cererilor sau alte acțiuni relevante. 22. Sistemul trebuie să permită adăugarea SLA-urilor (Service Level Agreements) pentru gestionarea mai eficientă a cererilor. Fiecare SLA trebuie să definească termene limită și criterii clare de procesare, astfel încât să fie monitorizat respectul față de timpul de răspuns și rezoluție. 23. Sistemul trebuie să permită încărcarea de documente prin funcționalitatea de drag and drop, validând automat formatul și dimensiunea acestora. Utilizatorii trebuie să poată vizualiza documentele direct în portal, fără a fi necesară descărcarea lor. 24. Portalul trebuie să asigure editarea colaborativă a documentelor, inclusiv salvarea automată a modificărilor și gestionarea versiunilor anterioare. 25. Sistemul trebuie să permită generarea de documente pe baza șabloanelor predefinite, cu opțiuni pentru formate precum Word și PDF. 26. Sistemul trebuie să includă în Backoffice un motor avansat de căutare, care să permită utilizatorilor să găsească documente și informații utilizând criterii multiple, cum ar fi metadatele, tipurile de documente sau statusul acestora. 27. Sistemul trebuie să permită gestionarea sesizărilor cetățenilor printr-un modul dedicat, care să includă: • Clasificarea automată a sesizărilor pe categorii predefinite. • Posibilitatea de atașare a fișierelor justificative (ex. fotografii, capturi de ecran). • Pentru marcarea exactă a locației problemei raportate. 28. Portalul trebuie să includă un sistem de programări online care să permită: • Alegerea automată a intervalului disponibil pe baza unui calendar sincronizat cu resursele interne. • Trimiterea automată a confirmărilor de programare prin email sau SMS. • Anularea sau reprogramarea solicitării de către utilizator, respectând regulile de gestionare stabilite de administrație. 29. Sistemul trebuie să permită vizualizarea în timp real a statusului cererilor și sesizărilor. Fiecare utilizator trebuie să poată verifica detaliile și progresul acțiunilor administrative direct din contul său, primind notificări pentru fiecare actualizare importantă. 30. Funcționalitatea de raportare trebuie să includă: • Generarea automată de rapoarte periodice pentru administratori, cu date precum numărul de cereri procesate, timpul mediu de răspuns și categoriile cele mai frecvent utilizate. • Rapoarte detaliate configurabile, care să permită exportul în formate standardizate (PDF, Excel) și să includă grafice și diagrame personalizate. 31. Portalul trebuie să fie integrat cu platformele naționale relevante, cum ar fi RoEID pentru autentificare sigură și Monitorul Oficial pentru publicarea automată a anunțurilor oficiale. 32. Sistemul trebuie să expună un API REST complet, permițând integrarea cu alte aplicații interne sau externe, inclusiv soluții ERP sau CRM. 33. Sistemul trebuie să accepte integrarea cu soluții de plăți online, permițând utilizatorilor să efectueze tranzacții în siguranță, cu confirmarea automată a statusului plăților. 34. Integrarea cu platforma de plăți trebuie să fie configurabilă, oferind administratorilor posibilitatea de a adăuga noi tipuri de taxe sau servicii direct din interfața de administrare. 35. Sistemul trebuie să includă rapoarte financiare detaliate, cu opțiuni de export în format Excel sau PDF, pentru a sprijini activitatea
--	--

	departamentelor de contabilitate și audit. 36. Portalul trebuie să permită conectarea la sisteme GIS pentru afișarea informațiilor geografice, cum ar fi localizarea sesizărilor pe hartă. 37. Portalul trebuie să permită integrarea cu soluții de autentificare biometrice, cum ar fi recunoașterea facială sau amprente digitale, pentru a îmbunătăți securitatea accesului utilizatorilor. 38. Sistemul trebuie să fie capabil să comunice cu alte baze de date guvernamentale pentru validarea automată a datelor introduse de utilizatori, reducând astfel erorile și timpul de procesare. 39. Integrarea cu soluții de management al documentelor trebuie să permită transferul fizic rapid al documentelor între portal și sistemele interne ale administrației. 40. Portalul trebuie să suporte integrarea cu platforme externe de colectare a feedback-ului cetățenilor, permițând analizarea sugestiilor și reclamațiilor direct din sistem. 41. Sistemul trebuie să includă mecanisme de protecție împotriva atacurilor brute-force, blocând accesul după un număr prestabilit de încercări nereușite de autentificare. 42. Sistemul trebuie să păstreze un jurnal detaliat al activităților utilizatorilor, inclusiv accesarea, modificarea și ștergerea datelor. Acest jurnal trebuie să fie accesibil doar administratorilor autorizați. 43. Platforma trebuie să includă politici avansate de parolare, care să permită configurarea lungimii, complexității și frecvenței de resetare a parolilor. 44. Sistemul trebuie să implementeze politici stricte de protecție împotriva scurgerilor de date, inclusiv criptarea end-to-end pentru toate transferurile de fișiere între utilizatori și server. 45. Portalul trebuie să includă mecanisme de detectare și prevenire a activităților frauduloase, cum ar fi: • Monitorizarea traficului pentru identificarea comportamentului suspect (ex. încercări multiple de autentificare nereușite). • Alerte automate pentru administratorii sistemului în cazul detectării unui potențial atac. 46. Sistemul trebuie să ofere opțiuni de audit intern, permițând administratorilor să vizualizeze și să analizeze istoricul complet al activităților desfășurate de utilizatori și să genereze rapoarte de conformitate. 47. Pentru conformitate legală, portalul trebuie să implementeze politici de păstrare a datelor conform legislației naționale și europene. 48. Sistemul trebuie să fie capabil să gestioneze vârfurile de trafic, utilizând tehnologii de echilibrare a încărcării pentru a preveni suprasolicitatea. 49. Portalul trebuie să includă un mecanism de cache inteligent pentru accelerarea procesării cererilor frecvente și reducerea timpului de răspuns al sistemului. 50. Platforma trebuie să fie optimizată pentru integrarea cu soluții de cloud computing, permițând scalarea automată a resurselor în funcție de nevoi, fără intervenția manuală a administratorilor. 51. Portalul trebuie să permită gestionarea propunerilor de proiecte comunitare printr-un modul dedicat, care să includă funcționalități de înregistrare, publicare și votare. 52. Sistemul trebuie să permită utilizatorilor autentificați să încarce propuneri detaliate, incluzând descrieri, obiective, costuri estimate și beneficiari vizați. Aceste propuneri trebuie să fie afișate într-un catalog organizat, cu opțiuni avansate de filtrare și sortare. 53. Votarea trebuie să fie disponibilă exclusiv utilizatorilor autentificați, iar portalul trebuie să prevină dublarea voturilor pentru același utilizator. După închiderea sesiunii de vot, sistemul trebuie să genereze automat un raport al rezultatelor, inclusiv statistici privind numărul de voturi per proiect și nivelul de participare. Proiectele câștigătoare trebuie marcate clar, iar administratorii trebuie să poată exporta datele pentru raportare suplimentară. 54. Sistemul trebuie să permită afișarea evenimentelor locale printr-un calendar interactiv integrat. Fiecare eveniment trebuie să includă informații detaliate, precum data, ora, locația, descrierea și organizatorii. Utilizatorii trebuie să poată sincroniza aceste evenimente cu aplicații externe (de ex., Google Calendar) printr-un link de export standardizat (ICS).
--	--

	55. Portalul trebuie să includă un modul de rezervări pentru spații publice, cu afișarea disponibilității în timp real. Funcționalitatea trebuie să permită selectarea unui interval de timp, completarea unui formular standard și, dacă este cazul, plata online a tarifelor asociate. 56. Sistemul trebuie să notifice utilizatorii despre starea cererii de rezervare (aprobată, respinsă sau în așteptare) și să permită descărcarea unui document oficial care să confirme rezervarea. 57. Portalul trebuie să includă un sistem de gamificare pentru implicarea civică, care să atribuie puncte utilizatorilor pentru activități precum raportarea problemelor, votarea proiectelor comunitare sau participarea la evenimente organizate de administrație. 58. Sistemul trebuie să permită ca pentru fiecare utilizator să se permită acces la un dashboard personal, unde să poată vizualiza punctele acumulate, nivelul de implicare și eventualele recompense disponibile. 59. Clasamentul utilizatorilor activi trebuie să fie generat automat și să fie afișat pe portal într-o secțiune dedicată, cu opțiuni de sortare pe criterii temporale (ex., săptămânal, lunar, anual). Punctele acumulate trebuie să poată fi utilizate pentru obținerea de beneficii simbolice, cum ar fi diplome de recunoaștere digitală sau alte recompense aprobate de administrație. 60. Sistemul trebuie să permită comunicarea directă între cetățeni și funcționari printr-un modul de mesagerie securizat. Fiecare utilizator trebuie să poată iniția o conversație pentru cazuri specifice, atașând documentele necesare în cadrul discuției. 61. Funcționalitatea trebuie să includă notificări în timp real pentru mesajele noi și posibilitatea de căutare a conversațiilor anterioare după cuvinte-cheie. 62. Portalul trebuie să permită programarea întâlnirilor online cu funcționarii administrației, afișând disponibilitatea acestora într-un calendar dedicat. Utilizatorii trebuie să poată selecta intervalul dorit, să completeze un formular de solicitare și să primească confirmări automate prin email. 63. Sistemul trebuie să includă un link unic pentru întâlnirile virtuale, care să fie securizat și valid doar pentru sesiunea programată. 64. Tablourile de bord pentru parametrii de mediu trebuie să fie alimentate cu date în timp real, colectate de la senzori integrați la nivel local. 65. Sistemul trebuie să afișeze grafic indicatori precum calitatea aerului, nivelurile de poluare fonică sau valorile de temperatură. Utilizatorii trebuie să poată selecta perioade de timp specifice pentru a vizualiza date istorice sau să compare zone geografice diferite. 66. Fiecare tablou de bord trebuie să includă opțiuni de export al datelor în formate precum Excel sau PDF, pentru analiză suplimentară. În plus, portalul trebuie să integreze notificări automate care să alerteze cetățenii în cazul depășirii limitelor acceptabile pentru anumiți parametri (de ex., poluare excesivă). 67. Portalul trebuie să integreze un serviciu de tip locker pentru documente, care să permită cetățenilor să depună documente oficiale și să ridice răspunsurile din același punct. Sistemul trebuie să asigure securitatea accesului prin utilizarea unui cod unic generat automat, transmis utilizatorului prin email sau SMS. Locker-ul trebuie să fie monitorizat și să includă opțiuni de notificare automată pentru utilizatori, atât la depunere, cât și la disponibilitatea documentelor de ridicat. 68. Sistemul trebuie să respecte standardele de accesibilitate WAI-ARIA și să fie proiectat pentru utilizatori cu dizabilități. Funcționalități precum citirea vocală a conținutului, mărirea textului sau utilizarea unui mod de contrast ridicat trebuie să fie disponibile nativ. Navigarea exclusiv prin tastatură și suportul pentru dispozitive asistive trebuie, de asemenea, integrate. 69. Modulul GIS trebuie să permită afișarea informațiilor geospațiale relevante într-o interfață interactivă, care să includă funcții avansate de căutare, suprapunere a straturilor și export al datelor. Sistemul trebuie să permită afișarea planurilor urbanistice, a zonelor protejate și a proiectelor aflate în derulare, contribuind la creșterea transparenței și sprijinirea procesului decizional. Dashboard-urile pentru sustenabilitate trebuie să afișeze date detaliate despre inițiativele ecologice ale administrației locale, precum eficientizarea energetică, reducerea emisiilor de carbon sau programele de reciclare. Fiecare proiect trebuie să fie asociat cu indicatori cheie de performanță (KPI), iar datele să fie actualizate periodic pentru a reflecta progresul.
--	--

SOLUTIE DE BACK-UP SISTEME INFORMATICE-1 buc.	In cadrul componentei de cloud computing, solutiile software oferate vor beneficia de mecanisme de backup gazduite in centre de date performante, de preferat acreditate de Autoritatea pentru Digitalizarea Romaniei (ADR), care respecta specificatiile tehnice mentionate in documentatia de atribuire. Aceste centre sunt puse la dispozitie de ofertant si asigura continuitatea, disponibilitatea si securitatea operatiunilor. Centre de date Avand in vedere natura sensibila a informatiilor si documentelor gestionate in cadrul proiectului, asigurarea unui nivel ridicat de securitate si disponibilitate a datelor este esentiala. Astfel este obligatoriu ca acesta să dețină două centre de date proprii în România și să stocheze datele beneficiarului în aceste două centre de date, acreditate în temeiul Legii nr. 135/2007, având Ordin de autorizare a centrului de date, valabil pentru ambele. La finalizarea proiectului, toate datele vor fi migrate în centrele de date ale Autorității Contractante fără costuri suplimentare. Cerințe specifice pentru Centrul de Date: • Prestatorul să dețină minim două centre de date proprii în România și să stocheze datele Autorității contractante în aceste centre de date pe perioada derulării contractului, acreditate în temeiul Legii 135/2007, având ORDIN de autorizare a centrului de date emis de ADR, valabil în momentul ofertării. Nu se accepta centre de date în curs de certificare. • Centrele de date acreditate conform legii 135/2007 trebuie să fie distribuite pe zone geografice diferite ale țării și să dispună de funcția de replicare geografică a datelor, astfel încât datele create sau actualizate într-o locație primară și apoi replicate într-o locație secundară să existe în ambele locații. Aceste locații rămân complet independente una de cealaltă, pentru a putea garanta accesul la date în orice situație neprevăzută. • Centrele de date trebuie să fie minim clasificate Tier 3 ready - redundanță N + 1 pentru toate subsistemele și conexiunile utilizate, cât și pentru căile de alimentare echipamente. • Centrele de date vor asigura o lățime de bandă garantată de acces prin internet de 100 Mbps. • Centrele de date trebuie să fie echipate cu mantrap, sistem control acces, supraveghere video complet integrat SCADA pentru monitorizare și control remote și local a tuturor subsistemelor. • Prestatorul trebuie să asigure, pentru preluarea datelor electronice de la beneficiar, o comunicație securizata de tip VPN sau fibra optica "point to point" între centrul primar de procesare ale Prestatorului și locația/locațiile beneficiarului. • Prestatorul trebuie să asigure conexiunea internet garantată de 100 mbps prin fibră optică, minim 2 furnizori ISP per centru de procesare primar, respectiv secundar, prin prezentarea unor documente/dovezi. • În vederea asigurării redundanței automate a conexiunii, fiecare locație trebuie să aibă acces la internet prin protocol BGP, conectat la minim 2 furnizori ISP independenți, folosind clasa proprie de IP tip PI (Provider independent) cu AS number propriu. • Prestatorul va specifica în cadrul ofertei minim una din clasele de IP deținute și AS number-ul acestuia, informație care să poată fi verificată pe site-ul www.ripe.net. • Prestatorul va prezenta un plan de continuitate a activității. Continuitatea activității în caz de avarie, necesita realizarea unui Centru Recuperare în caz de Dezastru (DRC - Disaster Recovery Center). • Centrul de date trebuie să aibă o structură scalabilă, atât în ceea ce privește echipamentele informatice utilizate cât și infrastructura de suport, cu scopul de a menține performanțele sistemului la un nivel constant în cazul apariției de condiții noi (mărirea capacității centrului de date). Centrul de date trebuie să aibă o infrastructură virtualizată pentru a asigura posibilitatea scalării dinamice a capacității de procesare și stocare. Disponibilitatea ridicată a serverelor să fie asigurată printr-o structură cluster și backup pentru aceste servere.
SOLUTIE DE INTELIGENTA ARTIFICIALA (A.I.) – 1 buc.	1. Interacțiune Publică (Cetățeni): Cetățenii vor putea accesa asistentul virtual direct pe website-ul primăriei, chiar și fără a fi autentificați. Aceștia vor putea interacționa cu informațiile disponibile publicului, cum ar fi documente, formulare, proceduri administrative și alte date relevante, utilizând un chatbot bazat pe Inteligență Artificială. Interacțiunea va fi simplă și intuitivă, iar cetățenii vor putea să își găsească rapid informațiile dorite prin întrebări directe.

- **Chatbot avansat bazat pe NLP:**
 - Un sistem bazat pe Inteligență Artificială, capabil să răspundă întrebărilor cetățenilor în limbaj natural, fără a necesita navigare complexă pe website.
 - **Disponibil 24/7:** Chatbot-ul este integrat pe website-ul primăriei și permite acces rapid la informații administrative publice, cum ar fi:
 - **Proceduri administrative:** „Cum pot solicita o autorizație de construire?”
 - **Ghiduri și formulare:** Chatbot-ul oferă linkuri directe către documentele relevante.
 - **Program de lucru și alte informații generale:** Cetățenii pot afla detalii despre orele de funcționare, locația primăriei etc.
- **Căutare semantică:**
 - Motorul de căutare permite utilizatorilor să acceseze informații detaliate, analizând nu doar cuvinte-cheie, ci și intenția utilizatorului.
 - **Beneficii suplimentare:**
 - Acces rapid la informații relevante, fără bariere tehnice.
 - Reducerea timpului necesar pentru găsirea informațiilor.
 - Ghidare personalizată pentru navigarea în portal.
 - **Exemple:**
 - „Care este programul de funcționare al primăriei?”
 - „Unde pot plăti impozitele?”
 - „Care sunt regulile pentru construirea unei anexe la casă?”
- **Crearea unui sentiment de încredere și transparență:**
 - Răspunsuri clare și detaliate despre procedurile administrative reduc incertitudinile cetățenilor.
 - **Exemplu:** „Procesarea cererii dvs. pentru autorizația de construire durează, de obicei, 30 de zile lucrătoare. Vă voi ține la curent cu statusul cererii odată ce este înregistrată.”
- **Reducerea necesității de a contacta direct personalul primăriei:**
 - Chatbot-ul poate rezolva autonom întrebările frecvente, ceea ce reduce timpul de așteptare pentru apeluri telefonice sau vizite fizice.
 - **Exemple:**
 - „Cum pot obține un certificat de urbanism?”
 - „Ce documente sunt necesare pentru înregistrarea unei firme?”
- **Promovarea digitalizării și utilizării platformelor online:**
 - Chatbot-ul educă cetățenii despre beneficiile utilizării portalului digital al primăriei, încurajându-i să creeze conturi și să acceseze servicii online.
 - **Exemplu:** „Puteți crea un cont pentru a vizualiza istoricul taxelor plătite. Doriți să începem?”
- **Acces continuu și suport în timp real:**
 - Cetățenii pot accesa chatbot-ul oricând, inclusiv în afara programului de lucru al primăriei, ceea ce este util pentru nevoi urgente.
- **Asistență în mai multe limbi:**
 - Chatbot-ul poate răspunde în mai multe limbi, adresând astfel nevoile comunităților diverse din punct de vedere cultural sau lingvistic.
 - **Exemplu:** „Doriți informații în engleză, maghiară sau română?”
- **Monitorizarea și îmbunătățirea experienței utilizatorilor:**
 - Chatbot-ul colectează feedback de la cetățeni după fiecare interacțiune, ajutând primăria să identifice domeniile care necesită îmbunătățiri.

	○ Exemplu: „V-a fost util răspunsul meu? Da/Nu. Dacă nu, vă rog să specificați ce informații lipseau.” • Personalizare și proactivitate: ○ Chatbot-ul identifică tipare în comportamentul utilizatorilor și oferă sugestii personalizate. ○ Exemplu: „Observ că ai mai completat o cerere similară anul trecut. Doriți să folosim aceleași date pentru o procesare mai rapidă?” 2. Instrumente pentru angajații primăriei: Pentru angajații primăriei, asistentul virtual va deveni un instrument puternic de interogare internă a datelor și documentelor, permițându-le să acceseze rapid informațiile din arhivele electronice, să verifice statusurile cererilor sau să genereze documente pe baza datelor existente. Angajații vor putea utiliza soluția pentru a răspunde la întrebările interne legate de diverse procese administrative sau pentru a automatiza anumite fluxuri de lucru, totul cu ajutorul Inteligenței Artificiale care va învăța din interacțiunile anterioare. Inteligența Artificială va facilita gestionarea și procesarea rapidă a cererilor, contribuind la eficiența și transparența comunicării între administrație și cetățeni. • Asistență pentru gestionarea cererilor: • Clasificare automată: Chatbot-ul analizează și clasifică cererile cetățenilor în funcție de tip, urgență și complexitate, trimițând automat solicitările către departamentele relevante. ○ Alocare resurse: Sugerează angajaților prioritizarea cererilor pe baza istoricului și volumului de muncă curent. • Automatizarea răspunsurilor frecvente: ○ Chatbot-ul poate genera automat răspunsuri pentru întrebările frecvente primite prin portal sau email, reducând sarcinile repetitive ale angajaților. • Căutare și acces rapid la documente: • Indexare avansată: Documentele din arhiva electronică sunt analizate și indexate, făcând posibilă căutarea prin fraze naturale (ex.: „Actele necesare pentru obținerea certificatului de urbanism”). • Sugestii inteligente: Pe baza solicitării unui angajat, chatbot-ul sugerează documente sau informații relevante. • Suport decizional: • Chatbot-ul analizează datele disponibile și oferă sugestii pentru soluționarea cererilor complexe, bazate pe precedente sau reguli interne configurate. • Exemple: ○ „Această cerere poate fi soluționată fără aviz suplimentar?” ○ „Care este termenul legal pentru această procedură?” • Instrument de formare pentru angajați: • Ghiduri și proceduri: Chatbot-ul poate servi drept un manual digital, oferind răspunsuri rapide despre proceduri interne, fluxuri administrative sau legislație aplicabilă. • Exemple: ○ „Care este procedura pentru aprobarea unui PUZ (Plan Urbanistic Zonal)?”
--	---

	○ „Cum se gestionează o contestație?” • Reducerea stresului operațional: • Prin gestionarea automată a întrebărilor frecvente, clasificarea documentelor și crearea rapoartelor, chatbot-ul reduce sarcina administrativă repetitivă, lăsând angajații să se concentreze pe cazurile complexe. • Integrarea cu procesele existente: • Funcționează alături de aplicații precum DMS (Document Management Systems), facilitând accesul direct la resursele necesare. • Căutare avansată în arhive: • Angajații pot accesa rapid documentele necesare utilizând căutări pe bază de cuvinte-cheie sau întrebări formulate natural (ex.: „Care sunt cererile aprobate în ultima lună?”). • Indexare avansată prin OCR: - Documentele scanate sunt procesate prin OCR (Optical Character Recognition), ceea ce permite căutări precise chiar și în documente fizice digitalizate. 4.Dashboard: ○ Analiză operațională: Generarea de rapoarte detaliate privind timpul mediu de procesare a cererilor, nivelul de satisfacție al cetățenilor și volumul de lucru. Soluția „Inteligența Artificială pentru Cetățeni și Administrație” aduce un grad ridicat de inovare prin: 1. Transformarea proceselor tradiționale în fluxuri complet digitalizate: 2. Integrarea RAG (Retrieval-Augmented Generation): ○ Permite extragerea și sintetizarea informațiilor relevante din documentele arhivate pentru răspunsuri personalizate și precise. ○ Sistemul combină căutarea tradițională cu generarea contextuală a răspunsurilor, oferind utilizatorilor informații clare și relevante în câteva secunde. 3. Automatizare bazată pe inteligență artificială: ○ Chatbot-ul funcționează ca un asistent virtual complet, capabil să ghideze utilizatorii prin procese complexe (de ex.: completarea unei cereri pentru autorizație de construire). ○ Sistemul detectează nevoile utilizatorilor pe baza întrebărilor și propune soluții proactive. 4. Interfață bazată pe limbaj natural: ○ Cetățenii pot interacționa cu soluția folosind întrebări în limbaj natural, fără a avea nevoie de cunoștințe tehnice sau de navigare complexă. ○ Motorul NLP este capabil să recunoască sinonime, întrebări incomplete și să sugereze completări logice. 5. Impact în timp real: ○ Monitorizarea în timp real a cererilor și notificările automate îmbunătățesc transparența și încrederea în instituție. ○ Rapoartele operaționale generate automat ajută la luarea deciziilor bazate pe date. 6. Accesibilitate universală: ○ Funcționalități pentru persoane cu dizabilități, inclusiv navigare vocală, text-to-speech și suport pentru contrast ridicat. ○ Disponibilitate multilingvă pentru comunitățile diverse, asigurând incluziunea digitală. 7. Scalabilitate pentru viitor: ○ Soluția este modulară, permițând adăugarea de noi funcționalități, cum ar fi integrarea cu platforme de plăți sau implementarea de noi fluxuri administrative (ex.: gestionarea sesizărilor publice). ○ Arhitectura trebuie să fie bazată atât pe cloud cât și pe on premises ceea ce permite extinderea fără a compromite performanța. 8. Economii financiare: ○ Reducerea costurilor operaționale prin automatizarea proceselor și reducerea utilizării documentelor fizice.
--	--

SERVICII DE DIGITALIZARE FOND ARHIVISTIC ISTORIC-1 buc.	1. Spatiul de procesare Ofertantul trebuie sa detina minim doua centre de procesare, cu capacitati echivalente, astfel incat in cazul aparitiei unor defectiuni sau calamitati naturale, activitatea de scanare sa poata fi continuata cu un impact minim asupra termenului de finalizare a proiectului. Ofertantul va indica locatia centrelor de procesare. Ofertantul trebuie sa faca dovada ca spatiul/spatiile in care va derula operatiunile de prelucrare/depozitare care ofera cel mai inalt nivel de securitate, astfel acesta trebuie sa detina: • Sistem de monitorizare antiefracție și intervenție rapidă asigurată de o societate specializată • Camere de luat vederi în centrele de procesare/depozitare cu înregistrarea permanentă a activității și posibilitatea de stocare a imaginilor • Sistem autorizat de stingere a incendiilor • Sistem de acces cu cartela Ofertantul va anexa ofertei, documentele justificative în vederea demonstrării cerințelor de mai sus. Ofertantul trebuie să asigure conexiunea internet garantată de 100 mbps prin fibră optică, minim 2 furnizori ISP per locație. În vederea asigurării redundanței automate a conexiunii, fiecare locație trebuie să aibă acces la internet prin protocol BGP, conectat la minim 2 furnizori ISP independenți, folosind clasa proprie de IP tip PI (Provider independent) cu AS number propriu Prestatorul va face dovada existenței, pentru fiecare locație, a minim 2 conexiuni FO cu ISP-uri independente 2. Dotari specifice Ofertantul trebuie sa dețină două centre de date proprii în România/alt stat UE și să stocheze datele beneficiarului în aceste doua centre de date, acreditate în temeiul Legii 135/2007, având ORDIN de autorizare a centrului de date, valabil pentru ambele. 2.1. Cerinte specifice Centru de Date • Tier 3 ready - redundanță N + 1 pentru toate subsistemele și conexiunile utilizate, căi multiple de alimentare echipamente • Echipat cu sistem stingere incendiu cu gaz inert • Echipat cu mantrap, sistem control acces, supraveghere video • Complet integrat SCADA pentru monitorizare și control remote și local a tuturor subsistemelor Pentru a asigura o maxima siguranță asupra datelor în timpul procesului de indexare în caz de calamitate naturală, cele 2 centre de date trebuie să fie pe falii geografii diferite și storage-ul datelor să fie georeplicat. 2.2. Echipamente de scanare Echipamentele de scanare utilizate vor asigura scanarea duplex într-o singură trecere. Se vor folosi scannere profesionale atât pentru A4/A3, pentru formate atipice mai mici de A4, precum și pentru documente tip planșe (A2, A1, A0). Prestatorul va opera suficiente echipamente pentru a asigura un flux continuu de procesare a documentelor, inclusiv în situația defectării unui echipament Echipamentele de scanare trebuie să permită cel puțin următoarele funcții necesare: 2.2.1. Scanner de mare viteză cu ADF • Mod de scanare simplex/duplex printr-o singură trecere • Format hârtie: până la A3 • Greutate hârtie: aprox 22-155 g/m² Mod document lung - 3000 mm max. • Viteza de scanare: de 100 ppm/200 ipm, color, alb-negru și în tonuri de gri.
---	---

	• Conectivitate USB 2.0 standard cu posibilitatea de conectare a unui echipament de scanare flatbed A3 Alimentare automata până la 500 coli • Alimentator fiabil pentru diferite tipuri de documente • Alimentare frontală și circuit rotativ pentru utilizare comodă • Detecție multifeed ultrasonică cu setări avansate de grosime și dimensiune a documentelor; • Senzori pentru detecția capselor pentru a evita deteriorarea documentelor Rezoluție optico de scanare: aprox 200-600DPI 2.2.2. Scannere Flatbed: • Mod de scanare simplex • Format hârtie: până la A3 • Scanare dublă continuă, într-un singur fișier • Să ofere posibilitatea scanării documentelor fragile, legate • Viteza de scanare minim 3.5 secunde pentru un format A3, color, alb-negru și în tonuri de gri • Sursa de lumina LED, echipamentul să nu aibă lampă care se încălzește. Se elimină astfel încălzirea sticlei de scanare, pentru a nu afecta documentele fragile • Posibilitatea de anulare a luminii ambiante permite utilizatorilor să scaneze cu capacul deschis și să obțină imagini de înaltă calitate. Această caracteristică să îmbunătățească productivitatea în cazul scanării unor volume importante la viteză mare 2.2.3. Scanner de carte format A2 • Acesta trebuie să permită scanarea documentelor degradate, scanare fără atingere, fără lumină caldă, păstrând integritatea documentelor. • Echipamentul are următoarele funcționalități: • Format maxim - A2++ (660 x 450 mm) • Rezoluție optica – 400-800 DPI • Timp de scanare - 0.5 sec indiferent de dimensiunea originalului; • Timp de ciclu complet - 4 sec indiferent de dimensiunea originalului; • Moduri scanare: color - 42bit input/ 24 bit output; gri 14 bit input/8 bit output; alb negru 1 bit input/1 bit output • Leagăn automat pentru cărți în formă de V cu reglare manuală independentă a unghiului de înclinare a leagănului; • Unghi de deschidere 90, 120 și 180 de grade inclusiv; • Sticlă de presiune securizată, pliabilă, fără cadru, cu acționare manuală și mecanism de blocare în poziție orizontală și verticală; • Detectarea automată a dimensiunii originalelor; • Abilitatea de a sări rapid la orice imagine scanată; • Împărțirea automată a unei pagini în două pagini separate cu salvarea ulterioară ca două fișiere separate; • Mod de mascare gratuit (selectarea fragmentelor) la previzualizare în timp real; 2.2.4. Scanner de plase până la A0+ • Documentele de format atipic sau mai mari de A3 vor fi scanate cu echipament ptr documente A0+ • Rezoluție optică - aprox 1200 dpi
--	---

- Lățime maximă de scanare - aprox 42inch (1067 mm)
- Detectează și afișează lățimea documentului în timp ce acesta este încărcat (mm sau inch)
- Viteza de scanare greyscale&mono - aprox 330 mm / sec
- Viteza de scanare color - aprox 300 mm / sec
- Alimentare prin față, ieșire prin spate
- Mod de scanare simplex printr-o singură trecere
- Trebuie să poată fi folosit pentru scanări de calitate înaltă a hărților de format mare, planurilor de situație, desenelor tehnice, randărilor arhitecturale și altor documente tehnice.
- Latime de scanare scanare de până la 1067 mm și cu o grosime de până la 2 mm.
- Folosește tehnologia digitală SingleSensor, tehnologie care combină senzori de contact CIS pentru a mări semnificativ calitatea optică și stabilitatea alinierii pixeli-lor.
- Alimentare dinamică cu documente
- Scannerul să aibă încorporată interfață digitală SuperSpeed USB 3.0. Interfață USB 3.0 lucrează la până 5Gb/sec

2.2.5. Echipamentele de scanare complexe:

- Stația de lucru trebuie să combine scanarea inovatoare de tip „drop feed” cu performanța unui scanner de producție de mare capacitate,
- Stația de lucru trebuie să ofere 4 tipuri de alimentare, având în vedere diversitatea și importanța documentelor:
 - automată de „tip drop-feed”
 - automată de tip pachet
 - alimentare unică
- Stația de lucru trebuie să scaneze începând cu o singură foaie tip, până la o varietate mare de dimensiuni și volume de hârtie
- Viteza de scanare până la 110ppm/220ipm @300 dpi
- Stația de lucru trebuie să dețină o bandă transportoare care să poată susține până la 700 pagini permițând o capacitate mare de procesare neîntreruptă, continuă.
- Stația de lucru trebuie să poată scana și procesa o gama variată de tipuri de hârtie de diferite dimensiuni max. A3
- Stația de lucru trebuie să dețină un dispozitiv extern de capturare a imaginilor
- Stația de lucru trebuie să dețină minim 4 bin-uri pentru detecția și colectarea diversificată a documentelor
- Stația de lucru trebuie să dețină scanner încorporat față-verso printr-o singură trecere
- Stația de lucru trebuie să permită rescanearea documentelor fără a întrerupe procesul inițial, în cazul în care a avut loc un blocaj de proces.
- Stația de lucru trebuie să conțină un modul de tip “Multi ID-assist” prin care să permită auto-clasificarea documentelor conform regulilor setate de operator.
- Stația de lucru trebuie să permită detecția multifeed ultrasónica cu setări avansate de grosime și dimensiune a documentelor;

Ofertantul va atașa la propunerea tehnică documente doveditoare din care să rezulte că deține minim un echipament din fiecare tip, menționat mai sus

2.3. Captura de date

Pentru asigurarea prestării eficiente și atingerii obiectivelor serviciilor, furnizorul trebuie să utilizeze pentru prestarea serviciilor o platformă informatică de procesare electronică și captură, cu scopul de a reduce timpul de căutare și identificare al documentelor, prin utilizarea documentelor digitale temporare

	rezultate și de a conserva documentele, în conformitate cu prevederile legale în vigoare, pe perioada derulării serviciilor de digitizare. 2.3.1. Platforma de procesare electronică și capture • Trebuie să asigure o modalitate standard de procesare la nivelul Instituției și exploatare a documentelor digitale rezultate. • Platforma de procesare va oferi transparență în urmărirea stadiului procesării documentelor pentru realizarea arhivei digitale, prin furnizarea de informații referitoare la status lucrări direct din platformă. • Platforma software trebuie să ofere, în paralel, un flux de arhivare conform legii nr. 135/2007, pentru eventualitatea în care există documente ce se doresc a fi arhivate conform legii nr. 135/2007. Se va lua în calcul un volum de 2Tb/an disponibil pentru documentele electronice arhivate conform legii nr.135/2007. • Platforma să aibă suport pentru toate etapele de arhivare fizică și computerizată a documentelor: urmărire inventariere fizică, clasificare documente primite, indexare și verificare metadate, respectiv căutare și vizualizare. • Platforma să nu aibă limită de licențiere la nivel de stafii de lucru. • Pentru procesul de OCR-izare se vor utiliza licențe care nu sunt limitate de volumul de pagini procesate. • Platforma să ofere posibilitatea de integrare cu un server de email pentru facilitarea setării canalului de import prin e-mail și transmiterii unor notificări pe e-mail. Este necesară monitorizarea automată a trasabilității interogărilor efectuate în arhiva electronică. Notificarea va fi transmisă către administratorul aplicației și va cuprinde: nume-user, data, ora, informații solicitate/documente accesate. • Platforma trebuie să demonstreze că reprezintă un tot unitar care are minimum server de web, aplicații și baze de date, integrate în cadrul aceluiași produs software de tip platformă. • Licența să fie însoțită de garanție și servicii de mentenanță oferite de producătorul platformei licențiate pe perioada derulării serviciilor de digitizare. • Platforma trebuie să ruleze într-o arhitectură de tip cluster și trebuie să ofere mecanisme de HA (high availability) atât pentru clustering cât și pentru load-balancing (echilibrarea încărcăturii). • Platforma trebuie să permită rularea pe ultima versiune de server a oricărei aplicații realizate/dezvoltate/testate pentru orice versiune anterioară (backward compatibility) fără a fi necesară migrarea ei (in-place upgrade). • Platforma trebuie să ofere posibilitatea de aplicare a unei teme unitare la nivel de Front-End, bazate pe un framework de tip Bootstrap. 2.3.2. Accesul în aplicație • Accesul în platformă se va face prin interfață web, cu acces dintr-un browser web standard precum Chrome, Firefox, Edge sau Safari pentru toate stațiile de lucru. • Platforma trebuie să furnizeze utilizatorilor acces diferit, în funcție de rolul lor în sistem cu permisiuni diferite în funcție de tipul de activitate (de exemplu operațiuni arhivare, indexare metavariabile, vizualizare documente, administrare proiecte). • Platforma permite integrarea cu sistem LDAP (cum ar fi Microsoft Active Directory). Permite sincronizarea automată între grupurile funcționale din aplicație și grupurile de utilizatori definite în sistemul de Active Directory • Platforma trebuie să permită setarea unui IP (sau lista de IP-uri) de la care se permite acces unui grup de utilizatori • Platforma trebuie să permită autentificare de tip single sign on - toate modulele/componentele vor avea același set de utilizatori și nu trebuie solicitată autentificarea pentru a accesa alt modul. • Platforma trebuie să permită setarea de OneTimePassword (OTP), cu generare de parolă one time, cu setarea timpului de viață.
--	---

- Platforma trebuie să permită schimbarea setărilor parolei și a limbii de către utilizator
- Nu vor salva parolele utilizatorilor în mod vizibil în baza de date, doar în forma criptată. Platforma nu stochează parolele utilizatorilor în text clar sau folosind o funcție hash care este considerată nesigură.
- Platforma trebuie să permită o arhitectură de autentificare unică (SSO).
- Platforma trebuie să suporte autentificarea SAML v1.1 și 2.0.

2.3.3. Cerințe Generele Tehnice ale Platformei

- Platforma trebuie să funcționeze pe conexiune securizată HTTPS.
- Platforma trebuie să fie testată de terță parte din punct de vedere penetrare la nivel de aplicație. Se va depune la ofertă testul de penetrare realizat.
- Platforma trebuie să fie un sistem complet integrat, scalabil, deschis și extensibil, ce va permite interoperabilitatea cu sisteme informatice terțe prin API (REST / WSDL / SOAP). Expune un API cu un set de metode/funcții pentru gestionarea procesului de digitizare (ex. IMPORT documente) și al documentelor digitizate (verificare status, export în alte aplicații), generând formate de reprezentare XML/JSON.
- Platforma trebuie să permită alegerea limbii de afișare (cel puțin Română, Engleză)
- Platforma trebuie să permită înregistrarea utilizatorilor de către administrator, cu setarea rolului și grupului de care aparține
- Platforma trebuie să comunice cu un ansamblu de stocare cu capabilități de tip object storage (prin protocol S3), block storage și file storage.
- Toate butoanele și funcțiile care nu pot fi folosite la un moment dat trebuie marcate în mod vizual ca inactive.
- Platforma trebuie să furnizeze confirmări/alerte. De exemplu atunci când utilizatorul efectuează o acțiune de ștergere trebuie să afișeze dialog/mesaj de confirmare pe ecran.
- Pentru acțiunile din timpul serviciilor de digitizare de lungă durată platforma trebuie să afișeze în mod grafic că acțiunea este în desfășurarea și progresul acestora.
- Platforma trebuie să furnizeze mesaje de confirmare la acțiunile de salvare pentru a face clar pentru utilizator că sistemul a înregistrat acțiunea dată.
- Platforma trebuie să permită vizualizarea log-ului de autentificare în platformă și acțiunile utilizatorilor.
- Configurare și administrare a platformei

2.3.3.1. Platforma trebuie să permită:

- gestionarea mai multor subcompanii (instituții subsidiare) în același timp.
- gestionarea mai multor proiecte în același timp.
- configurarea de tipologii de documente cu metadescriptori, care pot fi comune în cadrul aceluiași proiect sau specifice unei tipologii de documente
- conexiunea mai multor documente într-un grup de documente (dosar/colecție de documente).
- setarea fluxului de procesare, utilizând diferite servicii (OCR-izare, clasificare) și regulile de validare
- permite afișarea unui link de acces pentru fiecare document, link ce poate fi transmis pe mail
- Setarea per tipologie de document a următoarelor servicii:
 - OCR-izare automată de către platformă cu urmărirea stării de prelucrare din interfață pentru un număr mare de documente
 - Clasificare automata
 - Rutarea documentelor pe fluxuri pot fi definite dintr-o interfață în aplicație, fără necesitatea de a scrie cod.

- Pentru implementarea proceselor de business complexe, sistemul va permite și dezvoltarea de scripturi pentru automatizări suplimentare.
- Setarea modulelor descrise mai jos

2.3.4. Metadescriptori:

- În cadrul platformei fiecare metadescriptor poate fi alocat uneia sau mai multor faze (de exemplu inventariere, sau indexare metadescriptori). În funcție de fază, datele aferente câmpului vor fi preluate în acea fază.
- În cadrul platformei trebuie să fie posibilă configurarea textului care va fi afișat pentru numele câmpului precum și descrierea acestora (pentru a permite adăugarea unor informații pentru utilizatorii care vor indexa sau verifica datele).
- Platforma trebuie să permită setarea tipului de dată per metadescriptor (ex. data, text, număr decimal, listă de valori predefinite). În funcție de tipul de metadescriptor setat, permite setarea unui anumit format.
- În cadrul platformei detaliile profilului metadescriptorului va fi afișat în mod vizual (detalii sub formă de listă/tabel etc.) și va fi editabil
- Platforma trebuie să permită preluarea automată a metadescriptorilor din textul documentelor folosind modalități inteligente, bazate pe cuvinte cheie sau expresii regulate REGEXP.
- Platforma trebuie să permită validare text extras din tabelele bazei de date alocate. Exemplu - extragerea numelui dosarului sau nr. volum dosar pot fi validate în tabelele Listă nume dosare alocate.
- Platforma trebuie să permită transformarea datelor preluate automat: prin formatarea datelor (ex. dacă data regăsită în text are alt format, decât cel setat), transformă toate literele în literele mari/mici sau alocarea unei valori predefinite, în funcție de valoarea găsită (de ex., dacă se regăsește 19% -> metadata va avea valoare predefinită 'G').
- În cadrul platformei calibrarea se face într-o pagină de simulare și rulare, pe un număr de documente de test stabilită de operator. Dacă rezultatul este acceptat, se aplică regula pe toate documentele deja existente în sistem și regula se va aplica pentru documentele nou importate.
- Platforma trebuie să permită setarea validării manuale pentru documentele care nu au trecut de extragerea automată a textului și validarea acestuia.

2.3.5. Canale import

- Platforma trebuie să permită rularea unui agent, care va fi pus pe anumite stații, și care să aibă acces la fișierele locale (salvate într-un anumit folder) și care transmite automat (printr-un API) fișierele aflate în acel folder. Aceasta trebuie să funcționeze atât pe stații cu sistem de operare Windows cât și Linux.
- Platforma trebuie să se integreze cu serviciul de e-mail intern.
- Platforma trebuie să permită încărcarea automată a e-mailurilor și atașamentelor transmise la anumite căsuțe de email, cu definirea de reguli avansate de procesare minim pe baza de: Subiect; expresii REGEX pe conținut/body mail; domeniu expeditor; adresa email expeditor; mail destinat to; mail destinat CC și BCC
- Platforma trebuie să dispună de reguli de setare conturi de email, reguli de import și acțiuni în fluxul de procesare se realizează într-o pagină de administrare.

2.3.6. Modulele Platformei

- toate modulele trebuie să fie accesibile dintr-un browser web

2.3.6.1. Modulul Statie Inventariere

- Să permită configurarea de stații de lucru și operațiuni de inventariere și alocare de operațiuni per stații de lucru
- Să permită stabilirea de fluxuri de lucru pentru prelucrarea cutiilor, prin setarea operațiunilor de inventariere
- Să permită configurarea regulilor de prelucrare cutii (ex. dintr-o cutie primită se sortează în două cutii)
- permită configurarea de grup de operatori care să lucreze pe stații s Să ofere trasabilitatea obiectului inventariat: palet/cutie/dosar
- Să ofere rapoarte/dashboard despre starea lucrării (cutii prelucrate, detalii pe ierahii de cutii/dosare).
- Sa ofere rapoarte, informații privind numele operatorilor care au efectuat activitatea de inventariere pe fiecare document în parte.
- Să fie posibilă preluarea datelor de inventariere precum identificatori documente, sau date de dosare, număr de pagini.
- Să fie posibilă alocarea unei baze de date de verificare pentru identificatorii de dosare/documente preluate
- Câmpurile de inventariere trebuie să fie configurabile
- Sa existe trasabilitate despre toate operațiunile efectuate
- Generare de Proces Verbal de predare cutii/dosare (cu date de identificare cutie/dosar)
- Platforma trebuie să permită regăsirea după cod de bare asociate cu identificatorul unic al cutiei/dosarului/documentului
- Se va furniza o aplicație mobilă (preferabilă pe Android), care va oferi informații pe baza unui identificator unic scanat (scanare de barcode 1D, 2D) sau introdus.

2.3.6.2. Modulul Clasificare

- Clasificarea și sortarea avansată a documentelor PDF să se poată realiza prin mai multe tehnici:
 - folosind separatori identificați automat.
 - folosind o analiză bazată pe conținut (cuvinte cheie)
 - folosind o analiză bazată pe aspect (layout)
 - abordare hibridă.
- Posibilitate de setare reguli de clasificare pentru fiecare tipologie de document, bazată pe cuvinte cheie și expresii regulate. Se pot defini cuvinte cheie pentru fiecare tip de document și ponderea acestor cuvinte cheie
- Calibrarea se face într-o pagină de simulare și rulare, pe un număr de documente de test stabilită de operator. Dacă rezultatul este acceptat, se aplică regula pe toate documentele deja existente în sistem și regula se va aplica pentru documentele nou importate.
- Posibilitatea de setare clasificare prin învățare, bazată pe aspect
- Dacă sunt aplicate mai multe tehnici de clasificare, să poată fi aplicată o regulă de votare

2.3.6.3. Modulul Statie Indexare si Validare

- Trebuie să fie posibilă configurarea de cel puțin 2 nivele de validare (validare primară, supervizare) cu alocare de grupuri de operatori per tipologii de documente sau per dosar (un operator indexează/validază un singur tip de document sau toate tipurile de document, la nivelul unui dosar) s în cazul procesării unui dosar, trebuie să fie posibilă setarea ordinii de validare a documentelor.
- Operatorii să primească automat documentul de validat (image PDF și metadata), după ordinea stabilită
- Afisarea simultană a documentului PDF și a câmpurilor de preluare a metadescrptorilor.

	• Să permită operațiuni OCR ON THE FLY pe imaginile scanate • Modalitate de vizualizare paralelă a metadescriptorului cu valoarea extrasă automat (dacă a fost setată extragerea automată pentru acest metadescriptor) și valoarea introdusă de operator. • Operatorii să aibă posibilitatea de a vizualiza alte documente din dosar (dacă proiectul este tarta la nivel de dosar), dacă este nevoie. • Operatorii (în funcție de rol) să aibă posibilitatea de modificare a tipului de document alocat (dacă acesta a fost clasificat greșit) • Operatorii (în funcție de rol) să aibă posibilitatea de tăiere a unui document PDF • Operatorii să aibă posibilitatea de alegere a unei excepții, la nivel de metadată (metadata nu poate fi validată) sau la nivel de document (ex. imaginea PDF este ilizibilă) • Platforma să aibă posibilitatea de a oferi rapoarte cu privire la metadatele indexate per operatori, tipologii de documente, dosare. 2.3.6.4. Modulul de Verificare Excepții • Trebuie să fie posibilă configurarea de cel puțin 2 nivele de tratare excepții (primară, escaladată) cu alocare de grupuri de operatori per tipologii de excepții (un operator indexează/validază un singur tip de excepție sau toate tipurile de excepții) • Operatorii să aibă posibilitatea de a vizualiza alte documente din dosar, dacă este nevoie • Operatorii (în funcție de rol) să aibă posibilitatea de modificare a tipului de document (dacă acesta a fost clasificat greșit) • Operatorii (în funcție de rol) să aibă posibilitatea de tăiere a unui document PDF • Operatorii să aibă posibilitate de validare, dacă excepția este acceptată. 2.3.6.5. Modulul Stație Urmărire operațiuni de indexare • Urmărirea stării de OCR-izare automată de către platformă • Urmărirea stării de validare realizată • Urmărirea cantităților de indexare realizate de operatori • Să fie posibilă urmărirea stării pentru toate documentele din platformă și afișarea de statistici și grafice privind numărul de documente și pagini procesate într-un interval de timp selectabil, număr de operatori și metadata validate, număr de excepții, etc. 2.3.6.6. Modulul Căutare și Vizualizare • Platforma trebuie să includă un modul de căutare și vizualizare a documentelor rezultate în urma procesului de digitizare. • Platforma trebuie să permită vizualizarea documentelor PDF folosind un vizualizator direct în browser cu navigare, paginare, mărire/micșorare, tipărire, căutare. • Să poată afișa informații detaliate despre fiecare fișier în parte inclusiv meta-descriptorii preluați conform celor de mai sus într-un format tabelar/liste de proprietăți. • Să ofere facilități avansate de cautare full-text în toate documentele din arhivă, căutarea în toți metadescriptorii, proprietățile documentelor și textele OCR-izate, folosind un singur câmp de tip text. • Platforma trebuie să permită căutarea folosind diverse expresii de căutare precum text exact, și, operatori logici (SI/SAU, diferit de, asemănător cu, etc) • Platforma trebuie să permită configurarea accesului la colecții de documente pentru grupuri de utilizatori, grupate pe mai multe nivele
--	--

	configurabile • Trebuie să fie posibilă descărcarea documentelor PDF doar pentru utilizatorii care au acest drept • Va fi permisă realizarea căutărilor în funcție de metadate, proprietăți ale documentelor (status, număr pagini, data încărcării în sistem, etc.), precum și căutare fulltext, în conținutul documentului OCR-izat (dacă a fost OCR-izat) per grupuri/roluri de utilizatori • Va fi permis exportul metadescrptorilor selectați per grupuri/roluri de utilizatori Aplicatia si functionalitatile descrise mai sus nu fac obiectul prezentei achizitii. Nu se doreste achizitionarea unei solutii informatice. Aplicatia si functionalitatile descrise mai sus nu fac obiectul prezentei achizitii. Nu se doreste achizitionarea unei solutii informatice, Solutia urmand a fi utilizata doar pe perioada de derulare a contractului 3. Acreditari si certificari Ofertantul trebuie sa faca dovada implementării următoarelor standarde: ISO 14001; ISO 9001; ISO 27001; ISO 20000-1 ISO 9001, ISO 14001, ISO 20000-1, ISO 27001, ISO 45001 Prestatorul trebuie sa aibe centrele de date certificate MCSI confor legii 135/2007 Prestatorul trebuie să fie autorizat ca administrator de servicii de arhivare electronică conform Legii 135/2007 - privind arhivarea documentelor în forma electronică. Acesta autorizație este necesara ptr a asigura securitatea datelor procesate in timpul serviciului de indexare Se va pune la dispoziția Beneficiarului o asigurare pentru erori și omisiuni (de ex Scrisoare de garanție din partea unei instituții financiare de specialitate sau Poliță de asigurare de răspundere civilă generală la o societate de asigurare) în valoare de 400.000 Euro, din care 300.000 pe eveniment, valabilă la data depunerii ofertei (diferența de 100.000 euro se va constitui după semnarea contractului). Prestatorul trebuie sa fie certificat pentru a furniza servicii calificate de marcare temporală în conformitate cu Regulamentul (UE) nr. 910/2014 (Regulamentul eIDAS). Serviciile calificate de marcare temporală pot dovedi faptul că o înregistrare electronică a existat înainte de o anumită perioadă de timp. Aceste servicii pot fi utilizate în sprijinul serviciilor de non-repudiare, pentru a dovedi că o semnătură electronică a fost generată în perioada de valabilitate a unui certificat cu cheie publică, pentru a sprijini arhivarea electronică pe termen lung. Serviciile calificate de marcare temporală asigură utilizarea unei surse de timp fiabile și gestionarea corectă a tuturor informatiilor din sistem. 4. Sesiune DEMONSTRATIVA pentru functionalitatile platformei de procesare electronica și creare proiect nou și configurarea acestuia cu tipologii de documente și metadate, conform caietului de sarcini. • Definire ierarhie de dosar cu mai multe tipologii de documente (se vor defini 3 tipuri) • Definirea unei stații de inventariere cutii și operațiuni (ex. recepție, legătorie, numerotare, pregătire documente pentru scanare, constituire unități arhivistice și legare, inventariere). • Vizualizarea informațiilor privind activitatea de inventariere de către reprezentantul instituției. • Definirea de reguli de clasificare automată pe 3 categorii de documente și rularea în pagină de simulare • a clasificării automate • Definirea de reguli de extragere automată pentru una sau două metadate și rularea în pagina de simulare a rezultatului. Se va demonstra folosind un document care conține mai multe metadate de același fel, iar platforma să extragă automat pe cel de pagina din document care are un titlu specific. • Importul automat a fișierelor scanate dintr-un folder și clasificarea automată a lor după 3 tipologii definite mai sus. • OCR-izare automată de către platformă cu urmărirea stării de prelucrare din interfață pentru un număr mare de documente. (100 documente)
--	---

	• Indexarea și validarea metadescriptorilor de către operator, pentru documentele unui dosar. • Setarea unei excepții de validare de către operatorul de validare • în modulul de validare se va demonstra extragerea automată prealabilă a datelor din câmpul număr document din conținutul text al documentului și validarea de către un operator. • Vizualizarea stării procesării de către administrator pentru documentele aflate în etapa de preluare meta-descriptori cu vizualizare grafic pentru numărul de documente și pagini procesate într-un interval de timp. • Setare export metadescriptori în format XML și imagine PDF. • Căutarea și vizualizarea a documentelor digitizate folosind căutare în tot textul documentului și în metadescriptori folosind diverse criterii de căutare. Documentul PDF se va afișa în browser folosind vizualizatorul împreună cu metadescriptorii asociați 5. Continuitatea activității Prestatorul va prezenta un plan de continuitate a activității. Continuitatea activității în caz de avarie, necesită realizarea unui Centru Recuperare în caz de Dezastru (DRC - Disaster Recovery Center). În ceea ce privește condiția de continuitate a activității proceselor de digitizare în cazul întreruperii funcționării centrului primar trebuie luat în considerare un centru de procesare alternativ, astfel încât operarea să poată fi reluată într-un interval de timp foarte scurt, care să nu perturbe activitatea serviciilor curente întreprinse în cadrul procesului. DRC va asigura continuitatea operării tuturor proceselor critice existente. Mecanismul utilizat este de replicare a proceselor între cele două locații astfel încât în ambele centre să se poată îndeplini în siguranță contractul. Principalele aspecte care trebuie luate în considerare în cadrul planului de continuitate sunt: • înalta Disponibilitate (High availability) este capacitatea de a procesa datele indiferent de defecțiunile locale, chiar dacă aceste probleme sunt în procese organizaționale, în utilități sau în echipamentele hardware sau software; acest concept trebuie luat în considerare la proiectarea soluției tehnice la nivelul echipamentelor și al infrastructurii; • Continuitatea operațiunilor este capacitatea de a menține lucrurile să ruleze atunci când totul funcționează corespunzător; • Recuperarea în caz de dezastru (Disaster Recovery) este capacitatea de a recupera un centru de date prin intermediul unui site diferit situat într-o locație diferită de cea a centrului primar de pe teritoriul României, dacă un dezastru distruge site-ul primar care devine astfel inoperabil. Specificul unei soluții de recuperare în caz de dezastru presupune continuarea activităților într-o altă locație și pe un hardware diferit. Prestatorul va prezenta soluția propusă privind planul de continuitate a activității. Prestatorul va asigura confidențialitate absolută asupra informațiilor procesate, în caz contrar va suporta sancțiunile prevăzute de legislația în vigoare. Având în vedere faptul că prestarea serviciilor presupune accesul la date cu caracter personal preluate de la Beneficiar sau transferate la Beneficiar, Prestatorul este responsabil de implementarea măsurilor stabilite de comun acord cu Beneficiarul în vederea asigurării protecției datelor cu caracter personal în conformitate cu Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. Relația contractuală dintre Beneficiar și Prestatorul de servicii trebuie să fie conformă cu cerințele prevăzute la art.28 GDPR.
SERVICII RECONSTRUCTIE WEBSITE-1 buc.	• Website-ul este construit conform structurii standard furnizate de MCID, care este organizată într-un mod clar și coerent pentru a asigura accesul facil la informații relevante. Această structură include secțiuni principale, precum Primărie și Consiliul Local, care oferă detalii despre administrația locală și activitatea acesteia. De asemenea, sunt integrate secțiuni dedicate pentru Informații de Interes Public, menite să asigure transparența și să răspundă nevoilor cetățenilor în ceea ce privește accesul la date oficiale. În cadrul structurii se regăsesc și capitole esențiale pentru Transparență și Integritate Instituțională, care contribuie la consolidarea încrederii publicului în instituțiile locale. Totodată, website-ul include acces la Monitorul Oficial Local, care facilitează consultarea documentelor oficiale publicate de administrație. Pe lângă aceste categorii

	principale, sunt disponibile și alte categorii și subcategorii, adaptate nevoilor comunității, pentru o navigare simplă și o experiență utilizator îmbunătățită. Astfel, structura site-ului respectă toate cerințele și standardele stabilite de MCID. - Website-ul este prevăzut cu diverse modalități de accesibilitate special concepute pentru a facilita utilizarea de către persoanele cu dizabilități. Aceste funcționalități sunt implementate pentru a asigura acces egal la informațiile și serviciile oferite, indiferent de nevoile specifice ale utilizatorilor. Printre măsurile incluse se numără opțiuni de ajustare a dimensiunii textului, contrast sporit pentru o vizibilitate mai bună, navigare optimizată cu tastatura și alte elemente care îmbunătățesc experiența utilizatorilor cu deficiențe de vedere, mobilitate sau alte tipuri de dizabilități. Aceste inițiative reflectă angajamentul website-ului de a respecta standardele internaționale privind accesibilitatea digitală și de a crea un mediu online incluziv, accesibil pentru toți. - Interfața website-ului este proiectată astfel încât să își mențină proporțiile și funcționalitatea optimă pe o gamă variată de dispozitive, indiferent de rezoluția acestora. Această caracteristică asigură o experiență plăcută și coerentă utilizatorilor, fie că accesează site-ul de pe un computer desktop, un laptop, o tabletă sau un telefon mobil. Prin implementarea unui design responsiv, elementele vizuale și funcționale ale interfeței se adaptează automat la dimensiunea ecranului utilizat, păstrând un echilibru între estetică și utilizabilitate. Această abordare modernă contribuie la crearea unei experiențe unitare și profesionale, garantând accesibilitatea conținutului și funcționalitatea completă pe orice dispozitiv. - Interfața website-ului este concepută pentru a fi utilizată cu ușurință de către cetățeni, oferind o experiență intuitivă și prietenoasă. Structura sa clară și bine organizată permite navigarea rapidă și accesul facil la informațiile și funcționalitățile disponibile. Fiecare element al interfeței, de la meniuri până la butoane și secțiuni, este proiectat cu scopul de a ghida utilizatorul într-un mod natural, fără a necesita cunoștințe tehnice avansate. Printr-o combinație de design modern și funcționalitate optimizată, website-ul asigură că toate categoriile de utilizatori, indiferent de experiența digitală, pot accesa și utiliza resursele disponibile într-un mod eficient și confortabil. - Website-ul este proiectat astfel încât informațiile puse la dispoziție să poată fi accesate cu ușurință de către cetățenii vorbitori de limbi străine. Acesta include opțiuni dedicate pentru traducerea conținutului în mai multe limbi, facilitând înțelegerea informațiilor de către utilizatorii internaționali sau cei care nu vorbesc limba română. Prin integrarea funcționalităților multilingve, precum selectarea rapidă a limbii dorite sau utilizarea unor traduceri clare și precise, website-ul își extinde accesibilitatea către un public divers. Astfel, indiferent de limba preferată, cetățenii pot accesa informațiile esențiale într-un mod simplu și eficient, consolidând deschiderea și accesibilitatea platformei. - Website-ul oferă o funcție de Căutare bine optimizată, care permite cetățenilor să găsească rapid informații sau documente specifice. Indiferent de complexitatea sau volumul informațiilor disponibile pe site, funcția de Căutare facilitează localizarea exactă a datelor dorite prin introducerea de cuvinte-cheie sau expresii. Astfel, utilizatorii beneficiază de o experiență mai rapidă și mai comodă, economisind timp și accesând direct resursele de care au nevoie. Această caracteristică contribuie la creșterea accesibilității și a utilizabilității platformei pentru toți cetățenii. - Website-ul afișează orarul de funcționare într-un mod dinamic, organizat pe zile, pentru a facilita accesul rapid și clar la informațiile necesare. Această funcționalitate permite cetățenilor să vizualizeze în timp real programul de lucru, adaptat pentru fiecare zi a săptămânii, eliminând orice confuzie legată de orele de funcționare. Orarul dinamic este integrat într-un format prietenos și ușor de utilizat, asigurând o navigare simplă și eficientă. Această abordare modernă îmbunătățește experiența utilizatorului, oferindu-le cetățenilor informații actualizate într-un mod intuitiv și accesibil. - Administrarea portalului se realizează printr-un sistem de autentificare securizat, bazat pe utilizator și parolă, asigurând accesul exclusiv persoanelor autorizate. Pentru a oferi un nivel suplimentar de securitate, platforma permite implementarea de restricții bazate pe clase de IP-uri, limitând accesul doar de la locații specifice sau rețele de încredere. Această combinație de măsuri de protecție garantează o administrare sigură a portalului, reducând riscul de acces neautorizat și protejând datele sensibile ale platformei. Prin acest sistem robust de securitate, portalul oferă atât funcționalitate, cât și protecție avansată pentru administratorii săi. - Platforma permite administratorilor și operatorilor să încarce rapid și eficient mai multe fișiere simultan, fie prin selectare în masă, fie utilizând funcționalitatea intuitivă de drag & drop. Această opțiune modernă simplifică procesul de gestionare a conținutului, economisind timp și efort atunci când este necesară încărcarea unui volum mare de documente. Interfața prietenoasă și optimizată asigură o utilizare ușoară, iar fișierele
--	---

	sunt gestionate eficient pentru a răspunde cerințelor de organizare și accesibilitate ale portalului. Această funcționalitate contribuie la creșterea productivității și la o administrare mai fluidă a resurselor digitale. - Website-ul oferă o funcționalitate avansată de gestionare a fișierelor, permițând utilizatorilor să le caute rapid folosind funcția Căutare integrată. Fișierele pot fi filtrate eficient după criterii precum data încărcării sau tipul de fișier, incluzând categorii precum imagini, videoclipuri, fișiere audio, documente text, foi de calcul și arhive. În plus, utilizatorii au posibilitatea de a previzualiza fișierele direct în funcție de tipul acestora, ceea ce facilitează identificarea rapidă a conținutului dorit. Această funcționalitate modernă contribuie la o organizare mai bună și la o experiență de utilizare îmbunătățită, economisind timp și oferind un acces mai intuitiv la resursele disponibile. - Portalul unitații este echipat cu o funcționalitate completă pentru publicarea, editarea și previzualizarea articolelor, oferind utilizatorilor un instrument eficient pentru gestionarea conținutului. Funcția de publicare permite adăugarea de articole noi pe platformă, oferind o interfață simplă și rapidă pentru introducerea textului, imaginilor, videoclipurilor și altor tipuri de conținut multimedia. Acest proces este gândit pentru a asigura un flux de lucru clar, fără complicații, astfel încât utilizatorii să poată contribui la portal fără dificultăți. - Opțiunea de editare permite modificarea oricărui articol deja publicat, având la dispoziție un editor ușor de utilizat, care permite actualizarea informațiilor, corectarea greșelilor sau adăugarea de noi detalii. Aceasta asigură că informațiile afișate pe portal sunt întotdeauna relevante, corecte și actualizate. De asemenea, funcția de previzualizare oferă posibilitatea de a vizualiza articolul înainte de publicare, oferind utilizatorilor șansa de a vedea cum va arăta conținutul pe portal și de a face ultimele ajustări, pentru a se asigura că totul este în conformitate cu standardele dorite. - Prin integrarea acestor funcționalități, portalul devine un instrument foarte eficient pentru gestionarea și actualizarea constantă a conținutului, oferind autorilor și administratorilor posibilitatea de a crea, ajusta și publica articole într-un mod ușor și organizat. Aceste caracteristici sunt esențiale pentru menținerea unui flux continuu de informații actualizate și pentru o comunicare eficientă cu utilizatorii portalului.
APLICATIE URBANISM -1 buc.	<i>Cerințe minimale și descriere funcționalități ale modului Urbanism</i> Obiectivul implementării Modulului de Urbanism este acela de a permite UAT un management integrat al documentațiilor de urbanism, bazat pe identificarea cu acuratețe de 100% și identificarea regimului tehnic aferent și aplicabil unui amplasament pe baza reglementărilor în vigoare existente și aplicabile acelui amplasament, la nivel de Regulament Local de Urbanism, conform prevederilor PUG-ului în vigoare, integrând nativ și automat prevederile aduse de toate PUZ-urile, PUD-urile și restricțiile existente. <i>Componenta de gestionare a documentațiilor de urbanism- cereri, emiteri CU/AC</i> <i>Cerințe minimale:</i> - Managementul documentelor specifice procesului de emiteri CU/AC- introducerea geocodată în soluția geospațială a documentelor specifice procesului de autorizare de tip cereri de emiteri CU/AC, CU, AC, gestionarea procesului de prelungire, PV de recepție la terminarea lucrărilor o Toate informațiile aferente procesului de urbanism vor fi poziționate fizic pe hartă, cu păstrarea unui istoric a tuturor documentațiilor gestionate, cu semnalizări pe baza unui cod de culori dinamic a iminenței expirării unor perioade de valabilitate. - Interfete de căutare sub formă de liste sau fise pentru consultarea informațiilor cu privire la documente de tip CU, AC emise la o adresă, cu filtrare după diferite criterii (tip lucrare, scop, beneficiar etc.) sau număr cadastral, sau număr topo cu posibilitatea de extragere a unui set de înregistrări sau a unei singure înregistrări și afișarea acestora direct în hartă. - Reprezentarea în hartă a locațiilor acolo unde documentele de tip CU, AC sunt expirate o Reprezentarea în hartă a locațiilor acolo unde documentele de tip CU, AC sunt în vigoare Sistemul trebuie să gestioneze activitatea departamentului de urbanism folosind tipuri de documente (autorizații, certificate, etc.) cu un format generat dinamic modificabil de către utilizator prin definirea de șabloane și de atribute multiple în funcție de nevoile evolutive ale clientului (fără limita de șabloane și fără limită de atribute sau de date folosite) ex: numele solicitantului, adresa acestuia, adresa obiectivului, valoarea taxelor etc. - Pentru fiecare tip de document se vor reține o serie de informații sub formă de date cu tipuri de date diverse (alfanumerice, numerice, grafice,

image etc.)

- Minimal, aplicația trebuie să aibă predefinite, fără a se limita doar la acestea, următoarele tipuri de șabloane: certificat de urbanism, autorizație de construcție.

- Aplicația va permite crearea ulterioară a altor tipuri de șabloane, în funcție de nevoile identificate pe parcursul utilizării.

- Operațiile disponibile asupra șabloanelor (minimal):

- Vizualizare;

- Modificare (cu reținerea istoricului tipului de document pe perioade de timp);

- Adăugare;

- Ștergere.

- Interfețele trebuie să poată permite filtrarea documentelor pe tipuri de documente.

- Interfețele trebuie să permită urmărirea poziției pe fluxul de procesare unde a ajuns cererea solicitantului.

- Interfețele trebuie să permită filtrarea și ordonarea documentelor în funcție de prioritate, vechime, termene de expirare etc.

- Aplicația trebuie să permită urmărirea încasării taxelor de emitere autorizație.

- Aplicația trebuie să asigure/să permită, fără a se limita doar la acestea, următoarele:

1. Reținerea datei de depunere a cererii, valabilitatea autorizațiilor/avizelor și să atenționeze apropierea termenului de expirare;

2. Localizarea pe hartă într-un sistem GIS al locațiilor pentru care s-au emis sau se solicită autorizații;

3. Căutarea pentru Autorizații/Avize emise, după filtre precum:

- a) Perioadă emitere;

- b) Solicitant;

- c) Alte filtre, cu posibilitate de memorare a condițiilor de filtrare și de utilizare ulterioară ținând cont de utilizatorul care le-a creat;

4. Calculul taxei pentru emiterea certificatului de urbanism;

5. Înscrierea, tipărirea, editarea, căutarea autorizațiilor de construire/desființare cu toate datele cerute de legislație;

6. Calculul taxei autorizației de construire;

7. Regularizarea taxei pentru acordarea autorizației de construire;

8. Alocarea automată de numere de înregistrare pentru înscrierile emise;

9. Evidența și înscrierea PV-urilor de recepție în sistem, în corelație cu autorizațiile aferente;

10. Evidența și înscrierea certificatelor de atestare a edificării construcțiilor în sistem, în corelație cu procesele verbale de recepție;

Aplicația trebuie să fie compatibilă cu legislația romană în vigoare și să permită modificări în acord cu evoluțiile legislative ulterioare, în principal prin parametrizare, fără a fi nevoie de modificarea codului.

WEB GIS:

Cerințe minime aplicație WEB GIS:

- Securizarea accesului la baza de date a sistemului integrat.

- Produsele software trebuie să asigure accesul utilizatorilor la sistem în mod securizat folosind mecanisme de autentificare și acordarea drepturilor, pe bază de roluri. Prin intermediul mecanismului propus se vor autentifica și autoriza în sistem utilizatorii definiți, în baza drepturilor de acces ce le-au fost alocate. După autentificare, fiecărui utilizator îi vor fi prezentate numai funcțiile pentru care este autorizat, în baza rolului deținut, excluzând posibilitatea de a apela în vreun fel alte funcții.

- Sistemul trebuie protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le înmagazinează. Sistemul va trebui să aibă implementat un sistem de securitate care va trebui să permită următoarele facilități:

	- Ierarhizarea în clase a utilizatorilor, conform unei politici de drepturi de acces adaptate și coerente prin gestionarea utilizatorilor și a drepturilor de acces - crearea de grupuri de acces și stabilirea drepturilor la nivel de grup sau la nivel individual (rezultatul fiind dat de reuniunea drepturilor de grup cu cele individuale); - Blocarea accesului direct la baza de date. Toate operațiile se vor face prin conectare la baza de date folosind aplicația; - Autentificarea utilizatorilor în aplicație trebuie să fie permisă de la orice punct de lucru din cadrul instituției; - Sistemul informatic oferit trebuie să includă toate componentele necesare asigurării integrității și confidențialității datelor. - Blocare acces la anumite layere în funcție de permisiuni, atât pentru vizualizare hartă, cât și pentru interogare harta. • Aplicația WEB GIS va putea fi folosită de un număr nelimitat de utilizatori ai beneficiarului, fără costuri suplimentare (de tipul cost per click pe hartă, consum de resurse) și pentru un număr nelimitat de utilizatori neautentificați aferenți portalului extern și fără costuri suplimentare (de tipul cost per click pe hartă, consum de resurse). • Aplicația WEB GIS trebuie să poată fi instalată pe mai multe tipuri de sisteme de operare, atât Windows cât și Linux sau alte asemenea. La fel și baza de date a aplicației. <i>Cerințe generale ale aplicației Web Gis:</i> - bara cu uneltele de bază specifice GIS, minim: zoom, pan, tool-tip; - funcții de căutare; - legenda pentru obiectele (elementele) și straturile tematice afișate; - posibilitatea de integrare și suprapunere automată cu date geospațiale disponibile în formate variate, printr-o interacțiune facilă; - să asigure funcționalitate «MapTip sau similar sau echivalent »-prin click să fie afișate o serie de informații alfanumerice setate de către administrator; - componentă publică construită pentru o interacțiune dinamică cu cetățeanul; - integrarea cu portalul web al UAT-ului; <i>Cerințe minimale:</i> • Posibilitatea generării rapoartelor conform legislației în vigoare (lista certificatelor de urbanism emise sau prelungite, lista începere lucrări, lista PV de recepție la terminarea lucrărilor, lista autorizațiilor emise sau prelungite — enumerarea de mai sus este doar una exemplificativă, aplicația trebuind să gestioneze totalitatea rapoartelor pe care legislația le impune) • Posibilitatea de a exporta rezultatele unui raport specific în format Excel. • Generarea, pe bază de criterii de selecție a informațiilor și a datelor care vor fi exportate în rapoarte, cu condiții de filtrare, ordonare etc a următoarelor rapoarte: a) Registrul de certificate urbanism; b) Registrul de autorizații construire/desfiintare; c) Registrul de procese verbale de încheiere lucrări; d) Registrul anunțurilor de începere lucrări; e) Registrul anunțurilor de încheiere lucrări. <i>Cerințe funcționale și caracteristici tehnice minime ce trebuie îndeplinite de aplicațiile informatice</i>
--	---

	Cerinte functionale generale Platforma pentru cetateni si platformele pentru gestionarea activitatilor de urbanism si cadastru vor fi gazduite in cloud apartinand ofertantului sau pe costurile ofertantului, accesul utilizatorilor facandu-se prin intermediul unui browser independent de sistemul de operare. Pentru aplicatiile informatice de backend (aplicatia de taxe si impozite locale, aplicatia destinata gestionarii registrului agricol, aplicatia informatica destinata gestionarii contractelor civile la nivelul UAT si celelalte aplicatii), instalarea acestora se poate face si pe server, unde va exista sistem de operare Windows Server, iar pe statiile de lucru se poate face instalarea aplicatiei, sau accesul utilizatorilor poate avea loc si prin intermediul unui browser, pentru portabilitate, optimizarea costurilor si usurinta administrarii centralizate a sistemului. Programul va fi dezvoltat pe platforma Microsoft SQL Server , instalabil pe un server cu sistem de operare Windows Server . În cazul în care se va folosi o altă platformă de baze de date, aplicatiile de backend vor fi livrate împreună cu toate licențele necesare funcționării sistemului, fără alte costuri suplimentare. Programul va indica cu claritate originea, conținutul și apartenența fiecărei date introduse. Programele vor trebui să prezinte un grad mare de parametrizare care să permită modificări rapide și facile. Rapoartele generate de programe trebuie să fie configurabile (coloane, rânduri, date tipăribile, antet, subsol, totaluri și subtotaluri, așezare în pagină etc.). Rapoartele trebuie să poată fi generate individual (de ex.: pentru o instituție publică subordonată sau un capitol de cheltuieli) precum și consolidat (de ex.: pentru o parte/toate instituțiile publice subordonate sau unele/toate capitolele de cheltuieli). Rapoartele trebuie să poată fi stocate electronic pentru o vizualizare ulterioară, printate în diferite formate (A4, A3) sau salvate ca fișiere .pdf, .doc, .xls, .xml etc. Toate modulele programelor trebuie să fie construite în conformitate cu prevederile legale și reglementările impuse de Ministerul Finanțelor Publice. Programul trebuie să poată fi adaptat noilor modificări legislative apărute ulterior. Programul va permite importul/exportul bazei de date. Programul va permite import/export de fișiere Visual FoxPro, Excel (.xls). text (.txt), word (.doc). Cerinte generale referitoare la interfața aplicației cu utilizatorul: Interfața aplicațiilor trebuie să fie integral în limba română. Toate ferestrele de dialog și mesajele trebuie să fie în limba română. Aplicațiile trebuie să folosească o interfață grafică consistentă, unitară la nivelul întregului produs, extensibilă, ușor de utilizat și ușor de învățat, bazată pe standarde de interfață: butoane, meniuri, filtre, sisteme de selecție. Interfața aplicațiilor trebuie să asigure verificarea câmpurilor de date obligatorii și opționale. Aplicațiile trebuie să furnizeze mecanisme de validare a introducerii datelor pentru evitarea tipurilor de date inconsistente. Aplicațiile trebuie să conducă utilizatorul în interiorul sistemului folosind meniuri și opțiuni. Pentru o operare eficientă, interfața trebuie să permită o căutare rapidă de informații după criterii multiple, cum ar fi: data, nr. document, valoare, tip operațiune, clasificare bugetară, denumirea bunurilor, nume/prenume, număr/dată contract, număr/dată chitanță etc. Aplicațiile trebuie să permită exportul datelor tabelare în formate de uz general: .pdf, .xls, .txt, .xlm, .html etc. Să ofere ajutor online pentru utilizarea aplicației, precum și manual în format electronic. Documentația oferită trebuie să fie actualizată cu fiecare versiune. Sistemul trebuie să dispună de funcția de ajutor la nivel de ecran (ajutor contextual, obligatoriu în limba română). Utilizarea aplicațiilor trebuie să fie intuitivă și simplă, iar erorile să se poată corecta ușor. Orice înregistrare introdusă greșit trebuie să se poată corecta. Aplicațiile nu trebuie să se blocheze aleator sau atunci când se introduc date greșite (date care ies din parametri sau sume) ci trebuie să avertizeze utilizatorul cu privire la eroare și să îi determine să introducă valoarea corectă. Aplicația nu trebuie să permită executarea operațiilor decât atunci când sunt îndeplinite toate condițiile necesare. Aplicațiile trebuie să pună la dispoziție un mecanism intuitiv și simplu de acces la datele din istoric, pentru anii precedenți, fără părăsirea aplicației. Administrarea utilizatorilor, a rolurilor și a drepturilor de acces trebuie să se facă dintr-o interfață intuitivă, dintr-un modul de configurare. Cerinte generale referitoare la raportări
--	---

	Facilitățile standard de raportare trebuie să cuprindă: -tipărirea rapoartelor în format text și/sau grafic folosind orice tip de imprimantă recunoscută de windows; -furnizarea tuturor rapoartelor în limba română; -furnizarea raportărilor on-line dar și facilități pentru interogări ad-hoc ale bazei de date integrate, pentru orice grup de tabele; -să permită filtrarea prin parametri care pot fi completați în momentul deschiderii raportului sau în momentul în care sunt executate de operator, dacă este cazul; -vizualizarea rapoartelor pe ecran înaintea tipăririi; - anularea tipăririi rapoartelor, înainte sau în timpul tipăririi; -posibilitatea reluării tipăririi unui raport de la un anumit articol/linie sau de la o anumită pagină, după o întrerupere accidentală a tipăririi; -exportul datelor rezultate în urma oricărei raportări în formate publice: .xls, .xml, .html, .csv, .rtf, .pdf, .txt etc. Pentru fiecare dintre rapoartele prezentate în oferta tehnică se va întocmi un document care să descrie formatul fiecărui raport, în următoarea structură: -Titlul raportului -Evenimentul declanșator al raportului -Descrierea conținutului pentru fiecare raport -Indicarea parametrilor de definire/selecție ai raportului -Macheta raportului: o captură de ecran sau o pagină care să cuprindă capul de tabel și, eventual, sfârșitul de raport: -Regulile de întocmire ale raportului; -Criteriile de ordonare a datelor; -Criteriile de grupare a datelor; -Formatul și orientarea raportului la imprimantă: (ex: A4, A3, orizontal/vertical). Cerințe generale referitoare la condițiile de exploatare, salvare/restaurare • Aplicațiile trebuie să se bazeze pe sistemul de prelucrare a tranzacțiilor (SPT). • Aplicațiile trebuie să permită accesul concurrent, în condiții optime, la baza de date a sistemului pentru cel puțin 50 de utilizatori simultan, cu evitarea blocărilor reciproce. • Actualizarea informațiilor din baza de date (adăugare/modificare/ștergere) efectuată de oricare dintre utilizatori trebuie să se realizeze în timp real. • Să nu conțină redundanțe. O informație să fie introdusă o singură dată în componentele sistemului. Aplicația trebuie să conțină rutine pentru verificarea consistenței și integrității datelor. • Aplicațiile trebuie să permită efectuarea operațiilor de back-up automat la un interval stabilit de către utilizatorii autorizați pentru operațiuni de salvare/restaurare a bazei de date și verificarea bazei de date, precum și corectarea eventualelor erori. Operația de restaurare a datelor (din back-up) trebuie să fie accesibilă din meniul programului informatic, doar utilizatorilor care au dreptul de a face back-up și/sau restaurare de baze de date. De asemenea, operațiunea de restaurare trebuie să se facă ușor și rapid și să poată fi efectuată de o persoană fără pregătire de specialitate în informatică și fără intervenția producătorului. • Aplicațiile trebuie să permită anularea de către persoanele autorizate a unei operațiuni efectuate și să dea posibilitatea raportării/vizualizării operațiunilor respective. • Utilizatorii trebuie să fie anunțați de o eventuală problemă în funcționarea rețelei, iar ieșirea din aplicație trebuie să se facă ușor și fără să afecteze datele introduse anterior în baza de date. • Aplicațiile nu trebuie să împiedice utilizatorii de a se conecta la sistem dacă acesta este în stare de eroare. • Aplicațiile trebuie să închidă automat sesiunile de lucru ale utilizatorilor în caz de inactivitate pe o anumită durată predeterminată de timp. • Cerințe generale referitoare la securitatea informațiilor
--	---

	• Pentru a se asigura confidențialitatea, securitatea informațiilor și monitorizarea accesului la date, aplicațiile vor fi prevazute cu un nomenclator de utilizatori și parole, administrați de către un administrator al aplicației, fără intervenția producătorului. • Aplicațiile trebuie să permită crearea de utilizatori și acordarea de drepturi de citire. introducere/actualizare, validare pentru fiecare modul al aplicației. • Utilizatorii autorizați ai aplicațiilor trebuie să aibă drepturi de acces la datele și funcțiunile acestora diferențiate în funcție de competențele ce le revin și configurabile, pentru ușurința gestionării, pe grupe de competențe corespunzătoare categoriilor de utilizatori. • Drepturile trebuie să poată fi definite atât individual, cât și la nivel de rol. Utilizatorii trebuie să poată avea atașate mai multe roluri. În funcție de drepturile utilizatorilor, fiecare dintre aceștia trebuie să poată accesa o anumită configurație de meniu, cea la care are dreptul și să poată efectua operațiuni doar pentru care are drepturi explicite. • Autentificarea utilizatorilor în aplicații trebuie să fie permisă de la orice punct de lucru din cadrul instituției. • Între categoriile de utilizatori ai aplicației trebuie să existe una cu drepturi speciale, predefinite, de administrare, care să realizeze: -definirea de utilizatori autorizați ai aplicației (atribuirea de nume utilizator și parolă); -crearea drepturilor de acces; -atribuirea drepturilor de acces pentru utilizatorii autorizați; -monitorizarea și controlul activității celorlalți utilizatori; -realizarea de validări globale asupra bazei de date pentru depistarea incoerențelor, inconsistenței informațiilor. • Aplicațiile trebuie să permită acordarea unui utilizator dreptul de salvare și restaurare a datelor. • Aplicațiile trebuie să permită jurnalizarea și raportarea detaliilor privitoare la accesul în sistem al utilizatorilor. • Mecanismul de tranzacționare și roll-back; în situația unei căderi accidentale a sistemului, toate tranzacțiile finalizate trebuie să fie permanente, iar cele nefinalizate trebuie anulate prin roll-back. • Aplicațiile trebuie să respecte condițiile de securitate, conform legislației în vigoare. Cerințe generale referitoare la performanțe în exploatare • Aplicațiile trebuie să ofere timpi de răspuns mici pentru: regăsirea, prelucrarea și actualizarea informațiilor din baza de date, exportul datelor în alte formate, precum și pentru transmiterea la imprimantă a diverselor rapoarte. • Timpii de răspuns menționați anterior nu trebuie să fie afectați semnificativ de: - creșterea numărului de utilizatori simultan conectați în sistem; -prelucrările masive de date. • Aplicațiile trebuie să permită extinderi ale numărului de utilizatori. • Flexibilitate pentru adaptare dinamică și dezvoltare, conform cerințelor care pot să apară. • Aplicațiile trebuie să permită urmărirea tuturor etapelor parcurse de orice document introdus în programul informatic (din ce a fost generat, ce alte documente a generat, în ce module a fost folosit etc.), precum și a persoanelor care lucrează și realizează modificări în baza de date.
INVENTARIEREA PATRIMONIULUI PUBLIC SI PRIVAT AL UAT - APLICATIE SOFTWARE SI SERVICII DE	<u>MODUL PATRIMONIU CU PLATFORMĂ INFORMATICĂ ȘI SERVICII INCLUSE</u> Funcționalități minime: <i>Crearea conturilor și definirea rolurilor</i> • Aplicația trebuie să permită crearea de conturi pentru utilizatori cu diferite nivele de acces de tipul: ○ Administrator ○ Tehnic

INVENTARIERE SOLUTII GIS-1 buc.	○ Vizitator ○ altele • Platforma trebuie să permită crearea unei structuri logice pentru gestionarea entităților subordonate primăriei • Aceste entități vor fi integrate într-o arhitectură flexibilă, care să permită gestionarea ierarhică a utilizatorilor și atribuirea de roluri în funcție de structura organizațională a primăriei sau a altor instituții publice afiliate. <i>Importul datelor existente</i> • Platforma trebuie să permită importul simplu și eficient al datelor din sistemele software deja utilizate de Autoritatea Contractanta. Acest import va include atât date administrative (de exemplu, informații despre active, registre, rapoarte) cât și date financiare sau tehnice • Platforma trebuie să fie capabilă să integreze date din diverse surse și sisteme existente și utilizate de către Autoritatea Contractantă fără a întrerupe activitatea curentă a primăriei. Integrarea trebuie să fie realizată fără erori și fără a solicita intervenția manuală constantă • Modulul trebuie să permită importul datelor existente în Contabilitate, din format digital (Excell, xml) • Modulul trebuie să permită importul geometriilor și atributele acestora în fișiere CGXML conforme cu platforma Ettera cât și a geometriilor de tip KML compatibile cu orice sistem spațial georeferențiat de tip web-based • Baza de date a primăriei trebuie să fie integrată ușor și fluid, fără efort din partea personalului primăriei și fără erori <i>Colectarea datelor din teren</i> • Platforma trebuie să permită actualizarea informațiilor de pe teren utilizând dispozitive mobile (telefoane inteligente, tablete, note-paduri) conectate la internet. • Utilizatorii trebuie să poată adăuga, modifica sau vizualiza date direct pe teren. • Platforma trebuie să permită actualizarea datelor în timp real. • Aplicația trebuie să fie optimizată pentru utilizarea pe termen lung pe dispozitive mobile, să aibă o interfață ușor de utilizat, consum redus de baterie și performanță constantă pe diverse tipuri de terminale mobile, inclusiv telefoane și tablete. • Platforma trebuie să permită utilizatorilor să importe fișiere spațiale de tip KML și CGXML direct de pe aplicația mobilă. Aceste fișiere vor conține date geospațiale, care vor fi preluate corect și integrate în sistem, fără a necesita intervenții suplimentare. • Platforma trebuie să includă funcționalitatea de determinare a locației exacte a utilizatorului pe teren prin GPS sau alte tehnologii de localizare. • Localizarea utilizatorului se poate face în două moduri: ○ Adresa utilizatorului trebuie să fie completată automat pe baza locației indicate de pointerul de pe hartă sau ○ Utilizatorul trebuie să poată căuta o locație pe hartă, iar pointerul să fie poziționat automat la adresa sau locația indicată • Toate datele actualizate de pe teren trebuie să fie sincronizate în timp real cu serverul central, fără erori • Aplicația trebuie să aibă o interfață prietenoasă, ușor de utilizat pe dispozitive mobile, care să permită operatorilor să completeze și să actualizeze rapid informațiile necesare • Platforma trebuie să poată accepta și importa fișiere geospațiale din diverse formate utilizate în industrie, direct de pe aplicația mobilă, inclusiv KML și CGXML. <i>Date spațiale și atribute standardizate pentru fiecare tip de activ</i> • Asocierea datelor spațiale și atributelor specifice fiecărui tip de activ (clădiri, drumuri, terenuri) • fiecare tip de activitate, să se genereze o fișă de colectare adaptată specificului activului inspectat.
--	---

- Fișa de colectare va solicita doar informațiile relevante
- Informațiile cuprinse pe fișa de date sunt predefinite, specific fiecărui activ inspectat, utilizatorul putând să aleagă valorile corecte
- Aplicația trebuie să permită descrierea detaliată a situației juridice a terenurilor, integrând și informații relevante din domeniul contabilității și gestiunii.
- Aplicația trebuie să faciliteze vizualizarea și gestionarea datelor tehnice ale terenurilor, inclusiv accelerarea seismică, tipul și clasa de sol, precum și vecinătățile, esențiale pentru analiza utilizărilor posibile ale terenurilor (ex. terenuri agricole, terenuri intravilane cu construcții).
- Aplicația trebuie să permită introducerea și gestionarea valorii de inventar și a valorii de concesiune a terenurilor, pentru o evidență completă a datelor economice.
- Aplicația trebuie să permită introducerea valorii terenurilor în orice monedă considerată relevantă pentru reflectarea corectă a valorii actuale pe piața imobiliară.

Arhiva digitala de documente

- Aplicația trebuie să permită centralizarea și securizarea documentelor relevante într-o arhivă digitală
- Aplicația trebuie să permită organizarea documentelor în categorii clar definite, pentru o gestionare eficientă și structurată a acestora.
- Aplicația trebuie să asigure acces rapid la documente pentru utilizatorii autorizați, printr-o interfață intuitivă și rapidă de căutare și vizualizare.
- Aplicația trebuie să permită configurarea unor nivele de acces diferite pentru utilizatorii autorizați, pentru a asigura protecția documentelor și prevenirea accesului neautorizat.
- Aplicația trebuie să garanteze stocarea sigură a documentelor, cu funcționalități de backup automat și posibilitatea de a urmări istoricul modificărilor pentru a preveni pierderea datelor.
- Aplicația trebuie să permită pentru fiecare activ introdus în sistem crearea unei arhive standardizate, ușor de utilizat, care să faciliteze digitizarea documentelor justificative aferente imobilului digitalizat.
- Platforma trebuie să permită previzualizarea, tipărirea direct din aplicație sau descărcarea documentelor justificative asociate fiecărui imobil, direct din arhiva digitalizată.
- Procesul de introducere a documentelor în arhiva digitală trebuie să fie intuitiv, cu un flux clar de utilizare, iar utilizatorii trebuie să fie ghidați de instrucțiuni simple și clare, în special în secțiunea dedicată actelor și imaginilor.

Documentare fotografica

- Aplicația trebuie să permită o vizualizare clară și detaliată a stării fiecărui activ
- Platforma trebuie să permită integrarea și vizualizarea imaginilor asociate activelor
- Aplicația trebuie să asigure transparență completă în administrarea patrimoniului
- Aplicația trebuie să permită încărcarea unui volum mare de imagini sau documentație fotografică, facilitând gestionarea eficientă a acestora.
- Platforma trebuie să ofere posibilitatea de a vizualiza imaginile sub formă de galerie, cu opțiuni de navigare ușoară între imagini.
- Aplicația trebuie să permită mărirea unei imagini la o dimensiune standard prin simpla selecție a acesteia, oferind o vizualizare clară și detaliată.
- Utilizatorii trebuie să poată naviga între imaginile mărite direct din galerie, fără a fi necesar să le descarce, pentru o experiență rapidă și eficientă.

Export de date

- Aplicația trebuie să permită partajarea și utilizarea datelor pentru analize externe sau raportări
- Platforma trebuie să permită exportul personalizat al datelor pentru un activ sau grupuri de active, în funcție de cerințele utilizatorilor.
- Aplicația trebuie să ofere utilizatorilor acces la datele relevante conform nevoilor lor specifice
- Aplicația trebuie să permită exportul fișei unui obiectiv în format PDF – Gata de printat.
- Aplicația trebuie să permită exportul datelor activului în format editabil Excel. Fisierul de export trebuie să cuprindă doar atributele activului.
- Platforma trebuie să permită exportul fișei activului în format editabil Word. Fisierul de export trebuie să cuprindă doar atributele activului.
- Aplicația trebuie să permită exportul hărții activului în format JPG. Harta exportată în format JPG poate să fie atașată Fișei de date a activului sau poate fi folosită ca fișier de sine stătător.
- Aplicația trebuie să permită exportul hărții activului în format KML (format spațial georeferențiat de tip open source). Fisierul poate fi descărcat în dispozitivul utilizatorului (telemobil sau calculator). Fisierul exportat în format KML trebuie să poată fi deschis cu orice sistem stereo-spațial, cum ar fi Google Earth,
- Harta activului exportată în format KML trebuie să conțină și toate atributele activului.
- Aplicația trebuie să permită vizualizarea și exportul pentru toate activele dintr-o categorie, similar cu exportul pentru un singur activ, printr-un meniu de export dedicat.
- Toate opțiunile de export menționate trebuie să fie valabile pentru întreaga suită de active, conform unui meniu de export centralizat.

Vizualizare patrimoniu cu posibilitate de partajare și embedare în infrastructura web actuală

- Aplicația trebuie să permită vizualizarea completă a patrimoniului, cu posibilitatea de partajare și consultare a datelor către dispozitive externe.
- Platforma trebuie să permită integrarea hărților și a altor informații relevante din aplicație în site-uri externe sau sisteme online, prin funcționalități de embedare.
- Funcția de embedare trebuie să asigure compatibilitatea cu infrastructurile digitale existente, sprijinind integrarea ușoară în site-urile instituțiilor publice, contribuind astfel la transparența datelor pentru cetățeni și colaboratori externi.
- Aplicația trebuie să permită vizualizarea datelor pe tot ecranul, menținând toate funcțiile Google, cu posibilitatea de a consulta activele în diverse configurații. Interacțiunea cu geometria sau pointerul trebuie să afișeze o casetă de informare cu detalii minime.
- Utilizatorii trebuie să poată accesa datele detaliate ale activului selectat printr-un click pe „Detalii”. În funcție de drepturile utilizatorului, aceștia trebuie să poată vizualiza sau edita informațiile.
- Aplicația trebuie să permită transmiterea hărții și a funcțiilor sale complete prin generarea unui link care poate fi copiat și trimis pe orice canal digital (e-mail, WhatsApp, Telegram, etc.).
- Platforma trebuie să permită embedarea hărții patrimoniului, cu toate funcționalitățile sale, prin acționarea unui buton care să copieze un cod în memoria temporară. Acest cod poate fi lipit în infrastructuri web externe.
- Aplicația trebuie să asigure un design responsive, astfel încât harta să se redimensioneze automat pentru a se adapta dimensiunii ecranului, respectând proprietățile paginii în care este integrată.

Analiza patrimoniu

- Aplicația trebuie să permită generarea de rapoarte detaliate și grafice financiare și operaționale bazate pe activele imobiliare.
- Platforma trebuie să utilizeze tehnologii de analiză avansată, inclusiv inteligența artificială (AI)
- Aplicația trebuie să permită introducerea valorii imobilului în orice monedă, inclusiv Aur (XAU), iar la analiza patrimoniului, aceste monede trebuie să poată fi convertite automat în moneda preferată.
- Aplicația trebuie să includă un grafic de tip PIE care să reprezinte raportul dintre numărul activelor și valoarea acestora pe fiecare categorie. Graficul trebuie să aibă un cerc exterior care să arate numărul activelor și un cerc interior care să arate valoarea acestora.
- Platforma trebuie să includă un grafic orizontal care să reprezinte numărul total al categoriilor de active, pentru a oferi o perspectivă reală asupra dimensiunii patrimoniului.
- Aplicația trebuie să includă un grafic vertical care să reprezinte valoarea totală a categoriilor de active, oferind o perspectivă reală asupra anvergurii patrimoniului.

Capacitatea platformei de a realiza procedura completa de Evaluare Vizuala Rapida

Procedura de EVALUARE VIZUALA RAPIDA privind diminuarea riscului seismic se realizeaza doar de catre personal autorizat, Evaluarea Vizuala Rapida este reglementata si descrisa de cadrul legislativ romanesc in special de legea 212/2022, procedura consta in: identificarea pe harta, geovectorizarea imobilului subiect, colectarea datelor solicitate si procesarea acestora in formularul standardizat conform Legii 212 din 12/07/2022, a Reglementarilor Tehnice din 14 decembrie 2022 (Metodologie de evaluare vizuala rapida a cladirilor Indicativ RTC 10 - 2022) din Noiembrie 2022. Formularul conform legii este exportat in format digital PDF.

- Aplicația trebuie să permită realizarea procedurilor standardizate de evaluare vizuală, în conformitate cu Legea 212 din 2022, pentru evaluarea rapidă a imobilelor.
- Platforma trebuie să organizeze datele colectate în timpul inspecției în sertare dedicate, asigurându-se că informațiile sunt ușor de accesat și structurate.
- Aplicația trebuie să permită identificarea imobilului prin vectorizarea acestuia sau prin utilizarea unui pointer pe harta interactivă. De asemenea, trebuie să includă un mod de vizualizare pe ecran complet.
- Platforma trebuie să colecteze toate datele necesare despre imobil în timpul inspecției, conform reglementărilor, și să le structureze eficient. Datele trebuie să includă accelerația seismică a zonei conform P 100-1, disponibile printr-o simplă acțiune de click pe harta zonei.
- Aplicația trebuie să includă un buton care va extrage informațiile din lege și va explica modul de interpretare a acestora, completând câmpurile corespunzătoare.
- Aplicația trebuie să permită utilizatorilor să confirme valoarea seismică orizontală, identificată prin pointer pe hartă, și să înregistreze aceste date în câmpul corespunzător.
- Aplicația trebuie să aibă opțiunea de a precompleta răspunsurile, care vor necesita doar selectarea corespunzătoare conform realității din teren. De asemenea, utilizatorii trebuie să poată încărca imagini sau schițe ale clădirii conform reglementărilor tehnice din „Metodologia de evaluare vizuală rapidă a clădirilor”.
- Aplicația trebuie să permită introducerea datelor referitoare la prestatorul serviciilor și la beneficiar, în funcție de tipul de cont al utilizatorului.
- Aplicația trebuie să permită finalizarea procedurii de inspecție tehnică și să permită verificarea și generarea formularului standardizat.
- Platforma trebuie să permită vizualizarea, editarea, ștergerea și exportarea listei imobilelor supuse evaluării vizuale rapide, cu opțiuni de:

- **Vizualizare:** pentru acces rapid la datele imobilului.
- **Editare:** pentru actualizarea informațiilor.
- **Ștergere:** pentru eliminarea datelor inutile.
- **Export:** opțiuni de export în formate diferite:
 - **Versiune direct pe imprimantă.**
 - **Versiune PDF.**
 - **Fișier editabil – CSV/Excel.**

- Aplicația trebuie să permită finalizarea procedurii de evaluare vizuală rapidă, conform prevederilor Legii 212 din 12/07/2022 și Reglementărilor Tehnice aprobate prin ORDINUL nr. 3.231 din 14 decembrie 2022. Acest proces include pașii necesari pentru generarea unui formular standardizat pe baza unui calcul automatizat al indicatorilor de asigurare seismică (IAS) și indicatorilor de priorizare a investițiilor (IPI).
- Platforma trebuie să permită vizualizarea tuturor datelor colectate în cadrul procesului de evaluare, organizate clar pentru fiecare imobil evaluat, într-o interfață ușor de navigat.
- În cazul identificării unor neconcordanțe în datele colectate, aplicația trebuie să permită editarea ușoară a acestora, inclusiv a geometriei, poziționării pe hartă, atributelor clădirii sau documentelor și imaginilor asociate. Acest lucru se face prin butonul de editare vizibil pe ecran.
- După editarea informațiilor, aplicația trebuie să afișeze un mesaj de confirmare a acțiunii de editare a datelor, astfel încât utilizatorii să poată verifica actualizările realizate.
- După procesul de verificare și eventuale editări, utilizatorii trebuie să poată accesa și vizualiza formularul standardizat printr-un buton dedicat. Formularul trebuie să fie organizat conform Legii 212 din 2022 și reglementărilor tehnice relevante, afișând indicii și factori de corecție care vor fi utilizați pentru calculul IAS și IPI.
- Utilizatorii trebuie să aibă posibilitatea de a naviga între secțiunile formularului pentru a vizualiza, edita sau șterge datele colectate.
- După completarea și verificarea formularului standardizat, aplicația trebuie să permită generarea unui formular final, NEEDITABIL, în format PDF. Acesta trebuie să fie exportabil printr-un buton clar marcat în interfață, iar formularul trebuie să fie complet conform reglementărilor tehnice.
- Formularul standardizat generat și exportat trebuie să fie în conformitate cu reglementările tehnice stabilite în „Metodologia de evaluare vizuală rapidă a clădirilor, Indicativ RTC 10 - 2022,” aprobate prin ORDINUL nr. 3.231 din 14 decembrie 2022.

Securitatea Datelor

- Platforma trebuie să dispună de o arhitectură de securitate avansată, care utilizează tehnologii de criptare de ultimă generație (simetrică și asimetrică), pentru a asigura protecția datelor sensibile. Aceasta trebuie să includă un sistem distribuit de tip blockchain pentru a garanta integritatea datelor, prevenind orice acces neautorizat sau modificare a acestora.
- Platforma trebuie să implementeze tehnologia Zero-Knowledge Proofs, care permite validarea datelor fără a le dezvălui conținutul, asigurând confidențialitatea absolută a informațiilor. Acest mecanism trebuie să fie integrat în fluxurile de procesare și transfer al datelor.
- Modulul de Patrimoniu trebuie să folosească un sistem distribuit de validare și consens, pentru a proteja datele împotriva atacurilor cibernetice avansate și vulnerabilităților. Acest sistem trebuie să fie eficient în garantarea unei protecții robuste și transparente a datelor.
- Platforma trebuie să includă tehnici avansate de machine learning și inteligență artificială pentru a monitoriza în mod continuu activitatea rețelei și fluxurile de date. Aceasta trebuie să permită identificarea și prevenirea amenințărilor și anomaliilor în timp real, asigurând astfel protecție activă împotriva atacurilor cibernetice sofisticate.

	- Platforma trebuie să permită realizarea de operațiuni complexe pe date criptate fără a compromite securitatea acestora. - Sistemul trebuie să fie complet scalabil și să se poată integra ușor în ecosisteme cloud hibride și infrastructuri on-premise. - Platforma trebuie să fie conformă cu reglementările internaționale privind protecția datelor, cum ar fi GDPR și HIPAA. - Modulul de Patrimoniu trebuie să protejeze datele ca cel mai valoros activ al organizației. Serviciile conexe: - Implementarea platformei în structura administrației publice: Instalarea și configurarea platformei pentru a corespunde nevoilor specifice ale Autorității Contractante, inclusiv crearea conturilor și setarea drepturilor de acces. - Importul datelor existente din infrastructura software actuală în MODULUL DE PATRIMONIU: Transferul și integrarea datelor din sisteme software existente în MODULUL DE PATRIMONIU. - Instructajul personalului: Organizarea de sesiuni de formare pentru utilizatorii platformei, de la operatorii tehnici la factorii de decizie. - Instructajul terților ce urmează să folosească platforma: Organizarea de sesiuni de formare pentru utilizatorii platformei, inclusiv specialiști externi (ing. Pentru EVR* și evaluator pentru evaluarea patrimoniului).
MODUL CADASTRU -1 buc.	<u>MODUL CADASTRU</u> <i>Componente ale aplicației de cadastru:</i> Hărți: - Va permite vizualizarea geospațială a imobilelor și terenurilor. - Va folosi o interfață grafică intuitivă și ușor de folosit pentru utilizatori. - Va oferi posibilitatea de a accesa și manipula baza de date geospațială de cadastru, în funcție de drepturile utilizatorilor, se permit operațiuni de creare, citire, actualizare sau ștergere asupra obiectelor spațiale din baza de date. - Va oferi posibilitatea de vizualizare a unor locații folosind Google street maps pentru a afișa situația din teren. Corelare autonomă și/sau interactivă a datelor din cadastru și registrul agricol: - Va trebui să faciliteze relaționarea dintre terenurile cu sau fără clădiri din modulul de cadastru cu terenurile din aplicația de registrul agricol. - Integrarea datelor între cele două aplicații se face în timp real folosind API-uri de conectare; - API-urile de integrare trebuie să comuncie într-un mod securizat folosind key de securitate pentru a nu permite accesul neautorizat la datele sistemelor. - Va oferi posibilitatea de selectare a cheilor unice de legătură dintre datele din cele două aplicații sau a criteriilor de relaționare. - Va oferi posibilitatea de a selecta grafic, pe hartă, geometriile terenurilor care trebuie asociate. - Va oferi posibilitatea de a selecta imobilele din date tabelare pentru relaționare. Publicitate: Înștiințarea deținătorilor de imobile cu privire la obligațiile lor legale: - Va permite accesul specialiștilor pentru efectuarea măsurătorilor. - Prezentarea actelor juridice referitoare la imobile. - Identificarea limitelor imobilelor împreună cu echipele de specialitate. - Verificarea informațiilor despre imobile în etapa de publicare a documentelor tehnice cadastrale (conform Art. 12 alin. 3 din Legea 7/1996 republicată). - Înregistrarea termenelor privitoare la imobile și generarea de avertizări specifice (de exemplu, împlinirea termenelor de posesie sau de afișare a ofertelor de vânzare). - Gestionarea ofertelor de vânzare pentru imobilele din extravilanul UAT, conform Legii 17/2014.

	- Va permite publicarea ofertelor de vânzare pentru imobilele din extravilanul UAT, în conformitate cu legislația în vigoare automat prin API-uri, direct in platforma cetateanului. Import/Export: - Va oferi interfețe pentru importul datelor din diferite formate: .cgxml, .gpkg, .shp, .dxf, .csv, etc. - Va oferi interfețe pentru exportul datelor în diferite formate: .gpkg, .shp, .dxf, .csv, etc. - Importul datelor se realizează în straturi dedicate, fără a afecta direct baza de date existentă. Generator de rapoarte: - Va pune la dispoziție generarea automată a documentelor specifice departamentului de cadastru. - Utilizarea șabloanelor prestabilite conform formularelor instituției. - Crearea de adeverințe, adrese, corespondență, comunicări, adeverințe APIA etc. - Va centraliza și afișa funcționarilor care utilizează modulul de cadastru, cererile venite din portalul cetateanului precum și cele de la ghiseu. Integrarea aplicației de cadastru cu alte sisteme: Modulul de Cadastru trebuie să fie dezvoltat folosind API-uri de integrare cu Platforma Software pentru cetățeni, cu aplicația de Registru Agricol, Impozite și taxe, Registratura și Document Management, Mijloace fixe/Patrimoniu în vederea comunicării datelor între acestea în timp real între acestea. Comunicarea prin API-uri trebuie să fie realizată securizat folosind key de securitate. - Registrul agricol: - o Corelarea și sincronizarea datelor pentru o gestionare unitară a informațiilor despre terenuri. - o Posibilitatea de a vizualiza informații despre gospodărie în vederea identificării și corelării terenurilor neidentificate. - Registratură și document management: - o Eficientizarea fluxului de documente și a corespondenței oficiale. - o Preluarea automată a numerelor de registratura din registrul general sau cele speciale unde este cazul. - o Înregistrarea formularelor provenite prin platforma cetateanului sau la ghiseul de cadastru direct în document management pe compartimentul specific care se ocupă de tipul de formular înregistrat. - Mijloace fixe / patrimoniu: - o Administrarea și monitorizarea bunurilor și patrimoniului local. - Impozite și taxe: - o Actualizarea automată a datelor fiscale și facilitarea calculului impozitelor și taxelor. - o Posibilitatea de vizualizare a fișei rolului pentru un anumit CNP/CUI în vederea identificării și corelării terenurilor. - Portal cetățean: - o Afișarea hărților tematice către cetățeni; - o Depunerea formularelor online. Caracteristici generale ale aplicației: <i>Păstrarea istoricului informațiilor:</i> - Aplicația va menține istoricul complet al datelor, permițând studiul facil al situațiilor anterioare referitoare la imobile. - Acces ușor la modificările efectuate și la evoluția imobilelor în timp. <i>Interfață grafică de lucru:</i> - O platformă intuitivă și user-friendly pentru interacțiunea cu baza de date geospațială de cadastru. - Suport pentru operațiuni GIS avansate, în funcție de drepturile utilizatorului.
--	---

- Platforma sa ofere posibilitatea de a fi accesata de oriunde, necesar fiind doar un acces la internet.

Acces prin aplicații GIS:

- Baza de date de cadastru va putea fi accesată folosind aplicații GIS.
- În funcție de drepturile utilizatorilor, se vor permite operațiuni de creare, citire, actualizare sau ștergere asupra obiectelor spațiale din baza de date.

Funcționalități detaliate ale Modulului de Cadastru:

Importul datelor din lucrările de cadastru sistematic:

- Facilitarea importului datelor generate în timpul lucrărilor de cadastru sistematic prin intermediul fișierelor de tip .cgxml.
- Datele sunt furnizate de persoana autorizată de ANCPI/OCPI care a executat lucrarea.
- Importul sa poata fi realizat dintr-o interfață a aplicației prin încărcarea fișierelor cu extensia .cgxml sau a unei arhive care conține fișierele.

Vizualizarea datelor importate:

- Datele importate pot fi vizualizate în:
 - Cadrul componentei hartă a aplicației prin autentificarea în modulul dedicat funcționarului.
 - Portalul cetățeanului prin hărțile tematice și publice puse la dispoziție de către instituție.
- Vizualizarea datelor atribut ale imobilelor importate.

Compararea datelor:

- Compararea prin suprapunere grafică a straturilor cu situația actuală din eTerra și lucrarea de cadastru sistematic.
- Compararea prin suprapunere grafică a straturilor cu blocurile fizice APIA și lucrarea de cadastru sistematic.

Interacțiunea cu cetățenii:

- Publicarea cu acces pentru cetățeni în modul de vizualizare în faza de consultare publică a lucrărilor de cadastru sistematic.
- Oferirea posibilității cetățenilor de a înregistra online contestații în perioada de consultare a populației.
- Oferirea posibilității cetățenilor de a încărca în platformă documente digitale referitoare la lucrările de cadastru sistematic.
- Documentele și cererile înregistrate trebuie să preia număr de registratura prin integrarea cu sistemul de Document management și Registratura folosind API-uri;
- Documentele depuse trebuie să ajungă în sistemul de Document management la compartimentul de specialitate.
- Cetățeanul trebuie să aibă posibilitate din platforma să comunice cu funcționarul primăriei prin intermediul unui sistem de mesaje oferit de platforma.
- Cetățeanul trebuie să poată fi notificat și pe email sau sms atunci când funcționarul îi scrie un mesaj.
- În portalul cetățeanului trebuie să poată fi definite diferite hărți tematice legate de modulul de cadastru.
- Aceste hărți tematice din modulul de cadastru sunt afișate în timp real, adică dacă se modifică anumite atribute sau date în harta din modulul de cadastru, aceste modificări se reflectă automat și în portalul cetățeanului fără să mai fie o intervenție suplimentară în portalul cetățeanului.

Corelarea cu registrul agricol:

- Folosind componenta de corelare autonomă și/sau interactivă a datelor din cadastru și registrul agricol, se va realiza relaționarea dintre terenurile cu sau fără clădiri din modulul de cadastru cu terenurile din registrul agricol.

Componenta de corelare autonomă și/sau interactivă a datelor din cadastru și registrul agricol:

Selectarea cheilor unice de legătură:

- Permite selectarea cheilor unice de legătură dintre datele existente în aplicația de cadastru și registrul agricol pentru a realiza relaționarea dintre cele două aplicații.

	<i>Selecție grafică pe hartă:</i> - Posibilitatea de a selecta grafic, pe hartă, geometriile terenurilor din aplicația de cadastru care trebuie asociate terenurilor din registrul agricol. <i>Selecție din date tabelare:</i> - Posibilitatea de a selecta din date afișate în format tabelar imobilele care relaționează între cele două aplicații. Componenta de publicitate a aplicației de cadastru: Înștiințarea deținătorilor de imobile: Va permite înștiințarea deținătorilor imobilelor cu privire la obligațiile acestora: - De a permite accesul specialiștilor să execute măsurătorile. - De a prezenta actele juridice referitoare la imobile. - De a identifica limitele imobilelor împreună cu echipele care realizează lucrările de specialitate. - De a verifica informațiile privitoare la imobilele pe care le dețin, în etapa de publicare a documentelor tehnice cadastrale (conform Art. 12 alin. 3 din Legea 7/1996 republicată). Gestionarea termenelor și avertizărilor: Se vor putea înregistra termene privitoare la imobile și genera avertizări specifice, cum ar fi: - Împlinirea termenelor de posesie. - Împlinirea termenelor de afișare a ofertelor de vânzare. Gestionarea ofertelor de vânzare: - Va permite înregistrarea ofertelor de vânzare ale imobilelor din extravilanul UAT pentru imobilele prevăzute de Legea 17/2014. - Va permite publicarea ofertelor de vânzare ale imobilelor din extravilanul UAT, conform legislației în vigoare. Componenta de import/export a aplicației de cadastru: Importul datelor: - Importul datelor din formatele: .cgxml, .gpkg, .shp, .dxf, .csv. - Importul datelor se va face în straturi dedicate acestei acțiuni, fără a afecta direct baza de date existentă. Exportul datelor: - Exportul datelor în formatele: .gpkg, .shp, .dxf, .csv. Generator de rapoarte și documente specifice: Generarea documentelor specifice departamentului de cadastru: - Aplicația va permite generarea documentelor specifice departamentului de cadastru. - Folosind șabloane prestabilite conform formularelor instituției și datele actuale ale aplicației de cadastru, se vor genera documente precum: - Adeverințe. - Adrese. - Corespondență. - Comunicări. - Adeverințe APIA. - Alte documente specifice activităților departamentului de cadastru din cadrul primăriei.
--	---

Echipamentele hardware necesare vor fi:

DESCRIERE	Cantitate
Server App Tehnologie: Tip: CISC 64 biți tip Intel Xeon minim generația a cincea sau echivalent; • Nuclee: minim 16 nuclee fizice per procesor; • Frecvența de bază: minim 3.6 GHz; • Cache: minim 45 MB Cache L3 sau echivalent; • Magistrală: 3 x UPI 20 GT/s sau echivalent; • Putere consumată: maxim 270W per procesor; • Număr de procesoare instalate: minim 2	1
Server Backup Tehnologie: Tip: CISC 64 biți tip Intel Xeon generația a patra sau echivalent; Nuclee: minim 12 nuclee fizice per procesor; Frecvența de bază: minim 2 GHz; Cache: minim 30 MB Cache L3 sau echivalent; Putere consumată: maxim 150 W per procesor; Număr de procesoare instalate: minim 1 Serverul va fi echipat cu: cel puțin 2 HDD min 600GB SAS, hot-plug / hot-swap, configurate în RAID 1; cel puțin 4 HDD min. 4TB SAS, hot-plug, configurate în RAID 5	1
UPS 3000VA rackabil 2U Online dubla conversie management 1 schuko + 4 IEC TED Electric TED004062 Sursa neîntreruptibilă – UPS Form factor: Rackabil, 2U, sistem de prindere rack inclus Putere: 3000VA / 2700W Tehnologie: Online dubla conversie Tip baterii: 6 baterii 12V 9Ah Timp de încărcare baterii: 3 ore Functii: protecție supratensiune, protecție suprasarcină, protecție supraincercare, protecție scurt-circuit Modul de management de la distanță inclus	1
Rack Dulap cablare structurată - Rack Dimensiuni: 42U, Înălțime: 2010mm, Latime: 800mm, Adâncime: 1000mm Grad de protecție: IP20 Încărcare maximă: 800kg	1
Laptop DELL sau similar	8
All-in-one DELL sau similar	7
Imprimantă laser Konika Minolta sau similar	5
Multifuncțională Kyocera sau similar	2
Multifuncțională / Plotter A0	1
Kiosk interactiv în interacțiunea cu cetățeanul	1
Drona	1
Tabla sală consiliu Samsung 85"	1
Licențe Autocad permanente	2

Tableta Huawei Matepad Paper / Lenovo Tab P12 Paper (conversie scris de mana in text nice to have)	20
Solutie IoT	1

Specificațiile tehnice minimale ale acestora sunt:

SERVER APP -1 buc:

Componenta	Cerințe tehnice minimale
Procesor	Tehnologie: • Tip: CISC 64 biți tip Intel Xeon minim generația a cincea sau echivalent; • Nuclee: minim 16 nuclee fizice per procesor; • Frecvența de bază: minim 3.6 GHz; • Cache: minim 45 MB Cache L3 sau echivalent; • Magistrală: 3 x UPI 20 GT/s sau echivalent; • Putere consumată: maxim 270W per procesor; • Număr de procesoare instalate: minim 2;
Memorie RAM	Cel puțin 128 GB DDR5 ECC 5600 MT/s, suport pentru tehnologii de protecție de tip Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection sau echivalent; Minim 16 sloturi de memorie disponibile în șasiu, posibilitate de instalare 8 TB de memorie RAM DDR5 RDIMM.
Capacitate de stocare internă	Server cu cel puțin 10 sloturi, hot-plug / hot-swap, de tip 2.5” instalate și disponibile în șasiu pentru instalarea modulelor de stocare SAS, SATA; Serverul va fi echipat cu cel puțin 2 module 3.84 GB SSD, 1DWPD, hot-plug / hot-swap, configurate în RAID 1;
Controller RAID intern	Controller RAID PCIe cu suport pentru 8 module SSD 2.5” hot-swap, suport pentru RAID 0, 10, 1, 5, 50, 6, 60; Memorie cache nevolatilă instalată la nivelul controller-ului de min 8 GB de tip DDR4 2666 MT/s; Controller-ul RAID trebuie să dispună de mecanisme interne de mărire a capacității online, configurare de disk hot-spare dedicat si global;
Interfață video	Interfață video integrată ce suportă o rezoluție minimă de 1920 x 1200
Interfețe rețea	• 2 porturi 1 Gbps Ethernet RJ-45; • 2 porturi 10/25 Gbps Ethernet instalate pe două interfețe PCIe distincte, echipate cu module optice 25Gbps SFP+ SR sau cabluri twinax;
Sloturi de expansiune	Pentru instalarea modulelor IO, echipamentul va dispune de sloturi PCI Express: • minim 3 sloturi extensie, PCIe x16 (cu 16 lane-uri PCI Express conectate);
Porturi	Minim: 1 x VGA, minim 2 x USB 2.0 (din care 1 frontal) și 1 x USB 3.0;
Management	Sistem încorporat de monitorizare a: procesoarelor, memoriilor, HDD-urilor, interfețelor IO, ventilatoarelor, surselor de alimentare, temperaturii; analize predictive de eroare pentru componentele sistemului cu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componente.
	LCD display sau panou cu LED-uri ce trebuie să permită citirea mesajelor de eroare cu panoul frontal instalat, fără operațiuni suplimentare;
	Aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului, capabilă de instalare locală și de la distanță, în mod neasistat, inclusiv configurare RAID;
	Echipamentul trebuie să fie livrat cu capacități hardware și software, instalate, activate și licențiate pentru următoarele funcționalități:

Componenta	Cerințe tehnice minimale
	• management de la distanță; • redirectare interfață grafică cu tastatură și mouse; • suport pentru virtual clipboard: copiere, taiere, lipire text de pe consola virtuală pe serverul gazdă; • posibilitate de pornire și oprire server de la distanță; • suport pentru remote media (virtual CD si floppy); • suport pentru SSL (Secure Socket Layer); • integrare cu Active Directory / LDAP (Lightweight Directory Access Protocol); • autentificare two-factor; • monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice; • managementul evenimentelor și alarmelor; • inventarul și monitorizarea componentelor (inclusiv GPU, module optice SFP); • instalarea update-urilor și patch-urilor; • analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat; • realizarea de rapoarte de performanță pe baza datelor transmise de senzori (streaming telemetry) care indică utilizarea resurselor sistemului de calcul (procesor, memorie, I/O), consumului de energie electrică, temperatură, independent de sistemul de operare și fără a consuma resurse de procesor din server; • repornirea și reconfigurarea automată a serverului; • permite generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere similare din infrastructură; • permite stocarea pe un NAS extern cu funcționalități de retenție a fișierelor pentru a asigura protecția la ștergere și modificare a fișierelor de update, șabloanelor de configurare și imaginilor de sistem de operare; • permite ștergerea securizată a unităților de stocare de tip SSD și HDD; • validare a configurației serverului față de o referință; • RESTful API cu suport Redfish; • integrare cu Microsoft System Center și cu VMware vCenter; • Interfețe acces utilizator: HTML5 Web GUI, SSH; • Funcționalitățile vor fi asigurate fără a fi necesară instalarea de agenți software. • Port dedicat 1 Gigabit Ethernet RJ-45 ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului;
Aplicație administrare	Trebuie să permită administrare și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți; Pentru a asigura compatibilitatea, aplicația trebuie să fie furnizată de același producător cu cel al server-elor; Trebuie să permită inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, interfețe IO, controllere RAID, unități de stocare; Trebuie să permită update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticității acestora; Trebuie să permită generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură; Trebuie să permită instalarea sistemelor de operare și virtualizare pe serverele aflate în administrare; Permite stocarea pe un storage extern cu funcționalitate de retenție a fișierelor sau server web, pentru a asigura protecția la ștergere și modificare a fișierelor de update, template-urilor de configurare și imaginilor de sistem de operare; Trebuie să ofere funcționalitatea de validare a configurației față de o referință; Monitorizează starea de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică; Permite ștergerea securizată a unităților de stocare de tip SSD si HDD.

Componenta	Cerințe tehnice minimale
	Trebuie să genereze grafice cu nivele de încărcare și utilizare ale serverelor cu un istoric pe o perioadă configurabilă de cel puțin 1 an
Format	Serverul rackabil trebuie să fie montabil în rack-uri standard de 19”. Înălțimea maximă a Serverul rackabil trebuie să fie maxim 1 RU. Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (șine glisante, braț de gestionare a cablurilor, șuruburi/captive). Serverul rackabil trebuie să aibă LED de localizare pentru identificarea poziției în rack. Panou frontal cu mecanism de închidere pentru securizare acces la discuri și LCD sau LED-uri pentru indicarea stării de funcționare a sistemului.
Securitate	Trusted Platform Module 2.0; Posibilitatea de a dezactiva butonul de pornire (<i>power</i>) din BIOS; Capabilități incluse pentru <i>chassis intrusion detection</i> ce utilizează sistemul de management încorporat, monitorizând și detectând: accesul la șasiu, îndepărtarea sau înlocuirea unei componente a serverului; Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate; Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), <i>OS boot loader</i> și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze; Suport hardware inclus pentru verificarea și validarea autenticității <i>firmware</i>-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare); Update-urile de <i>firmware</i> trebuie să fie semnate criptografic de către producătorul echipamentului oferat pentru a fi autentificate la instalare; Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Log-urile acestor informații de audit vor fi securizate și vor putea fi accesate doar din componenta de management a soluției propuse; Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului; Suport inclus pentru utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare și posibilitatea de a utiliza un certificat personalizat pentru semna un Linux OS <i>boot loader</i>; <i>Firmware rollback</i>; Protecție pe perioada transportului la intervenție asupra hardware: suport inclus pentru verificarea securizată a componentelor echipamentului livrat la beneficiar prin care să se asigure că echipamentul este exact cum a plecat de la producător.
Surse alimentare electrica	Serverul trebuie alimentat printr-un sistem de surse de alimentare electrică care trebuie să îndeplinească următoarele cerințe: • număr surse interne instalate: minim 2; • funcționare în regim „N+1”; • surse de tip „hot pluggable”; • clasa de eficiență: 80 PLUS Titanium • putere: minim 650 W per sursă. Ofertantul trebuie să livreze minim 2 cabluri de alimentare electrică de tip C13-C14 pentru conectarea la PDU, de lungime minim 2m.
Sistem de operare licențiat și instalat	Ubuntu
Compatibilitate sistem de operare	Serverul trebuie să fie compatibil cu sistemele de operare: Microsoft Windows Server 2016, 2019, 2022 Hyper-V, Red Hat Enterprise Linux 7,8,9, SUSE Linux Enterprise Server 15, Ubuntu Server LTS 20.04, 22.04, VMware ESXi 7.0, 8.0;
Garanție și suport	Garanția hardware va fi de minim 60 de luni. Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – <i>Next Business Day</i>) care să garanteze diagnosticarea echipamentului sau

Componenta	Cerințe tehnice minimale
	modului defect, înlocuirea acestuia în maxim o zi lucrătoare de la momentul deciziei, fără alte costuri. Pe toată perioada de suport activ al echipamentului oferat, în cazul în care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale pentru beneficiar. Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Discurile defecte nu se vor returna, vor rămâne în posesia beneficiarului. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Va fi asigurat accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software oferate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software oferat). Echipamentele oferate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate moral, ce nu se mai află în linia curentă de fabricație a producătorului). Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului oferat, indiferent de upgrade-urile ulterioare ale acestuia.

SERVER BACKUP -1 buc:

Componenta	Cerințe tehnice minimale
Procesor	Tehnologie: • Tip: CISC 64 biți tip Intel Xeon generația a patra sau echivalent; • Nuclee: minim 12 nuclee fizice per procesor; • Frecvența de bază: minim 2 GHz; • Cache: minim 30 MB Cache L3 sau echivalent; • Putere consumată: maxim 150 W per procesor; • Număr de procesoare instalate: minim 1;
Memorie RAM	Cel puțin 64 GB DDR5 ECC 5600 MT/s, suport pentru tehnologii de protecție de tip Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection sau echivalent; Minim 10 sloturi de memorie disponibile în șasiu, posibilitate de instalare 8 TB de memorie RAM DDR5 RDIMM.
Capacitate de stocare internă	Server cu cel puțin 12 sloturi, hot-plug / hot-swap, de tip 2.5"/3.5" instalate și disponibile în șasiu pentru instalarea modulelor de stocare SAS, SATA; Serverul va fi echipat cu: cel puțin 2 HDD min 600GB SAS, hot-plug / hot-swap, configurate în RAID 1; cel puțin 4 HDD min. 4TB SAS, hot-plug, configurate în RAID 5;
Controller RAID intern	Controller RAID PCIe cu suport pentru 8 module SSD 2.5" hot-swap, suport pentru RAID 0, 10, 1, 5, 50, 6, 60; Memorie cache nevolatilă instalată la nivelul controller-ului de min 8 GB de tip DDR4 2666 MT/s; Controller-ul RAID trebuie să dispună de mecanisme interne de mărire a capacității online, configurare de disk hot-spare dedicat si global;
Interfață video	Interfață video integrată ce suportă o rezoluție minimă de 1920 x 1200
Interfețe rețea	• 2 porturi 1 Gbps Ethernet RJ-45; • 2 porturi 10/25 Gbps Ethernet instalate, echipate cu module optice 25Gbps SFP+ SR sau cabluri TWINAX;
Sloturi de expansiune	Pentru instalarea modulelor IO, echipamentul va dispune de sloturi PCI Express: • minim 3 sloturi extensie PCIe x8;
Porturi	Minim: 2 x VGA (din care 1 frontal), minim 2 x USB 2.0 (din care 1 frontal) și 1 x USB 3.0;
Management	Sistem încorporat de monitorizare a: procesoarelor, memoriilor, HDD-urilor, interfețelor IO, ventilatoarelor, surselor de alimentare, temperaturii; analize predictive de eroare pentru componentele sistemului cu posibilitatea anunțării administratorului de sistem despre

	iminenta defectare a uneia dintre componente. LCD display sau panou cu LED-uri ce trebuie să permită citirea mesajelor de eroare cu panoul frontal instalat, fără operațiuni suplimentare; Aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului, capabilă de instalare locală și de la distanță, în mod neasistat, inclusiv configurare RAID;
	Echipamentul trebuie să fie livrat cu capabilități hardware și software, instalate, activate și licențiate pentru următoarele funcționalități: • management de la distanță; • redirectare interfață grafică cu tastatură și mouse; • suport pentru <i>virtual clipboard</i>: copiere, taiere, lipire text de pe consola virtuală pe serverul gazdă; • posibilitate de pornire și oprire server de la distanță; • suport pentru <i>remote media</i> (virtual CD și floppy); • suport pentru SSL (Secure Socket Layer); • integrare cu Active Directory / LDAP (Lightweight Directory Access Protocol); • autentificare <i>two-factor</i>; • monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice; • managementul evenimentelor și alarmelor; • inventarul și monitorizarea componentelor (inclusiv GPU, module optice SFP); • instalarea <i>update</i>-urilor și <i>patch</i>-urilor; • analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat; • realizarea de rapoarte de performanță pe baza datelor transmise de senzori (<i>streaming telemetry</i>) care indică utilizarea resurselor sistemului de calcul (procesor, memorie, I/O), consumului de energie electrică, temperatură, independent de sistemul de operare și fără a consuma resurse de procesor din server; • repornirea și reconfigurarea automată a serverului; • permite generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere similare din infrastructură; • permite stocarea pe un NAS extern cu funcționalități de retenție a fișierelor pentru a asigura protecția la ștergere și modificare a fișierelor de update, șabloanelor de configurare și imaginilor de sistem de operare; • permite ștergerea securizată a unităților de stocare de tip SSD și HDD; • validare a configurației serverului față de o referință; • RESTful API cu suport Redfish; • integrare cu Microsoft System Center și cu VMware vCenter; • Interfețe acces utilizator: HTML5 Web GUI, SSH; • Funcționalitățile vor fi asigurate fără a fi necesară instalarea de agenți software. • Port dedicat 1 Gigabit Ethernet RJ-45 ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului;
Aplicație administrare	Trebuie să permită administrare și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți; Pentru a asigura compatibilitatea, aplicația trebuie să fie furnizată de același producător cu cel al server-elor; Trebuie să permită inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, interfețe IO, controllere RAID, unități de stocare; Trebuie să permită update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticității acestora; Trebuie să permită generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură; Trebuie să permită instalarea sistemelor de operare și virtualizare pe serverele aflate în

	administrare; Permite stocarea pe un storage extern cu funcționalitate de retenție a fișierelor sau server web, pentru a asigura protecția la ștergere și modificare a fișierelor de update, template-urilor de configurare și imaginilor de sistem de operare; Trebuie să ofere funcționalitatea de validare a configurației față de o referință; Monitorizează starea de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică; Permite ștergerea securizată a unităților de stocare de tip SSD si HDD. Trebuie să genereze grafice cu nivele de încărcare și utilizare ale serverelor cu un istoric pe o perioada configurabilă de cel puțin 1 an
Format	Serverul rackabil trebuie să fie montabil în rack-uri standard de 19”. Înălțimea maximă a Serverul rackabil trebuie să fie maxim 2 RU. Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (șine glisante, braț de gestionare a cablurilor, șuruburi/captive). Serverul rackabil trebuie să aibă LED de localizare pentru identificarea poziției în rack. Panou frontal cu mecanism de închidere pentru securizare acces la discuri și LCD sau LED-uri pentru indicarea stării de funcționare a sistemului.
Securitate	Trusted Platform Module 2.0; Posibilitatea de a dezactiva butonul de pornire (<i>power</i>) din BIOS; Capabilități incluse pentru <i>chassis intrusion detection</i> ce utilizează sistemul de management încorporat, monitorizând și detectând: accesul la șasiu, îndepărtarea sau înlocuirea unei componente a serverului; Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate; Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), <i>OS boot loader</i> și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze; Suport hardware inclus pentru verificarea și validarea autenticității <i>firmware</i>-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare); Update-urile de <i>firmware</i> trebuie să fie semnate criptografic de către producătorul echipamentului oferat pentru a fi autentificate la instalare; Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Log-urile acestor informații de audit vor fi securizate și vor putea fi accesate doar din componenta de management a soluției propuse; Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului; Suport inclus pentru utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare și posibilitatea de a utiliza un certificat personalizat pentru semna un Linux OS <i>boot loader</i>; <i>Firmware rollback</i>; Protecție pe perioada transportului la intervenție asupra hardware: suport inclus pentru verificarea securizată a componentelor echipamentului livrat la beneficiar prin care să se asigure că echipamentul este exact cum a plecat de la producător.
Surse alimentare electrica	Serverul trebuie alimentat printr-un sistem de surse de alimentare electrică care trebuie să îndeplinească următoarele cerințe: • număr surse interne instalate: minim 2; • funcționare în regim „N+1”; • surse de tip „hot pluggable”; • clasa de eficiență: 80 PLUS Titanium • putere: minim 1100 W per sursă. Ofertantul trebuie să livreze minim 2 cabluri de alimentare electrică de tip C13-C14 pentru conectarea la PDU, de lungime minim 2m.
Solutie software	Soluția trebuie să fie flexibilă și scalabilă și să permită instalarea pe două și trei nivele de

backup instalata	arhitectură; prin nivele de arhitectură se înțelege nivelul agent de backup, nivelul server de management și nivelul de server media de realizare și stocare a backup-urilor. Soluția trebuie să permită administrarea din interfața GUI, CLI și RestfulAPI; Soluția trebuie să poată funcționa independent de o anumită tehnologie hardware. Soluția trebuie să poată fi instalată pe medii fizice, virtuale cât și pe medii cloud. Soluția trebuie să permită instalarea cel puțin pe următoarele sisteme de operare: Windows, Linux și Solaris. Soluția trebuie să suporte integrarea cu discuri DAS, NAS, SAN pentru stocarea fișierelor de backup. Soluția trebuie să suporte integrarea cu celelalte echipamente de stocare propuse în cadrul acestui proiect, precum și cu cele existente în infrastructura beneficiarului, în mod nativ sau prin protocolul OST (OpenStorage). Soluția trebuie să identifice segmentele de date unice la nivelul agenților de backup, pentru optimizarea traficului prin rețea. Soluția trebuie să suporte transferul datelor prin LAN și SAN. Soluția trebuie să permită reluarea unui backup nefinalizat cu succes de la ultimul checkpoint. Soluția trebuie să permită reluarea unei restaurări nefinalizate de la ultimul checkpoint. Soluția trebuie să ofere capacități pentru efectuarea de backup-uri sintetice. Soluția trebuie să automatizeze crearea de multiple copii ale backup-urilor pe diferite medii de stocare cu politici diferite de retenție. Soluția trebuie să permită crearea de backup-uri prin politici sau manual. Soluția trebuie să asigure asistență pentru operațiile importante: instalare, creare activități de salvare / restaurare, formatare medii de stocare, etc. Soluția trebuie să ofere posibilitatea de a efectua Bare Metal Restore (funcționalități de restaurare complet automatizate care includ sistemul de operare, configurația, aplicațiile și datele) pentru Windows și Linux (RHEL, SUSE) fără a necesita integrarea cu soluții terțe, instrumente native ale sistemului de operare sau instrumente pentru crearea de imagini. Soluția trebuie să ofere toate tipurile de backup: full, incremental și diferențial. Soluția trebuie să permită integrarea cu sisteme de tip LDAP pentru autentificarea utilizatorilor. Soluția trebuie să asigure suport pentru protecția containerelor Docker. Soluția trebuie să asigure suport pentru protecția aplicațiilor care rulează în containere Docker pe volume de date persistente. Soluția trebuie să asigure suport pentru Kubernetes. Soluția trebuie să asigure suport pentru multiplexing și multistreaming. Soluția trebuie să asigure agenți dedicați pentru protecția sistemelor de baze de date oferite; Soluția trebuie să asigure protecție pentru următoarele sisteme de operare: Windows, RHEL, SUSE Linux Enterprise Server, CentOS, Ubuntu; Soluția de backup trebuie să asigure suport pentru efectuarea de snapshot-uri la nivel destorage. Soluția trebuie să suporte utilizarea protocolului Network Data Management Protocol (NDMP) pentru a iniția și controla salvarea/restaurarea sistemelor Network Attached Storage (NAS). Soluția trebuie să suporte NDMP v2, v3 și v4. Soluția trebuie să suporte salvări NDMP local și 3-way, funcționalitatea Direct Access Recovery (DAR). Soluția trebuie să permită actualizarea automată a tuturor clienților. Soluția trebuie să asigure posibilitatea de a salva mediile virtuale Open Stack. Soluția să asigure un modul de monitorizare și administrare centralizat. Acesta trebuie să asigure funcționalități de alertare și raportare pentru soluția propusă. Rapoartele și alertele trebuie să fie predefinite, dar să existe și posibilitatea de a crea rapoarte noi, prin utilizarea interfeței vizuale de tip point and click, sau drag and drop, dar și prin executia de fraze SQL custom peste baza de date de tip repository sau catalog a soluției de backup. Soluția nu trebuie să necesite instalarea niciunui agent (permanent sau temporar) pentru salvarea mașinilor virtuale. Soluția trebuie să permită salvarea completă și restaurarea granulară pentru Active Directory
------------------	---

	fără a fi necesară integrarea cu mecanismele native de backup ale acestor aplicații. Soluția trebuie să permită backup de tipul “Incremental Forever”, astfel încât să salveze doar blocurile modificate. Aceste blocuri să poată fi ulterior combinate cu backup-ul anterior pentru a sintetiza un nou full backup, pentru o restaurare mult mai rapidă. Procesul de deduplicare a datelor să poată fi efectuat inline sau post proces de backup. Procesul de deduplicare trebuie să folosească segmente de dimensiuni variabile, pentru eficientizarea factorului de deduplicare. Pentru a facilita protecția sistemelor pentru care nu există agenți dedicați, să permită crearea de mount point-uri de tip NFS și CIFS direct din sistemul de deduplicare al datelor, iar datele salvate în mount point-uri să fie deduplicate și protejate în sistemul de deduplicare. Soluția trebuie să asigure suport pentru aplicarea procesului de deduplicare atât la sursa datelor de protejat cât și la nivelul sistemului de stocare al backup-urilor. Soluția trebuie să asigure suport pentru deduplicare globală. Soluția trebuie să asigure replicare de tip „one-to-one”, „one-to-many”, „many-to-one” și topologii de replicare cascadată a datelor deduplicate. Soluția trebuie să asigure criptarea datelor replicate, în vederea securizării acestora pe perioada transferului între locații. Soluția trebuie să permită prevenirea accesului neautorizat la aplicația de backup prin mecanisme de control acces bazate pe roluri. Soluția trebuie să asigure suport pentru criptarea datelor, atât cele aflate în tranzit, cât și celor salvate. Soluția trebuie să includă propriile mecanisme pentru administrarea cheilor de criptare. Soluția trebuie să asigure suport pentru autentificare în interfața Web de administrare folosind mecanisme 2 Factor Authentication. Soluția trebuie să asigure mecanisme de protecție împotriva Ransomware, la nivel de client și la nivelul stocării backup-urilor, pentru a determina dacă nu cumva datele au fost deja afectate de ransomware. Acest mecanism trebuie să funcționeze în momentul rulării backup-ului, în momentul salvării pe disc și imediat înainte de orice tentativă de restaurare. Soluția trebuie să permită instalarea unui număr nelimitat de clienți de backup indiferent de tipul acestora. Soluția trebuie licențiată pentru întreaga capacitate protejată, minim 4TB și nu trebuie să aibă limitări în funcție de numărul de procesoare, sau de numărul de mașini fizice sau virtuale protejate. Soluția nu trebuie să fie limitată de politica de retenție aleasă și nici de capacitatea ocupată de backup-uri, indiferent unde sunt acestea pastrate (disk, tape, sau cloud). Suport pentru software pe o perioadă de 60 luni, acoperind dreptul beneficiarului de a face update-uri și upgrade-uri, precum și acces direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.
Sistem de operare	Serverul trebuie să fie compatibil cu sistemele de operare: Microsoft Windows Server 2016, 2019, 2022 Hyper-V, Red Hat Enterprise Linux 7,8,9, SUSE Linux Enterprise Server 15, Ubuntu Server LTS 20.04, 22.04, VMware ESXi 7.0, 8.0;
Garanție și suport	Garanția hardware va fi de minim 60 de luni. Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – <i>Next Business Day</i>) care să garanteze diagnosticarea echipamentului sau modulului defect, înlocuirea acestuia în maxim o zi lucrătoare de la momentul deciziei, fără alte costuri. Pe toată perioada de suport activ al echipamentului oferit, în cazul în care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale pentru beneficiar. Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Discurile defecte nu se vor returna, vor rămâne în posesia beneficiarului. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Va fi asigurat accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software oferite (firmware, drivere componente, pachete software de la

	producător incluse în echipamentul software oferat). Echipamentele oferate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate moral, ce nu se mai află în linia curentă de fabricație a producătorului).
--	--

UPS -1 buc:

A0114968	Online	UPS 3000VA rackabil 2U Online dubla conversie management 1 schuko + 4 IEC TED Electric TED004062
A0115817	Modul	Modul SNMP-NANO pentru UPS-urile online TED 1-100KVA New

Descriere tehnica

Sursa neintreruptibila – UPS

Form factor: Rackabil, 2U, sistem de prindere rack inclus

Putere: 3000VA / 2700W

Tehnologie: Online dubla conversie

Tip baterii: 6 baterii 12V 9Ah

Timp de incarcare baterii: 3 ore

Functii: protectie supratensiune, protectie suprasarcina, protectie supraincarcare, protectie scurt-circuit

Modul de management de la distanta inclus

Termen de garantie: 12 luni

RACK -1 buc:

DESCRIPTION
Dulap cablare structurată DT, 42U H2010 x W800 x D1000, 19"
Set role (2 cu frână, 2 fără) pentru dulapuri DT
Unitate de tavan cu 4 ventilatoare, DT, termostat analogic
PDU 19", 8xSchuko, profil PVC 1,25U, cablu conex.2m, RAL7035

Descriere tehnica

Dulap cablare structurată - Rack

Dimensiuni: 42U, Inaltime: 2010mm, Latime: 800mm, Adancime: 1000mm

Grad de protectie: IP20

Incarcare maxima: 800kg

Termen de garantie: 12 luni

Accesorii Dulap cablare structurată – Rack

Set role - 2 role cu frană, 2 role fara) pentru dulap cablare structurata, incarcare maxima 600kg

Unitate de tavan cu 4 ventilatoare, termostat analogic

Dimensiuni: Inaltime: 50mm, Latime: 390mm, Adancime: 390mm

Bara de alimentare echipamente - PDU 19"

Dimensiuni: Inaltime: 57,50mm, Latime: 483mm, Adancime: 50mm

Module de alimentare: 8 x Priza tip Schuko, cablu alimentare in lungime de 2m

LAPTOP -8 buc:

Display

Diagonala	15.6 inch
Rezolutie	1920 x 1080
Format	Full HD
Suprafata	Anti-Glare
Tehnologie ecran	IPS
Rata Refresh	60 Hz
Luminozitate	250 nt
NTSC Gamut	45%
Procesor	
Nume	Intel® Core™ i7
Familie	Intel® Core™ i7 din a treisprezecea generatie Raptor Lake
Tip	i7
Numar nuclee	10
Numar thread-uri	12
Frecventa turbo max	5 GHz
Smart Cache	12 MB
Tehnologie	10 nm
Procesor grafic integrat	Intel® Iris™ Xe Graphics
Altele	10 cores: 2 P-cores and 8 E-cores
Memorie	
Capacitate	16 GB
Tip memorie	DDR4
Suport maxim	64 GB
Stocare	
Solid State Disk	Da
Capacitate SSD	512 GB
Tip SSD	M.2 PCIe

ALL IN ONE -7 buc:

Display	
Diagonala	27 inch
Touchscreen	Da
Widescreen	Da
Format	FHD
Ecran	LED Backlit
Suprafata ecran	Anti-Glare
Rezolutie	1920 x 1080 pixeli
Culori	16.7 milioane

Unghi de vizualizare	178/178 grade
Webcam integrat	Da
Microfon integrat	Da
Senzor webcam	2.0 mpx
Rezolutie webcam	1920 x 1080 pixeli
All-in-One	Da
Procesor	
Producator	Intel
Socket	1744
Nucleu	Raptor Lake
Familia	Core 7 Series 1
Tehnologie de fabricatie	Intel 7 nm
Max TDP	55 W
Grafica integrata	Intel Graphics
Memorie RAM	
Capacitate RAM	32 GB
Tip	DDR4
Frecventa	3200 MHz
Sloturi memorie	2
Tip sloturi memorie	SODIMM
Slot 1	16 GB
Slot 2	16 GB
Memorie maxima	32 GB
Stocare	
Tip stocare	SSD
Capacitate SSD	1 TB
Detalii	M.2 PCIe 4.0 NVMe SSD
Placa Video	
Tip	Dedicata
Software	
Sistem de operare	Windows 11 Pro
Diverse	
Periferice	Tastatura + Mouse
Altele	Cablu alimentare
Unitate Optica	
Altele	No Optical Drive
Placa De Baza	
Chipset	Intel
Sloturi	1x M.2

IMPRIMANTA LASER A4 -5 buc:

Tehnologie printare	Laser
Mod printare	Monocrom
Utilizare	Home & office
Functii principale	Printare Scanare Copiere
Format general imprimanta	A4
Printare fata/verso (Duplex)	Automat
Alimentator automat de documente (ADF)	Da
Scanare fata/verso automat (Duplex)	DADF (single-pass)
Functii speciale	Copiere fata-verso automat
Conectivitate	USB Retea
Continut pachet	Cablu alimentare 1 x Toner 1 x Imprimanta multifunctionala
Cablu USB inclus	Nu
Consumabil pachet	Starter
Tip display	LCD LED
Ciclu de lucru maxim (pagini/luna)	80000
Volum recomandat de printare (pagini/luna)	2000
Culoare	Alb Negru
Specificatii consumabile	
Tip consumabil	Toner
Consumabile compatibile	TK-1270 Toner Kit 10000 pagini
PN consumabil	TK-1270
Imprimanta	
Viteza de printare monocrom	40 ppm
Rezolutie printare (DPI)	1200 x 1200
Scanner	
Format scanner	A4
Rezolutie optica (ADF-DPI)	600 x 600
Functii scanner	Scan to PC Scanare catre E-mail Scanare catre FTP TWAIN Scan to USB Host WIA scan
Viteza de scanare (ADF)	40 ipm
Copiator	
Viteza de copiere monocrom	40 ppm
Rezolutie copiere (DPI)	600 x 600
Parametrii zoom	25 - 400%
Manevrare hartie	
Capacitate hartie intrare (coli)	350

Capacitate hartie iesire (coli)	150
Capacitate alimentare automata documente (ADF)	50
Numar tavi hartie	2
Greutate hartie	60-220 g/mp
Specificatii tehnice	
Frecventa procesor	1 GHz
Capacitate memorie	1 GB
Putere consumata	574 W
Nivel zgomot	52 dB
Interfata	USB 2.0 Hi-Speed 1000BaseT/100Base-TX/10Base-T USB Host
Format fisier	JPEG TIFF Open XPS Encrypted PDF High compression PDF PDF/A-1 PDF/A-2
Timp de incalzire	19 s
Timp de raspuns printare	6.4 s
Sistem de operare compatibil	Windows 10 Mac OS X 10.9 - 10.11 Chrome OS Windows 11 64-bit

IMPRIMANTA A3 -2 buc:

Tehnologie printare	Laser
Mod printare	Monocrom Color
Utilizare	Home & office
Functii principale	Printare Scanare Copiere
Format general imprimanta	A3
Printare fata/verso (Duplex)	Automat
Alimentator automat de documente (ADF)	Da
Conectivitate	USB Ethernet Retea
Continut pachet	1 x Imprimanta 1 x Cablu de alimentare 1 x Alimentator automat reversibil de documente DF-633 Tonere TN-227 CMYK
Tip display	LCD LED
Dimensiune display	7 inch
Ciclu de lucru maxim (pagini/luna)	125000
Volum recomandat de printare (pagini/luna)	10000
Aplicatii printare cloud & mobile	Mopria AirPrint Konica Minolta Print Service (Android) Konica Minolta Mobile Print (iOS/Android) optional: WiFi Direct
Culoare	Negru
Specificatii consumabile	
Tip consumabil	Toner
Imprimanta	
Viteza de printare monocrom	25 ppm

Viteza de printare color	25 ppm
Rezolutie printare (DPI)	1800 x 600
Scanner	
Format scanner	A3
Rezolutie scanare (DPI)	600 x 600
Copiator	
Rezolutie copiere (DPI)	600 x 600
Parametrii zoom	25 - 400%
Manevrare hartie	
Capacitate hartie intrare (coli)	1100
Capacitate hartie iesire (coli)	250
Numar tavi hartie	2
Greutate hartie	60 - 256 g/mp
Specificatii tehnice	
Capacitate memorie	6.144 MB
Capacitate stocare	256 GB
Interfata	USB 2.0 Wi-Fi 802.11 b/g/n/ac (optional) 1 x 10/100/1000-Base-T Ethernet
Timp de incalzire	20 s
Timp de raspuns printare	8.4 s 6.8 s
Sistem de operare compatibil	Windows 7 (32/64); Windows 8.1 (32/64); Windows 10 (32/64); Windows Server 2008 (32/64); Windows Server 2008 R2; Windows Server 2012; Windows Server 2012 R2; Windows Server 2016; Windows Server 2019; Macintosh OS X 10.10 or later; Linux

PLOTTER A0 -1 buc:

Tehnologie printare	Inkjet
Mod printare	Color
Functii principale	Printare
Format general imprimanta	A0
Numar duze printare	15360
Printare fata/verso (Duplex)	Manual
Consumabil pachet	Starter
Sistem de operare compatibil	Microsoft Windows 11
Dimensiune display	4.3 inch
Scanner	
Rezolutie scanare (DPI)	600 x 600
Caracteristici tehnice	
Capacitate memorie	2 GB
Imprimanta	
Rezolutie printare (DPI)	2400 x 1200

Manevrare hartie	
Formate hartie compatibile	A0
Capacitate maxima hartie	1

KIOSK INTERACTIV IN INTERACTIUNEA CU CETATEANUL -1 buc:

Tip produs	Sistem de prezentare
Tip montare	De sine statator
Utilizare	Interior
Tensiune alimentare	220 V
Material	Metal
Functii	Conectare USB

DRONA -1 buc:

Caracteristici generale	
Manevrabilitate	Aer
Tip alimentare	Acumulator
Asamblare	Asamblat
Sistem de operare	Android iOS
Conectivitate	Bluetooth USB Wi-Fi GPS
Senzori	Accelerometru Altitudine Senzor evitare obstacole Infrarosu Senzor gravitate
Caracteristici tehnice	
Tip GPS	GPS/GLONASS
Autonomie acumulator	34 min
Performante drona	
Distanta maxima de operare	18 km
Autonomie timp de zbor	34 min
Altitudine maxima	4000 m
Viteza maxima	16 m/s
Viteza maxima de ascensiune	5 m/s
Viteza maxima de coborare	5 m/s
Acuratete de planare	Vertical: ± 0.1 m (with Vision Positioning), ± 0.5 m (with GPS Positioning) Horizontal: ± 0.3 m (with Vision Positioning), ± 0.5 m (with GPS Positioning)
Unghi maxim de inclinare	40 °
Temperatura de operare	-10 - 40 °C

TABLA INTERACTIVA -1 buc:

Caracteristici generale	
Gama	SMART
Putere consumata	528 W
Greutate	75.2 Kg
Lungime	1945.8 mm
Latime	89 mm

Inaltime	1151.1 mm
Culoare	Alb Negru
Afisare	
Diagonala	85 inch
Tehnologie display	VA
Tip rezolutie	4K
Rezolutie optima	3840 x 2160
Aspect imagine	16:09
Format ecran	Wide
Luminozitate	350 cd/m ²
Timp de raspuns	8 ms
Unghi maxim vizibilitate orizontala/verticala	178 / 178
Contrast tipic	4000:01:00
Rata de refresh (maximala)	60 Hz
Conectivitate	
Porturi video	2 x HDMI 2.0 1 x DisplayPort 1.2
Porturi audio	1 x Mini Jack
Data ports	1 x RS232 1 x USB-C 1 x RJ-45 3 x USB-A
Facilitati	
Functii speciale	Touchscreen
Montare pe perete	VESA 400 x 400 mm
Continut pachet	1 x Display interactiv

LICENTE AUTOCAD -2 buc:

Caracteristici generale	
Tip aplicatie	AutoCAD
Varianta de comercializare	Licenta electronica
Utilizare	PC MAC
Versiune	Office Professional Plus
An	2025
Limba	Toate limbile
Numar dispozitive	1
Numar utilizatori	1
Valabilitate	3 ani

TABLETA -20 buc:

Conectivitate	Fara SIM
Sistem de operare	Android
Versiune sistem operare	MediaTek SoC Platform

Tehnologie	Bluetooth GPS GNSS
Continut pachet	1 x Cablu Incarcare 1 x Tableta 1 x Lenovo Tab Pen Plus
Culoare	Gri
Inaltime	6.9 mm
Latime	293.37 mm
Grosime	190.76 mm
Greutate	615 g
Material	Aluminiu
Producator procesor	MediaTek
Model procesor	MediaTek Dimensity 7050
Numar nuclee	8
Frecventa	2.6 GHz
Tehnologie procesor	6 nm
Producator chipset video	ARM
Afisare	
Tehnologie display	IPS
Diagonala display	12.7 inch
Rezolutie	2944 x 1840
Memorie	
Tip memorie	LPDDR4
Capacitate memorie	8 GB
Stocare	
Capacitate stocare	256 GB
Tip slot memorie	Card microSD, suporta pana la 1TB (exFAT)
Capacitate maxima card de memorie	1 TB
Conectivitate	
Versiune Bluetooth	Bluetooth 5.1
Wireless	Wi-Fi® 6, 802.11ax 2x2 + BT5.1
Porturi	USB Type-C
Acumulator	
Capacitate acumulator	10200 mAh
Multimedia	
Rezolutie camera principala	8 Mpx
Rezolutie camera frontala	13 Mpx
Redare audio	Dolby Atmos

SOLUTIE IoT -1 buc:

1. Specificații Solutie IoT

- *Indice de Protecție la Intrare:* IP65
- *Dimensiuni:*
- *Lungime netă:* 82,50 mm

- *Lățime netă:* 82,50 mm
- *Înălțime netă:* 60 mm
- *Diametru exterior:* 82,50 mm
- *Greutate:* 0,1 kg

2. Funcționalități și Controler Inteligent

2.1. Control și Monitorizare

- Controler dedicat pentru gestionarea inteligentă a luminii în sistemele de iluminat rutier.
- Comunicare prin rețea mesh automată de 2,4 GHz.

2.2. Senzori Integrați

- ***Senzor de luminozitate:** Măsoară luminozitatea ambientală și permite controlul automat al iluminatului pe baza valorilor de prag definite.
- ***Senzor de calitate a aerului:** Monitorizează continuu parametrii de mediu (praf fin, COV, NOx, umiditate, temperatură ambientală).
- ***Senzor de zgomot:** Permite monitorizarea zgomotului de fond; funcțiile pot fi setate individual cu valori prag, iar nivelurile minime și maxime sunt înregistrate și afișate.

2.3. Funcții Avansate

- ***Poziționare GNSS:** Asigură date precise de geopoziționare și timp, adaptând controlul luminii la locația geografică exactă.
- ***Funcția AstroDim:** Ajustează automat profilurile de control al luminii în funcție de orele exacte de răsărit și apus, utilizând datele de geolocalizare.
- ***Configurabilitate:** Toți parametrii senzorilor pot fi setați la fața locului pentru corpuri de iluminat individuale sau pentru grupuri.

2.4. Conectivitate și Integrare

- ***eSim încorporat:** Permite integrarea corpului de iluminat într-o platformă de gestionare a luminii pe bază de web.
 - Serviciul este furnizat gratuit pentru o perioadă de 5 ani de la livrare, cu posibilitate de prelungire pentru încă 5 ani, contra cost.
- ***Monitorizare la distanță:** Controlul individual al controlerelor se poate realiza direct, prin conexiune instantanee la cloud, fără necesitatea unui gateway suplimentar.
- ***Protocoale de comunicație:** Suport global pentru LTE Cat M1, NB-IoT NB2 și EGPRS.
- ***Compatibilitate suplimentară:**
 - Interfață compatibilă cu cerințele Smart Lighting Ready (SLR) conform specificațiilor Zhaga.
 - Compatibil cu protocoalele DALI DT6 și DT7.
- ***Certificări și aplicații:**
 - Adecvat pentru implementarea în orașe inteligente datorită capacității D4i (tip A) și certificării SR.

3.3. Managementul utilizatorilor și accesul la sistem

În urma rezultatelor obținute din studiul de fezabilitate, acest capitol abordează strategia de implementare a Sistemului Informatic Integrat și Interoperabil. Sistemul propus este avansat, dezvoltat pe tehnologii moderne. Acesta reprezintă o soluție complexă care va fi dezvoltată pe o perioadă de 24 luni și care aduce cu sine îmbunătățiri pentru administrația publică locală, regională și nu numai.

Interfețele vor asigura o experiență facilă, în timp ce posibilitatea de generare a rapoartelor dinamice și capacitatea de a realiza previziuni vor aduce un suport inestimabil în luarea deciziilor administrative.

Unul dintre aspectele cheie ale acestui proiect este integrarea tuturor sistemelor externe existente într-un

singur sistem, asigurând astfel coeziunea și interoperabilitatea necesare pentru o administrare eficientă și transparentă a datelor și a proceselor administrației publice.

Etapele de implementare a proiectului:

Ciclul de viață al proiectului de Implementare a Sistemului Informatic Integrat și Interoperabil pentru digitalizarea proceselor din cadrul Primăriei comunei GORGOTA va fi constituit din opt etape: inițiere, planificare și proiectare, Aprobare cerere de finanțare, organizare proceduri de achiziție, execuție, evaluare și monitorizare, recepție și CP finală/ încheiere.

Inițiere:

Inițierea reprezintă prima etapă a ciclului de viață al proiectului. În această fază este definită ideea de proiect și este realizat studiul de fezabilitate pentru a analiza disponibilitatea instituției de a-l realiza, costul final și contribuția acestuia la obiectivele de afaceri ale primăriei.

Odată ce cerințele și oportunitățile de îmbunătățire sunt clare, echipa de proiect va proceda la proiectarea soluției Sistemului Informatic Integrat și Interoperabil. În paralel cu proiectarea soluției Sistemului Informatic Integrat și Interoperabil, se va lua în calcul și rezultatul studiului de fezabilitate a proiectului, care a implicat analizarea aspectelor financiare, alocarea resurselor, timpul necesar pentru implementare și identificarea riscurilor potențiale.

Planificare și proiectare:

Planificarea și proiectarea reprezintă cea de-a doua etapă a ciclului de viață a proiectului. Planificarea va începe cu precizarea scopului, a obiectivelor specifice ale proiectului și descrierea pașilor ce trebuie urmați.

Proiectarea dezvoltării Sistemului Informatic Integrat și Interoperațional va fi o etapă intensă și riguroasă, care va necesita colaborarea strânsă a echipei de proiect, a specialiștilor IT și a reprezentanților Primăriei. Comunicarea eficientă cu părțile interesate și implicarea lor activă în proces vor fi esențiale pentru a asigura că toate cerințele și obiectivele sunt înțelese corect și că soluția propusă va satisface nevoile și așteptările tuturor utilizatorilor.

La această etapă, echipa de dezvoltare va trebui să pregătească documentația tehnică care va include următoarele elemente:

- Specificații tehnice;

Acest document va conține descrierea în detaliu a modului în care sistemul va fi dezvoltat. El va include cerințele funcționale și ne-funcționale, precum și descrierea detaliată a caracteristicilor sistemului. Cerințele funcționale vor descrie funcțiile pe care va trebui să le realizeze produsul final, după implementarea proiectului. Cerințele ne-funcționale vor fi anexate cerințelor funcționale și vor fi divizate în mai multe tipuri: de calitate, de operare, de performanță, de fiabilitate, de securitate, etc.

- Diagrama de arhitectură;

Această diagramă va oferi o imagine de ansamblu a structurii sistemului, inclusiv componentele sale principale și modul în care acestea interacționează.

- Diagrama de baze de date;
Documentația tehnică va include o descriere a structurii licențelor solicitate, relațiilor și a modului în care datele sunt stocate și accesate.
- Diagrama de flux a proceselor;
Această diagramă va arăta cum sunt gestionate datele și procesele în cadrul sistemului, evidențiind modul în care informațiile sunt transmise și procesate.
- Descrierea interfețelor solicitate;
Va detalia modul în care vor arăta și funcționa interfețele utilizatorului, inclusiv ecranele, butoanele și funcționalitățile disponibile.
- Descrierea tehnologiilor solicitate;
Vor fi specificate tehnologiile, limbajele de programare, framework-urile și alte instrumente utilizate în dezvoltarea sistemului.

Documentația tehnică va fi responsabilitatea echipei de dezvoltare. Aceasta va servi drept ghid pentru achiziționarea licențelor software, dar va fi, de asemenea, utilă pentru mentenanța și suportul ulterior al sistemului.

Într-un final, va fi realizat planul de management al proiectului de către managerul de proiect împreună cu echipa de lucru. Acesta va include structura detaliată a activităților și matricea de alocare a responsabilităților, graficul de execuție, planul jaloanelor, planul de comunicare, planul financiar și planul de management al calității, al resurselor și al riscului.

Planul jaloanelor va oferi o imagine clară asupra evoluției în timp a proiectului datorită faptului că va include lista fazelor importante a proiectului, inclusiv data realizării lor.

Punctul de trecere la următoarea etapă va presupune aprobarea planului de management al proiectului de către beneficiarul proiectului.

Aprobare cerere de finanțare:

Pe baza datelor descrise și a Sistemului Informatic Integrat și Interoperațional solicitat, se solicită finanțare prin Programul Regional Sud- Muntenia 2021-2027,

Prioritatea 1 - O regiune competitivă prin inovare, digitalizare și întreprinderi dinamice,

Obiectivul Specific RSO 1.2 - Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al companiilor, al organizațiilor de cercetare și al autorităților publice,

Apel de proiecte: PRSM/473/PRSM_P1/OP1/RSO1.2/PRSM_A38,

Organizare proceduri de achiziție:

După aprobarea cererii de finanțare și semnarea contractului de finanțare se vor demara procedurile de achiziție.

Procedurile de achiziție pot fi demarate și concomitent cu depunerea cererii de finanțare, cu invocarea clauzei suspensive privind eventualitatea în care contractul de finanțare nu va fi semnat.

Execuție:

Execuția activităților proiectului presupune desfășurarea acestora conform specificațiilor din documentația tehnică și planul de management al proiectului. Echipa de proiect trebuie să execute sarcinile respectând toate cerințele pentru a nu exista abateri semnificative de la plan, a nu depăși volumul de resurse estimat și a se încadra în limita de timp. Managerul de proiect este însărcinat să aloce resursele necesare în mod eficient și să ofere consultanță în permanență împreună cu operatorul economic desemnat pentru asigurarea serviciilor de consultanță.

În paralel cu etapa de dezvoltare și configurare, vor fi efectuate testări tehnice a funcționalităților implementate conform planului de testare tehnică care trebuie să includă scenariile de testare pentru fiecare funcționalitate în parte.

Orice schimbare semnificativă sau problemă apărută în timpul procesului de implementare va fi raportată și discutată în mod transparent, pentru a se găsi soluții eficiente.

De asemenea, este esențial ca echipa de proiect să monitorizeze în mod regulat progresul activităților, să identifice eventualele deviații de la plan și să implementeze măsuri corective prompte, astfel încât să se asigure că proiectul rămâne pe calea sa către succes.

Etapile de dezvoltare și implementare ale Sistemului Informatic Integrat și Interoperațional vor cuprinde:

- Stabilirea specificațiilor necesare pentru funcționarea corectă a Sistemului Informatic Integrat și Interoperațional;
- Achiziționarea efectivă a licențelor și a echipamentelor IT necesare Sistemului Informatic Integrat și Interoperațional, conform specificațiilor și cerințelor stabilite în etapa anterioară;
- Completarea planului de testare tehnică, în caz de necesitate;
- Realizarea testelor pentru a se asigura că Sistemul Informatic Integrat și Interoperațional funcționează conform așteptărilor, inclusiv testarea integrității datelor și a securității sistemului;
- Rezolvarea eventualelor deficiențe identificate în cadrul testelor pentru a asigura buna funcționare a Sistemului Informatic Integrat și Interoperațional;
 - Finalizarea manualelor de utilizare pentru a facilita utilizarea și administrarea Sistemului Informatic Integrat și Interoperațional;
 - Instruirea utilizatorilor pentru a asigura o tranziție eficientă și familiarizare cu Sistemul Informatic Integrat și Interoperațional;
 - Acordarea de sprijin la sediul beneficiarului pentru utilizarea inițială a Sistemului Informatic Integrat și Interoperațional, în caz de necesitate.

Având în vedere faptul că natura livrabilelor este pur digitală, realizarea activităților descrise în cadrul Studiului de Fezabilitate pot fi realizate de la sediul Prestatorului.

Beneficiarul poate solicita întâlniri în scopul evaluării și monitorizării progresului și, de asemenea, în scopul de a prezenta contextul necesar implementării fiecărui livrabil din cadrul proiectului.

Evaluare și monitorizare:

La această etapă vor fi realizate rapoarte de progres al proiectului. Acestea vor conține analiza situației

generale a proiectului, progresul, modificările realizate de la ultima raportare, neregularități, decizii legate de proiect, controlul costurilor, riscuri și măsuri pentru gestionarea lor. Ele vor fi livrate către managementul proiectului, dar și către beneficiarul proiectului pentru a asigura transparență și implicare activă în procesul de implementare.

Evaluarea tehnică va fi activitatea principală și va consta în evaluarea funcționalității produsului hardware și software. Monitorizarea va trebui să fie un proces continuu pentru ca rezultatele proiectului să fie realizate conform celor mai înalte standarde posibile.

De asemenea, furnizorul va dezvolta un plan de monitorizare a proiectului, astfel încât să poată fi evaluat în mod regulat progresul și să se ia măsuri corective în cazul în care apar abateri de la plan.

Planul de monitorizare a proiectului

Planul de monitorizare pentru implementarea Sistemului Informatic Integrat și Interoperațional trebuie să conțină informații detaliate cu privire la activități, roluri și resursele alocate, având ca scop asigurarea unei implementări eficiente a proiectului.

Planul de monitorizare a proiectului pentru o perioadă de raportare include următoarele informații:

- Progresul înregistrat în îndeplinirea indicatorilor de etapă;
- Progresul înregistrat în îndeplinirea indicatorilor de realizare;
- Progresul înregistrat în îndeplinirea indicatorilor de rezultat;
- Progresul înregistrat în îndeplinirea indicatorilor specifici de proiect;
- Activități implementate și rezultate obținute pe parcursul perioadei de raportare;
- Analiza rezultatelor activităților în raport cu obiectivele stabilite;
- Prezentarea echipei de management și a echipei de implementare responsabili pentru implementarea activităților;
- Documentarea oricăror modificări sau ajustări aduse indicatorilor pe parcursul implementării proiectului;
- Documentarea și gestionarea oricăror abateri sau întârzieri față de planul de monitorizare inițial;
- Înregistrarea observațiilor cheie privind progresul proiectului și formularea propunerilor pentru perioada următoare în vederea remedierii eventualelor deficiențe.

Recepție, CP finală/ închiere:

Încheierea este etapa finală a proiectului. Se va asigura că au fost finalizate integral toate sarcinile și că rezultatele au fost acceptate de către beneficiar.

Pentru încheierea proiectului este necesară testarea Sistemului Informatic Integrat și Interoperațional de către beneficiar. Înainte de demararea etapei de testare funcțională de către beneficiar, echipa de testare a acestuia va participa la o sesiune dedicată de instruire organizată de către furnizor, cu scopul de a familiariza echipa de testare cu modul de utilizare a Sistemului Informatic Integrat și Interoperațional, cu configurările realizate și cu metodologia de testare. Testarea efectuată de către beneficiar se va realiza utilizând scenariile de testare agreeate în prealabil, din planul de testare tehnică, beneficiarul având libertatea să ruleze orice alt test pe care îl consideră necesar în vederea validării modului de funcționare a funcționalităților solicitate și proiectate în cadrul Sistemului Informatic Integrat și Interoperațional.

3.4. Securitatea sistemului și a datelor

Implementarea unui sistem robust de securitate va fi de importanță majoră pentru protejarea datelor sensibile și a informațiilor cetățenilor. Accesul la date trebuie să fie controlat, iar transmiterea informațiilor să fie securizată pentru a evita posibilele vulnerabilități.

Securitatea informațiilor este primordială pentru protejarea informațiilor sensibile și a resurselor informatice ale Primăriei. Prevederile de securitate sunt concepute pentru a crea un mediu sigur și controlat, în care datele și procesele sunt protejate împotriva accesului neautorizat, pierderii sau distrugerii. Ele stabilesc standarde clare privind gestionarea parolelor, accesul la rețele și sisteme, monitorizarea activității, criptarea datelor și multe altele.

După analiza Politicii și Regulamentului de Securitate IT din cadrul Primăriei comunei GORGOTA, aprobat prin dispoziția primarului, a fost constatat că acest regulament îndeplinește toate prevederile necesare pentru asigurarea securității și confidențialității informațiilor și resurselor informatice utilizate în cadrul instituției. Nu s-a simțit necesitatea de a replica prevederile de securitate din Politică și Regulamentul de Securitate în studiul de fezabilitate.

Este important de subliniat că această Politică și Regulament de Securitate trebuie aplicate și asupra Sistemului Informatic Integrat. Acest lucru implică respectarea tuturor prevederilor privind securitatea, managementul datelor și controlul accesului la informații, astfel încât să se asigure o funcționare corespunzătoare și să se minimizeze riscurile de securitate pentru toate componentele Sistemului Informatic Integrat.

Prin includerea acestor politici și reguli de securitate, se demonstrează angajamentul față de standardele de securitate și confidențialitate și se asigură că SII propus în acest studiu de fezabilitate va fi gestionat în conformitate cu cele mai bune practici de securitate.

Securitatea datelor reprezintă un pilon fundamental al oricărui sistem digital modern, necesitând implementarea unor măsuri riguroase pentru protecția informațiilor sensibile și prevenirea accesului neautorizat. Această securitate trebuie abordată dintr-o perspectivă multidimensională, incluzând atât aspecte tehnice, cât și politici organizaționale menite să asigure integritatea, confidențialitatea și disponibilitatea datelor.

Criptarea datelor constituie una dintre cele mai eficiente metode de protecție împotriva accesului neautorizat, atât în timpul stocării, cât și pe parcursul transmisiei acestora. Utilizarea unor algoritmi de criptare avansați, precum AES-256 pentru criptarea simetrică și RSA-4096 pentru criptarea asimetrică, asigură un nivel ridicat de securitate și protecție împotriva atacurilor de tip brute force. Implementarea unor protocoale sigure de comunicare, precum TLS 1.3 și IPsec, garantează că datele sunt protejate pe întregul flux de transfer, prevenind interceptările neautorizate și atacurile de tip man-in-the-middle. În plus, utilizarea tehnologiilor de tokenizare și hashing pentru stocarea informațiilor sensibile, cum ar fi datele de autentificare și informațiile financiare, reduce semnificativ riscurile asociate compromiterii datelor.

Controlul accesului este un alt aspect esențial al securității datelor, asigurând că doar utilizatorii autorizați au permisiunea de a accesa sau modifica informațiile sensibile. Implementarea unui model de

control al accesului bazat pe roluri (RBAC) permite definirea unor permisiuni stricte pentru fiecare utilizator, reducând astfel suprafața de atac. În plus, adoptarea unui sistem de autentificare multifactorială (MFA), care combină parole complexe, autentificare biometrică și tokenuri hardware, crește semnificativ nivelul de protecție împotriva atacurilor de tip phishing și credential stuffing.

Pe lângă măsurile tehnice, este esențială implementarea unor **politici și proceduri stricte privind securitatea datelor**. Organizarea unor sesiuni periodice de training pentru angajați, realizarea de audituri de securitate și adoptarea unor mecanisme de monitorizare continuă sunt elemente cheie pentru detectarea și prevenirea incidentelor de securitate. În plus, utilizarea unor sisteme avansate de detecție a intruziunilor (IDS) și prevenție (IPS), împreună cu soluții de securitate bazate pe inteligență artificială, permit identificarea și neutralizarea amenințărilor cibernetice în timp real.

Astfel, printr-o abordare integrată care combină criptarea avansată, controlul riguros al accesului și implementarea unor politici de securitate eficiente, se poate asigura protecția optimă a datelor sensibile și menținerea unui mediu digital sigur și de încredere.

3.4 Interoperabilitatea

Interoperabilitatea reprezintă un element fundamental în dezvoltarea și implementarea soluțiilor digitale destinate administrației publice, având rolul de a facilita integrarea și comunicarea eficientă între diverse sisteme informatice. Aceasta trebuie să fie aliniată la standardele impuse de cadrul ISA² (Interoperability Solutions for Public Administrations, Businesses and Citizens), asigurând schimbul optimizat de date și informații între instituțiile guvernamentale, atât la nivel național, cât și european. Pentru atingerea acestui obiectiv, este esențială adoptarea unor soluții software scalabile, capabile să gestioneze volume mari de date, menținând în același timp securitatea, consistența și integritatea acestora.

Utilizarea standardelor deschise constituie o cerință esențială pentru asigurarea compatibilității între platforme diferite și evitarea dependenței de furnizori specifici (vendor lock-in). Adoptarea unor formate de date structurate, precum XML, JSON și RDF, împreună cu protocoale de comunicare standardizate, cum ar fi RESTful APIs și SOAP, permite o interconectare robustă între sistemele administrației publice. De asemenea, utilizarea standardelor de autentificare și autorizare, cum ar fi OAuth 2.0 și OpenID Connect, garantează un acces securizat și eficient al utilizatorilor la serviciile digitale. Implementarea unui model semantic comun, bazat pe ontologii și clasificări standardizate, facilitează interpretarea unitară a datelor și îmbunătățește interoperabilitatea între platforme eterogene.

Integrarea cu sisteme externe reprezintă un alt aspect critic al interoperabilității, având impact direct asupra eficienței și fluidității proceselor administrative. Conectarea cu registrele naționale, bazele de date centralizate și arhivele electronice trebuie să se realizeze prin mecanisme sigure și eficiente, asigurând atât consistența, cât și confidențialitatea datelor procesate. De exemplu, utilizarea unor gateway-uri de interoperabilitate bazate pe standarde precum eIDAS pentru autentificare transfrontalieră sau PEPPOL pentru schimbul electronic de documente poate facilita comunicarea interinstituțională la nivel european. În plus, implementarea unor mecanisme de sincronizare și replicare a datelor între diferite sisteme asigură coerența informațiilor și minimizează riscurile asociate incongruenței datelor.

Pentru a susține o interoperabilitate eficientă și sustenabilă pe termen lung, este necesară adoptarea unui **cadru de guvernare a datelor**, care să reglementeze procesele de schimb și acces la informații între instituții. Acest cadru trebuie să includă politici clare privind accesul la date, mecanisme de audit și monitorizare, precum și strategii de gestionare a conformității cu reglementările internaționale în materie de protecție a datelor, cum ar fi GDPR. În plus, utilizarea tehnologiilor emergente, precum blockchain pentru auditabilitate și securitate sau inteligența artificială pentru analiza și clasificarea datelor, poate aduce îmbunătățiri semnificative în eficiența schimbului de informații.

Astfel, prin aplicarea acestor principii și tehnologii avansate, interoperabilitatea sistemelor administrației publice devine un factor esențial în creșterea eficienței și transparenței instituționale, facilitând o colaborare eficientă și sigură între diverse entități guvernamentale și contribuind la îmbunătățirea serviciilor oferite cetățenilor.

3.5. Sustenabilitatea

Sustenabilitatea reprezintă un principiu fundamental în proiectarea și dezvoltarea sistemelor informatice destinate administrației publice, având rolul de a asigura menținerea și actualizarea acestora pe termen lung. Un sistem sustenabil trebuie să fie construit pe o arhitectură flexibilă, capabilă să se adapteze cerințelor în continuă schimbare, oferind în același timp suport tehnic, actualizări periodice și posibilitatea de extindere a funcționalităților pentru a răspunde nevoilor emergente ale utilizatorilor și ale instituțiilor.

Mentenanța și suportul sunt componente esențiale ale sustenabilității unui sistem informatic, necesitând implementarea unui plan detaliat care să asigure funcționarea optimă și remedierea promptă a eventualelor deficiențe. Acest plan trebuie să includă actualizări regulate ale software-ului pentru a remedia vulnerabilitățile de securitate, a îmbunătăți performanța și a introduce noi funcționalități, aliniate cerințelor legislative și tehnice în vigoare. De asemenea, este imperativă existența unei echipe de suport tehnic, capabile să ofere asistență utilizatorilor, să monitorizeze funcționarea sistemului și să implementeze măsuri preventive pentru evitarea incidentelor critice.

Scalabilitatea constituie un aspect critic al sustenabilității, întrucât sistemul trebuie să fie proiectat astfel încât să poată gestiona un volum crescut de date și un număr tot mai mare de utilizatori, fără a compromite performanța sau securitatea. Utilizarea unei arhitecturi modulare și a tehnologiilor de virtualizare și orchestrare, precum containerele Docker și platformele Kubernetes, permite extinderea resurselor în mod dinamic, în funcție de cerințele operaționale. În plus, adoptarea unui model de infrastructură bazat pe cloud computing oferă o flexibilitate sporită, permițând scalarea verticală și orizontală, reducerea costurilor operaționale și asigurarea continuității serviciilor prin redundanță și mecanisme avansate de recuperare în caz de dezastru.

Pentru a garanta sustenabilitatea pe termen lung, este esențială integrarea unor mecanisme de automatizare a proceselor de mentenanță, precum **actualizările automate, detectarea anomaliilor prin inteligență artificială și utilizarea unor soluții de monitorizare proactive**. Implementarea unor instrumente de DevOps, cum ar fi CI/CD (Continuous Integration/Continuous Deployment), contribuie la

optimizarea ciclurilor de dezvoltare și implementare, reducând riscurile asociate implementărilor defectuoase și minimizând timpii de întrerupere a serviciilor.

Astfel, un sistem informatic sustenabil nu doar că răspunde cerințelor actuale, dar este și pregătit să evolueze, oferind o bază solidă pentru inovație și dezvoltare continuă în administrația publică. Prin aplicarea principiilor menționate, se asigură o infrastructură rezilientă, eficientă și capabilă să sprijine digitalizarea administrației într-un mod sigur și fiabil.

Implementarea unui sistem digital performant, care integrează gestionarea documentelor, portalul e-Cetățean, chatbot-ul AI, website-ul instituțional și infrastructura hardware a Primăriei, necesită un plan detaliat de mentenanță și sustenabilitate. Acest plan trebuie să asigure funcționarea optimă a sistemului pe termen lung, să prevină apariția vulnerabilităților de securitate și să permită evoluția continuă a infrastructurii digitale.

Mentenanța sistemului se va desfășura pe mai multe niveluri, incluzând monitorizarea performanței, actualizări regulate de software și securitate, intervenții tehnice prompte și optimizări continue. Pe de altă parte, sustenabilitatea proiectului implică alocarea resurselor financiare și umane necesare, instruirea constantă a personalului și adaptarea la cerințele legislative și tehnologice emergente.

Dintre strategiile de mentenanță, atât pentru componenta Hardware, precum și pentru cea Software, amintim:

a. Mentenanța preventivă

Mentenanța preventivă presupune o abordare proactivă pentru a evita defectările critice și a menține sistemul la un nivel optim de funcționare. Aceasta include:

Monitorizarea continuă a performanței serverelor și a resurselor utilizate pentru a preveni supraîncărcarea infrastructurii.

Actualizări periodice ale sistemelor de operare și aplicațiilor pentru a elimina vulnerabilitățile de securitate.

Teste regulate de stres și scalabilitate pentru a asigura capacitatea de răspuns la creșteri bruște ale cererii de acces la platforme.

Scanări de vulnerabilitate și audituri de securitate pentru identificarea și remedierea punctelor slabe.

b. Mentenanța corectivă

Această componentă implică intervenții tehnice rapide pentru remedierea eventualelor defecțiuni sau erori. Se va implementa un sistem de ticketing pentru raportarea problemelor de către utilizatori, cu termene clare de rezolvare, în funcție de gradul de criticitate. De asemenea, echipele IT vor avea planuri de intervenție rapidă pentru remedierea incidentelor critice, cum ar fi atacurile cibernetice, erorile de software sau defecțiunile hardware.

c. Automatizarea proceselor de mentenanță

Pentru eficientizarea activităților de mentenanță, se vor implementa soluții de automatizare, precum:

- Sisteme de patch management automatizat, care aplică într-un mod controlat actualizările de securitate.

- Algoritmi de machine learning pentru detectarea anomaliilor și prevenirea incidentelor.
- Backup-uri automate și soluții de recuperare a datelor pentru a preveni pierderea informațiilor esențiale.

3.6 Confidențialitatea datelor

Principalele riscuri legate de confidențialitatea datelor în proiectele de digitalizare:

- Atacuri cibernetice: Hackeri pot accesa ilegal sistemele informatice și pot fura date cu caracter personal.
- Eroarea umană: Angajații pot comite erori în gestionarea datelor, ducând la divulgarea accidentală a informațiilor sensibile.
- Pierderea sau deteriorarea echipamentelor: Dispozitivele de stocare a datelor pot fi pierdute, furate sau deteriorate.
- Parteneri externi: Transmiterea datelor către terți poate expune informațiile la riscuri suplimentare.

Măsuri pentru asigurarea confidențialității datelor:

- Evaluarea riscurilor enumerate în cadrul SF: Identificarea și evaluarea tuturor riscurilor potențiale legate de securitatea datelor.
- Implementarea măsurilor tehnice: Utilizarea de firewalls, sisteme de detecție a intruziunilor, criptare a datelor, autentificare în doi factori și alte tehnologii de securitate.
- Măsuri organizatorice: Stabilirea unor politici clare privind securitatea datelor, instruirea angajaților, efectuarea de audituri de securitate și stabilirea unor proceduri de răspuns la incidente.
- Protecția datelor cu caracter personal prin design: Integrarea măsurilor de protecție a datelor încă din faza de proiectare a sistemelor informatice.
- Supravegherea continuă: Monitorizarea constantă a sistemelor informatice pentru a detecta și răspunde prompt la orice incident de securitate.
- Cooperare cu autoritățile: Colaborarea cu autoritățile competente în cazul unor incidente de securitate.

Confidențialitatea datelor reprezintă un pilon esențial al securității informațiilor în cadrul Primăriei, având un rol crucial în protejarea informațiilor sensibile ale cetățenilor și ale instituției. Odată cu digitalizarea proceselor administrative și migrarea tot mai multor servicii către platforme informatice, protejarea datelor devine o prioritate strategică. Implementarea unor soluții de securitate avansate, alături de politici clare de acces și de instruire continuă a angajaților, este esențială pentru prevenirea accesului neautorizat, a pierderilor de date și a scurgerilor de informații.

Prin adoptarea unor metode riguroase de protecție și monitorizare, Primăria asigură că datele colectate și gestionate sunt protejate împotriva amenințărilor interne și externe. Aceasta implică utilizarea criptării, controalelor de acces sofisticate, autentificării multiple și unui sistem de monitorizare continuă. În plus, instruirea personalului contribuie la reducerea riscului uman, una dintre principalele cauze ale breșelor de securitate.

- Criptarea datelor

Pentru a preveni accesul neautorizat, toate datele sunt criptate folosind algoritmi avansați, atât în repaus, cât și în tranzit. Criptarea este esențială pentru a preveni expunerea accidentală a informațiilor și accesul neautorizat de către terți.

Datele stocate pe serverele locale sunt protejate prin criptare AES-256, oferind un nivel ridicat de siguranță și reducând riscul de furt de date în cazul accesului fizic la infrastructură.

Datele transmise prin rețea sunt criptate prin protocoale TLS (Transport Layer Security), prevenind interceptarea acestora și garantând că numai destinatarii autorizați pot accesa informațiile.

Pentru protecția informațiilor confidențiale din bazele de date, sunt utilizate metode de criptare avansate, precum tokenizarea și hashing-ul.

- Controlul accesului la date

Sistemul utilizează un model de acces bazat pe roluri (RBAC), care asigură că doar utilizatorii autorizați au acces la informațiile relevante pentru funcția lor. Acest model limitează expunerea datelor doar la persoanele care au nevoie de ele pentru desfășurarea activităților specifice.

În plus, este implementat un control bazat pe atribute (ABAC), care permite restricționarea accesului pe baza unor factori contextuali, precum locația utilizatorului, dispozitivul utilizat sau momentul accesului. Astfel, accesul la date este gestionat dinamic, reducând riscurile asociate cu expunerea excesivă a informațiilor sensibile.

- Monitorizare și audit

Toate accesările și modificările efectuate asupra datelor sunt monitorizate printr-un sistem de auditare avansat. Soluțiile SIEM (Security Information and Event Management) sunt integrate pentru detectarea anomaliilor și a potențialelor breșe de securitate, generând alerte automate în cazul unor comportamente suspecte.

În plus, se mențin jurnale detaliate ale activităților utilizatorilor, care permit investigarea incidentelor de securitate și identificarea rapidă a eventualelor amenințări. Aceste jurnale sunt analizate periodic pentru a detecta tipare de atac și pentru a îmbunătăți măsurile de protecție existente.

- Autentificare și autorizare

Autentificarea utilizatorilor se face prin metode multiple, garantând un nivel ridicat de securitate:

- Autentificare multi-factor (MFA), combinând parolele cu coduri unice generate prin aplicații dedicate sau dispozitive hardware.
- Certificate digitale pentru autentificarea securizată a utilizatorilor.
- Protocoale OAuth 2.0 pentru integrarea cu servicii externe, menținând securitatea și confidențialitatea datelor.

Politici stricte de gestionare a parolelor, impunând utilizarea unor parole complexe și schimbarea acestora la intervale regulate.

- Protecția împotriva amenințărilor externe

a. Firewall și sisteme de prevenire a intruziunilor

Soluțiile de firewall avansate și sistemele de prevenire a intruziunilor (IDS/IPS) sunt implementate pentru a detecta și bloca atacurile cibernetice în timp real. Aceste sisteme analizează traficul de rețea pentru a identifica și neutraliza amenințările înainte ca acestea să afecteze infrastructura IT.

b. Protecția împotriva atacurilor DDoS

Sistemele de protecție DDoS sunt integrate pentru a preveni suprasolicitarea infrastructurii IT a Primăriei, asigurând continuitatea operațiunilor. Aceste soluții filtrează traficul malițios și previn blocarea accesului la serviciile online.

c. Scanare și testare de vulnerabilități

Testele periodice de penetrare și scanările de vulnerabilități sunt realizate pentru a identifica punctele slabe ale infrastructurii și a le remedia proactiv. Aceste măsuri permit detectarea și eliminarea eventualelor breșe de securitate înainte ca acestea să fie exploatare de atacatori.

- Instruirea angajaților Primăriei

a. Training periodic

Angajații sunt instruiți periodic cu privire la bunele practici de securitate cibernetică, inclusiv recunoașterea atacurilor de tip phishing, utilizarea parolelor sigure și manipularea responsabilă a datelor sensibile. Aceste sesiuni de instruire contribuie la reducerea erorilor umane și la prevenirea incidentelor de securitate.

b. Simulări de atacuri cibernetice

Primăria organizează periodic exerciții de simulare a atacurilor cibernetice pentru a testa răspunsul personalului la posibile incidente de securitate. Aceste simulări permit identificarea punctelor slabe și îmbunătățirea strategiilor de apărare.

c. Politici clare de confidențialitate

Fiecare angajat este obligat să respecte politici stricte de confidențialitate, iar accesul la date este revizuit constant pentru a preveni utilizarea neautorizată a informațiilor. Politicile sunt actualizate constant pentru a se conforma reglementărilor în vigoare și celor mai bune practici din domeniul securității cibernetice.

3.7 Matricea de complementaritate dintre proiectele aflate în implementare sau implementate și proiectul ce se dorește a fi finanțat

Matricea de complementaritate este un instrument strategic care permite evaluarea modului în care proiectul, în cazul nostru de digitalizare, se integrează și se aliniază cu celelalte inițiative existente într-o instituție publică. Acest instrument este esențial pentru a evita suprapunerile, a maximiza eficiența investițiilor și a asigura o tranziție digitală fluidă și coerentă.

La elaborarea matricei de complementaritate plecăm de la:

- **Identificarea sinergiilor:** Ajută la identificarea punctelor comune și a oportunităților de colaborare între proiecte.
- **Prevenirea duplicărilor:** Evită alocarea inutilă a resurselor către activități care sunt deja în curs de desfășurare.

- **Optimizarea investițiilor:** Asigură o utilizare eficientă a bugetului, concentrând eforturile asupra proiectelor cu cel mai mare impact.
- **Ameliorarea planificării:** Contribuie la o planificare mai bună a implementării, ținând cont de dependențele dintre proiecte.
- **Facilitarea gestionării schimbării:** Ajută la gestionarea mai eficientă a schimbării organizaționale, prin alinierea proiectelor cu obiectivele strategice ale instituției.

În cazul Comunei GORGOTA, proiectul este complementar cu

4. RESURSE

4.1. Personal si instruire

Pentru asigurarea capacității manageriale și instituționale în cadrul acestui proiect, se recomandă desemnarea unui manager de proiect care va coordona toate aspectele implementării, începând de la momentul obținerii finanțării și până la finalizarea și evaluarea investiției. Acest manager poate fi selectat din rândul personalului specializat al primăriei și/sau poate fi un expert extern cu experiență în gestionarea proiectelor similare.

Managerul de proiect va fi responsabil pentru coordonarea tuturor activităților și va colabora strâns cu reprezentanții primăriei, echipa de proiect și toate celelalte părți implicate în implementarea proiectului. De asemenea, va menține comunicarea și colaborarea cu toate instituțiile relevante care ar putea fi implicate în finalizarea proiectului.

Asigurarea capacității manageriale și instituționale este definitorie pentru succesul oricărui proiect. Alte recomandări pentru a asigura o capacitate managerială și instituțională adecvată:

- Planificare a resurselor umane;
 - o Identificarea și evaluarea nevoilor de resurse umane pentru gestionarea și operarea sistemului.
 - o Selectarea personalului potrivit cu competențele necesare.
 - o Asigurarea de training-uri și dezvoltare continuă pentru echipa de management și pentru personalul cheie.
- Definirea rolurilor și responsabilităților;
 - o Stabilirea clară a rolurilor și responsabilităților personalului.
 - o Desemnarea unui administrator principal care să coordoneze toate procesele legate de sistem și să asigure buna funcționare a lui.
- Structură organizațională eficientă;
 - o Formarea unui departament sau a unei echipe dedicate pentru gestionarea Sistemului Informatic Integrat.
 - o Definirea relațiilor și fluxurilor de comunicare între departamentele sau echipele implicate în gestionarea sistemului.
- Politici și proceduri clare;
 - o Dezvoltarea unor politici și proceduri clare pentru gestionarea sistemului. Acestea ar trebui

să acopere aspecte precum securitatea datelor, gestionarea incidentelor, actualizări și întreținere, inclusiv și utilizarea sistemului.

o Asigurarea că toți angajații cunosc și respectă politicile și procedurile definite.

- Parteneriate și consultanță externă;
 - o Angajarea consultanților sau specialiștilor externi pentru sprijinul în gestionarea sistemului.
 - o Parteneriate sau colaborați cu alte organizații sau instituții care au experiență în gestionarea sistemelor similare.
- Evaluare și îmbunătățiri continue;
 - o Realizarea evaluărilor regulate ale capacității manageriale și instituționale și identificarea punctele slabe sau nevoile de îmbunătățire.
 - o Implementarea măsurilor pentru a consolida capacitatea managerială și instituțională pe măsură ce proiectul evoluează.

Asigurarea capacității manageriale și instituționale este un proces continuu și dinamic. Este importantă adaptarea la schimbările din cadrul instituției și din mediul extern pentru a asigura gestionarea eficientă a sistemului și pentru a atinge obiectivele stabilite.

De asemenea, încheierea prevede în sine și etapa de instruire a utilizatorilor finali din cadrul primăriei.

Etapa de instruire reprezintă un aspect fundamental în implementarea cu succes a Sistemului Informatic Integrat și Interoperațional pentru Digitalizarea Proceselor în cadrul Primăriei comunei GORGOTA. Această etapă cuprinde totalitatea activităților de formare și pregătire a utilizatorilor, având ca obiectiv să îi doteze cu cunoștințele și competențele necesare pentru a utiliza eficient sistemul informatic integrat.

După încheierea proiectului, va fi întocmit un raport final al proiectului. Acest raport va cuprinde descrierea rezultatelor obținute, nivelul de satisfacție al beneficiarului proiectului și evaluarea îndeplinirii obiectivelor. Această etapă va fi încheiată odată cu acceptarea proiectului de către beneficiar.

Se va efectua un audit final, atât financiar, cât și tehnic IT, de către auditori externi independenți. Aceste audituri au rolul de a certifica că proiectul a fost implementat în locația specificată în contract, că activele achiziționate sunt în stare de funcționare, iar obligațiile asumate în cadrul contractului de finanțare, inclusiv cele referitoare la securitatea aplicației, testarea nivelelor de securitate ale sistemului informatic, protecția informației și respectarea reglementărilor privind datele cu caracter personal, au fost îndeplinite din punct de vedere tehnic și financiar.

Raportul de audit financiar final va cuprinde o evaluare detaliată a tuturor cheltuielilor efectuate în cadrul implementării proiectului.

Pentru a asigura o instruire completă și bine structurată, furnizorul va adopta o metodologie de management de proiect care să includă componente și procese dedicate acestei etape.

În acest sens, se vor elabora instrucțiuni specifice de lucru pentru activitățile tipice desfășurate în cadrul sistemului Sistemului Informatic Integrat Mixt bazat pe microservicii, pentru a asigura o utilizare corectă și eficientă a sistemului.

Iată lista de instrucțiuni specifice pentru activitățile tipice desfășurate în cadrul acestui sistem:

- Instrucțiuni pentru accesarea sistemului:
 - o Cum să accesați platforma sau interfața sistemului (URL, autentificare etc.).
 - o Cum să vă autentificați cu credențialele corecte și să vă asigurați că sunteți conectat în mod corespunzător.
- Navigarea în sistem:
 - o Prezentarea interfeței utilizatorului și a elementelor de meniu.
 - o Cum să navigați între diferitele module sau funcționalități ale sistemului.
- Migrarea datelor:
 - o Cum vor fi migrate datele în sistem, inclusiv formatele acceptate și pașii necesari.
 - o Cum să corectați sau să actualizați datele introduse în caz de erori.
- Generarea de rapoarte:
 - o Cum să utilizați funcțiile de generare a rapoartelor pentru a extrage informații și date relevante.
 - o Cum să personalizați și să configurați rapoartele în funcție de nevoile dvs.
- Securitate și confidențialitate:
 - o Cum să respectați politicile și procedurile de securitate ale sistemului.
 - o Cum să protejați confidențialitatea datelor și să preveniți accesul neautorizat.
- Soluționarea problemelor comune:
 - o Cum să identificați și să raportați problemele sau erorile comune și cum să căutați soluții sau asistență.
- Instrucțiuni pentru actualizări și întreținere:
 - o Cum să vă actualizați și să vă mențineți aplicația sau instrumentele utilizate în cadrul sistemului.
- Suport și contacte:
 - o Cum să contactați echipa de suport tehnic sau de asistență în caz de întrebări sau probleme.
- Exemple de scenarii de lucru:
 - o Exemple concrete de cum să utilizați sistemul pentru sarcini specifice sau pentru a rezolva probleme frecvente.

Instrucțiunile trebuie să fie clare, concise și ușor de urmărit, cu capturi de ecran sau exemple practice, acolo unde este cazul. De asemenea, este important să se ofere sesiuni de instruire și asistență în timp real pentru a ajuta utilizatorii să se familiarizeze cu sistemul și să răspundă la orice întrebări sau dificultăți întâmpinate. Furnizorul se va asigura că instruirea utilizatorilor va fi personalizată și adaptată nevoilor specifice ale categoriilor de personal din cadrul Primăriei comunei GORGOTA. Un manager de proiect cu expertiză tehnică va coordona întregul proces de instruire și va asigura că resursele beneficiarului sunt disponibile la momentele prevăzute în calendarul de implementare. De asemenea, acesta va superviza procesul de instruire pentru a se asigura că se urmăresc obiectivele stabilite, iar utilizatorii învață să folosească eficient sistemul.

În cadrul planului de instruire se vor detalia următoarele aspecte:

- Aria de funcționalitate din cadrul sistemului care va fi acoperită în fiecare fază de instruire și categoria de utilizatori alocată fiecărei faze;
- Perioada de desfășurare a fiecărei faze de instruire, pentru a se stabili un calendar coerent și bine structurat;
- Cunoștințe minime necesare pentru fiecare fază de instruire, astfel încât toți utilizatorii să aibă nivelul de cunoștințe adecvat pentru a folosi sistemul în mod eficient;
- Infrastructura hardware-software necesară pentru derularea sesiunilor de instruire, asigurându-se că beneficiarul dispune de echipamente și resursele tehnice necesare pentru formare;
- Modalitatea de desfășurare a instruirii prioritar va avea loc online la solicitare poate fi realizată și la sediile beneficiarului;
- Furnizarea suportului de curs în limba română, prin manuale de utilizare tipărite și în format digital, pentru ca utilizatorii să aibă resurse de referință în timpul instruirii și ulterior;
- Se va detalia planul de instruire pentru fiecare modul de formare, indicând numărul de ore alocate, categoriile de personal vizate și tematica acoperită în cadrul procesului de pregătire. Pentru a se asigura o punere în aplicare cât mai eficientă a Sistemului Informatic Integrat și Interoperațional,

se vor organiza sesiuni de instruire pentru un număr minim de utilizatori și administratori. Astfel, se va acoperi întregul spectru de activități și funcționalități pe care sistemul le implică:

- Instruire generală pentru gestionarea Sistemului Informatic Integrat și Interoperațional, pentru cei implicați în gestionarea proiectului de implementare a sistemului, inclusiv manageri de proiect și coordonatori;
- Instruire pentru 2-3 administratori de aplicații, care vor fi responsabili de gestionarea și configurarea sistemului la nivel avansat;
- Instruire pentru utilizatori avansați, care au nevoie de cunoștințe avansate pentru a utiliza funcționalități complexe ale sistemului, cum ar fi rapoarte personalizate, analize de date sau funcționalități specifice departamentelor lor;
- Instruire pentru personalul de asistență tehnică, responsabili cu furnizarea de suport tehnic și asistență utilizatorilor. Aceasta poate include sesiuni de depanare, soluționare a problemelor comune și procese de gestionare a solicitărilor de asistență.
- Instruire pentru personalul de securitate, responsabili cu aplicarea politicilor de securitate și protecție a datelor în cadrul sistemului. Aceasta poate include măsuri de prevenire a amenințărilor cibernetice și gestionarea incidentelor de securitate.
- Instruire pentru actualizări și întreținere pentru personalul care va efectua actualizarea sistemului și menținerea acestuia în funcțiune. Aceasta poate include proceduri de actualizare, backup și restaurare a datelor.
- Instruire pentru raportarea și analiza datelor pentru utilizatorii care au nevoie să efectueze analize complexe asupra datelor din sistem și să creeze rapoarte avansate pentru luarea deciziilor strategice;

Aceste sesiuni suplimentare ar trebui să fie personalizate în funcție de nevoile și specificațiile sistemului și să fie oferite în funcție de rolurile și responsabilitățile diferitelor echipe din cadrul primăriei.

Această abordare va contribui la creșterea adoptării și eficienței utilizării Sistemului Informatic Integrat și Interoperațional și va facilita tranziția către un mediu de lucru digital și modern în cadrul Primăriei comunei GORGOTA.

4.2. Resurse materiale: nu este cazul

5. MENTENANTA SI SUSTENABILITATE

După finalizarea cu succes a implementării, faza de operare și mentenanță a sistemului va necesita o forță de muncă mai mică pentru a asigura funcționarea corespunzătoare a acestuia. Se estimează că, în această fază, va fi necesar cel puțin 1 specialist pentru a administra și întreține sistemul: administrator/inginer IT/administrator de rețea și securitate sau o persoană cu atribuții în acest sens. Aceste locuri de muncă vor contribui la menținerea eficienței și performanței sistemului pe termen lung.

Serviciile de mentenanță corectivă din perioada de garanție a produselor și licențelor software se va solicita să fie incluse în prețul bunului.

Mentenanța corectivă reprezintă totalitatea operațiunilor de intervenție la un echipament/produs care se efectuează ca urmare a unor defecțiuni sau funcționării în afara parametrilor optimi cu scopul de a restabili capacitatea de funcționare optimă a echipamentului/produsului.

Mentenanța corectivă include localizarea, diagnosticarea defectelor, inclusiv intervenția pentru restabilirea bunei funcționari și trebuie efectuată pentru toate părțile componente ale produsului atunci când autoritatea/entitatea contractantă semnalează un incident.

Contractantul trebuie să includă în costurile mentenanței corectivă toate costurile aferente intervenției, cum ar fi, dar fără a se limita la: forța de muncă, piesele de schimb, alte materiale sau consumabile, costurile cu transportul echipamentului/produsului de la sediul beneficiarului la locul efectuării operațiilor de mentenanță corectivă, dacă este cazul. Activitățile de mentenanță corectivă se vor realiza, de regulă, în locațiile unde sunt instalate echipamentele. În cazul în care activitățile de mentenanță corectivă necesită operații tehnologice mai complicate, acestea pot fi executate și la sediul contractantului, caz în care se întocmește un proces verbal de custodie.

După fiecare intervenție corectivă, contractantul trebuie să se efectueze teste de funcționare care să demonstreze că echipamentul/produsul funcționează în parametrii optimi și să prezinte un raport care să includă activitățile realizate, piesele de schimb utilizate, precum și rezultatele testelor de funcționare.

Pe toată durata contractului și în perioada de garanție, Furnizorul va asigura suport tehnic. Furnizorul va pune la dispoziția Autorității Contractante fără costuri, o aplicație de ticketing prin care se poate semnaliza orice problemă/defecțiune în garanție, pentru gestionarea unui incident și va conține cel puțin monitorizarea incidentelor de la deschidere până la rezolvare, analiza incidentelor și detaliilor privind producerea incidentului, realizarea rapoartelor de incident. Aplicația va fi detaliată în cadrul ofertei. Contractantul va asigura un punct de contact dedicat personalului autorizat al autorității/entității contractante unde se poate semnaliza orice problemă/defecțiune care necesită mentenanță corectivă sau solicită suport tehnic contractantului în gestionarea unui incident, disponibil, pentru a se asigura că orice situație semnalată este tratată cu promptitudine.

Contractantul va răspunde în timp util la orice incident semnalat de autoritatea/entitatea contractantă, în funcție de nivelul incidentului. Fiecare incident este caracterizat de un nivel de prioritate, care va evidenția impactul acestuia asupra funcționalităților produsului.

Se va solicita ca fiecare echipament să fie furnizat cu o disponibilitate a pieselor de schimb de cel puțin 2 ani de la data livrării (achiziționarea pieselor de schimb nu face obiectul prezentei proceduri). Ofertantul va prezenta în propunerea tehnică:

- a) recomandări cu privire la piesele de schimb care trebuie să existe în mod curent pentru a facilita efectuarea în cel mai scurt timp a operațiunilor de mentenanță corectivă;
- b) timpul de livrare estimativ pentru piesele de schimb recomandate;
- c) alte informații relevante.

Toate piesele de schimb/materiale consumabile asigurate de contractant trebuie să respecte cerințele tehnice și de calitate ale producătorului echipamentului.

Nu se solicită în mod obligatoriu ca contractantul să asigure piese de schimb și orice alte materiale consumabile după expirarea perioadei de garanție.

Indicatorii tehnico- economici sunt în conformitate cu cei detaliați în cadrul studiului de fezabilitate.

Proiectul tehnic a fost elaborat de către: TRUST BGE CONF S.R.L.

Elaborat conform contractului/ achiziției în SEAP: DA37845319 /07.04.2025