ROMÂNIA
JUDEŢUL PRAHOVA
CONSILIUL LOCAL AL MUNICIPIULUI PLOIEŞTI

HOTĂRÂREA NR. 175

pentru modificarea Hotărârii nr. 158 din 31.03.2025 privind aprobarea documentației și a indicatorilor tehnico-economici pentru proiectul „Timpul tău e prețios, nu-l pierde la cozi și ghișee! Digitalizarea este soluția!” în cadrul Programului Regional Sud Muntenia 2021-2027

Consiliul Local al Municipiului Ploieşti:

Văzând Referatul de aprobare nr. 208/16.04.2025 al domnului primar Mihai - Laurențiu Polițeanu, Raportul de specialitate comun nr. 5097/15.04.2025 al Direcției Tehnic-Investiții, nr. 219/15.04.2025 al Serviciului Relații Internaționale, Proiecte cu Finanţare Internaţională, ONG și Implementare Proiecte și nr. INFO 42/15.04.2025 al Compartimentului Informatică, Raportul de specialitate nr. 200/16.04.2025 al Direcției Administrație Publică, Juridic-Contencios, Achiziții Publice, Contracte și Raportul de specialitate nr. 138/16.04.2025 al Direcției Economice, referitoare la modificarea Hotărârii nr. 158 din 31.03.2025 privind aprobarea documentației și a indicatorilor tehnico-economici pentru proiectul „Timpul tău e prețios, nu-l pierde la cozi și ghișee! Digitalizarea este soluția!” în cadrul Programului Regional Sud Muntenia 2021-2027, beneficiar fiind Serviciul Public Finanțe Locale Ploiești;

Ținând cont de avizul Comisiei de specialitate nr. 1 - Comisia de buget finanțe, control, administrarea domeniului public și privat, studii, strategii și prognoze, din data de 16.04.2025;

În conformitate cu prevederile:

- Ghidului solicitantului din cadrul Programului Regional Sud - Muntenia 2021-2027 - Obiectiv de Politică 1 - O Europă mai competitivă și mai inteligentă, prin promovarea unei transformări economice inovatoare și inteligente și a conectivității TIC regionale, 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; Operațiunea B - Investiții în dezvoltarea infrastructurii, serviciilor și echipamentelor IT relevante și necesare, precum și achiziția, dezvoltarea, testarea și pilotarea soluțiilor și aplicațiilor digitale (PaaS, SaaS, etc);
- Apelul de proiecte: PRSM/473/PRSM_P1/OP1/RSO1.2/PRSM_A38;
- Hotărârea de Guvern nr. 941/2013 privind organizarea şi funcţionarea Comitetului Tehnico-Economic pentru Societatea Informaţională, cu modificările şi completările ulterioare;

Având în vedere:

- Decizia nr. 179/30.08.2024 a Autorității de Management pentru Programul Regional Sud Muntenia 2021-2027, privind aprobarea Ghidului Solicitantului “Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al organizațiilor de cercetare și al autorităților publice, prin investiții în dezvoltarea infrastructurii, serviciilor și echipamentelor IT relevante și necesare”;

- Strategia Integrată de Dezvoltare Urbană a Municipiului Ploiești 2021-2027, aprobată prin Hotărârea Consiliului Local nr. 290/25.07.2024;

În temeiul prevederilor art. 129, alin. (2), lit. b) și alin. 4), lit. d) și ale art. 196, alin. (1), lit. a) din Ordonanța de Urgență a Guvernului nr. 57/2019 privind Codul Administrativ, modificată și completată ulterior;

HOTĂRĂŞTE:

Art. 1 Anexa nr. 3 – Proiect tehnic – la Hotărârea Consiliului Local al Municipiului Ploiești nr. 158/31.03.2025 privind aprobarea documentației și a indicatorilor tehnico-economici pentru proiectul „Timpul tău e prețios, nu-l pierde la cozi și ghișee! Digitalizarea este soluția!” în cadrul Programului Regional Sud Muntenia 2021-2027, se modifică și se înlocuiește cu anexa la prezenta hotărâre.

Art. 2 Serviciul Relații Internaționale, Proiecte cu Finanţare Internaţională, O.N.G și Implementare Proiecte, Direcția Economică și Direcția Tehnic-Investiții vor duce la îndeplinire prevederile prezentei hotărâri.

Art. 3 Direcția Administrație Publică, Juridic-Contencios, Achiziții Publice, Contracte va aduce la cunoștință celor interesați prezenta hotărâre.

Dată în Ploiești, astăzi, 16 aprilie 2025

Contrasemnează:

PREȘEDINTE DE ȘEDINŢĂ,
Gheorghe SÎRBU-SIMION

SECRETAR GENERAL,
Laurențiu DIȚU

Anexa 0a HCL 175/2025

ROMÂNIA JUDEȚUL PRAHOVA CONSILIUL LOCAL PLOIEȘTI

Proiect tehnic

"TIMPUL TĂU E PREȚIOS, NU-L PIERDE LA COZI ȘI GHIȘEE! DIGITALIZAREA ESTE SOLUȚIA!"

CUPRINS

1. OBIECTIVELE PROIECTULUI

Obiectivul general

Obiectivul general al proiectului constă în valorificarea avantajelor digitalizării în beneficiul cetățenilor și al mediului de afaceri din Municipiul Ploiești prin dezvoltarea unui sistem informatic integrat și asigurarea infrastructurii hardware și software necesare pentru prestarea unor servicii publice electronice noi și semnificativ îmbunătățite de către Serviciul Public Finanțe Locale Ploiești, serviciu public cu personalitate juridică care funcționează sub autoritatea Consiliului Local al Municipiului Ploiești. Sistemul informatic integrat propus va avea rolul de a dezvolta și îmbunătăți serviciile publice electronice din perspectiva interacțiunii cetățenilor și a reprezentanților mediului privat de afaceri cu instituțiile și autoritățile publice, și anume Municipiul Ploiești și Serviciul Public Finanțe Locale Ploiești.

Obiective Tehnice

1. **Implementarea unui sistem integrat de gestionare a activității Serviciului Public Finanțe Locale Ploiești, cu includerea tuturor modulelor necesare in acest sens.**
2. **Asigurarea scalabilității si flexibilității pentru actualizări viitoare:** Proiectarea arhitecturii sistemului într-un mod scalabil, astfel încât să poată fi extins și actualizat pe măsură ce cerințele organizaționale și tehnologice evoluează, fără a necesita restructurări majore.

Concluzie

Acest proiect de digitalizare va transforma modul în care SPFL Ploiești gestionează activitatea proprie, asigurând o mai mare eficiență, transparență și adaptabilitate la cerințele moderne. Prin intermediul soluțiilor digitale propuse, SPFL Ploiești va deveni o instituție mai agilă, pregătită să răspundă nevoilor, actuale și viitoare, ale cetățenilor și companiilor din România.

2. CERINȚE PRIVIND SOLUȚIA TEHNICĂ

2.1. Cerințe generale

Soluția tehnică propusă va avea în vedere particularitățile de implementare la nivelul SPFL Ploiești, precum și funcționalitățile existente și complementare necesare.

În acest sens, analizele efectuate la nivel instituțional au condus la următoarele concluzii:

- soluția propusă să fie scalabilă din punct de vedere al capacității datelor înmagazinate, astfel încât să poată menține caracteristicile de performanță odată cu creșterea volumului de date;
- datele existente să fie importate / migrate;
- utilizarea unei arhitecturi software bazate pe standarde deschise, modulare, care să permită adăugarea de funcționalități și componente noi, precum și integrarea bidirecțională cu sisteme partenere;
- asigurarea licențelor corespunzătoare în funcție de necesități.

2.2. Prevederi de securitate

Securitatea sistemului va fi asigurată la toate nivelurile:

- la nivel fizic, accesul în sala serverelor la sisteme se va face conform politicilor de securitate stabilite la nivelul cloud-ului guvernamental. Accesul se va face în funcție de drepturi, rolul fiecărui operator și activitatea ce trebuie desfășurată;
- la nivel de server, se va folosi infrastructura din cloud-ul guvernamental astfel încât mașinile virtuale/partițiile să poată fi utilizate similar serverelor fizice, în sensul că se va permite comunicarea între două mașini virtuale/partiții doar prin canalele special definite în acest scop;
- la nivel de comunicații, prin folosirea tehnicilor specifice de izolare a traficului și implementarea de sisteme hardware și software dedicate de securitate;
- la nivel software, prin capabilitățile de securitate proprii ale componentelor software de bază și prin modalitatea de proiectare și implementare a componentelor aplicative;
- la nivel de utilizatori, prin implementarea unui sistem de gestiune a identității utilizatorilor.

Principiile care stau la baza asigurării securității cibernetice a sistemului sunt:

- **Principiul conformității** - Implementarea sistemului deține sau poate acomoda mecanisme tehnice pentru aplicarea reglementărilor naționale aplicabile (ex: GDPR) și a standardelor internaționale în vigoare privind protecția informațiilor procesate (ex: ISO).
- **Principiul optimizării costurilor** - toate investițiile necesare pentru asigurarea securității se stabilesc pe baza rezultatelor unui proces periodic de analiză a riscului.
- **Principiul responsabilități de securitate partajate** - rolurile și responsabilitățile entităților implicate în furnizarea și operarea serviciilor trebuie să fie stabilite, reglementate și asumate. Pentru implementarea măsurilor de securitate de către administratorii și beneficiarii resurselor, în concordanță cu responsabilitățile stabilite, sistemul informatic trebuie să integreze mecanisme tehnice necesare.
- **Principiul protecției informațiilor**
    a. Informațiile trebuie protejate în tranzit și în stocare împotriva accesării sau modificării de către entități neautorizate;
    b. Informațiile trebuie sa fie disponibile fără întârziere la cererea entităților autorizate.
- **Principiul securității pe întreg ciclul de viață al sistemului** - Securitatea este integrată în toate fazele ciclului de viața ale sistemului, de la analiză și proiectare până la scoaterea din uz a resurselor sau serviciilor.
- **Principiul securizării operațiunilor** - aplicarea mecanismelor pentru detectarea și prevenirea atacurilor cibernetice, prin raportare la o abordare pe niveluri pentru securizarea proceselor de furnizare a serviciilor publice din sistem.

3. DESCRIEREA TEHNICĂ A PROIECTULUI

3.1. Cerințele funcționale ale sistemului

3.1.1. Funcționalități specifice pentru Portal Servicii Publice către cetățeni și societăți comerciale (front-office)

Portalul de Servicii publice este poarta unică de acces a cetățenilor și a societăților comerciale către serviciile publice oferite de SPFL Ploiești prin intermediul acestui proiect. Serviciile publice propuse a fi oferite prin intermediul acestui portal vor fi stabilite în faza de analiză a proiectului și trebuie să faciliteze introducerea în sistemul informatic a informațiilor provenite de la public, inclusiv atașarea de documente și plata taxelor online prin integrarea cu un procesator de plați electronice. După introducerea unei cereri sau introducerea unei informații în sistemul integrat, acestea vor urma fluxuri digitale prin intermediul celorlalte module ale arhitecturii de digitalizare a SPFL, integrate cu portalul de servicii publice. Astfel se facilitează digitalizarea SPFL în relație cu cetățenii, cu mediul de afaceri și alte instituții.

Pentru facilitarea introducerii de servicii publice este nevoie ca Portalul de Servicii publice să se integreze cu sistemele ROeID și eIDAS pentru identificarea facilă a persoanelor fizice și cu ONRC, pentru obținerea facilă a datelor despre societățile comerciale.

Portalul trebuie să fie accesibil de pe orice dispozitiv conectat la internet, inclusiv computere, telefoane mobile și tablete și să ofere o experiență optimizată pentru fiecare dintre acestea, oferind capabilități multi-language. Designul trebuie să fie responsive, adaptându-se automat la dimensiunile ecranului utilizat, asigurând astfel o experiență de navigare fluentă și ușor de utilizat. Accesibilitatea trebuie să includă și respectarea normelor de accesibilitate web pentru persoanele cu dizabilități, asigurând suport pentru citirea ecranului, contrast ajustabil și navigare prin tastatură.

Portalul contribuie la principiile dezvoltării durabile prin promovarea transparenței și accesului echitabil la informații, asigurând o gestionare eficientă a resurselor și facilitând comunicarea între public și SPFL Ploiești. În plus, portalul respectă Carta drepturilor fundamentale a Uniunii Europene, oferind acces egal pentru toți utilizatorii, fără discriminare de gen, origine sau dizabilități și este conceput pentru a fi accesibil persoanelor cu dizabilități, conform art. 9 din Convenția ONU privind drepturile persoanelor cu dizabilități, respectând standardul WCAG pentru accesibilitatea web.

Cerințele de securitate sunt de asemenea fundamentale, având în vedere natura sensibilă a datelor gestionate. Portalul trebuie să implementeze un sistem robust de autentificare și autorizare. Fiecare utilizator va trebui să creeze un cont unic, iar accesul la diverse funcționalități sau informații va fi diferențiat în funcție de profilul utilizatorului (cetățean, societate comercială). Măsurile de protecție a datelor trebuie să respecte cerințele Regulamentului General privind Protecția Datelor (GDPR), iar toate comunicările între utilizator și servere vor trebui criptate prin SSL/TLS. Datele personale și comerciale vor trebui stocate în mod securizat, cu audituri periodice și mecanisme avansate de monitorizare a securității.

Interfața portalului trebuie să fie intuitivă și ușor de utilizat, cu un sistem de navigare clar și simplu. Fiecare categorie de utilizatori va avea o secțiune dedicată, cu funcționalități și informații specifice, dar toate secțiunile trebuie să fie integrate într-o structură unitară. Pentru a facilita accesul și utilizarea portalului, acesta trebuie să includă un motor de căutare intern, care să permită identificarea rapidă a informațiilor sau a

serviciilor dorite. De asemenea, trebuie să existe un sistem de asistență integrat, care să ofere suport online prin ghiduri de utilizare și o secțiune de întrebări frecvente (FAQ).

În ceea ce privește administrarea portalului, trebuie să fie prevăzut un sistem de gestionare ușoară a conținutului, care să permită actualizarea rapidă și simplă a informațiilor disponibile publicului. Administratorii portalului trebuie să aibă acces la instrumente de monitorizare a performanței platformei, rapoarte privind traficul și utilizarea funcționalităților, precum și capacitatea de a gestiona conturile utilizatorilor și permisiunile acestora.

În concluzie, acest portal va trebui să fie o platformă puternică, securizată și ușor de utilizat, care să răspundă nevoilor variate ale cetățenilor și societăților comerciale. Prin intermediul acestui portal, SPFL Ploiești va putea să ofere servicii publice moderne, accesibile și eficiente, facilitând o mai bună comunicare și cooperare între acesta și utilizatori.

Exemple de utilizare ale portalului sunt: informare/asistenta, gestionare formulare pentru prestarea de servicii electronice, primire solicitări și eliberare documente, precum și interacțiunea automată cu sistemele back-office: taxe și impozite, registratură, publicare informații.

3.1.1.1. Componenta front-office servicii online pentru acoperirea funcționalitălilor oferite in mod normal de o activitate la ghișeu

Componenta de tip front-office va avea rol de interfață cu publicul in vederea furnizării de servicii în format electronic: informare/asistență, formulare disponibile și depunerea online a documentelor la registratura instituției.

Printre serviciile electronice puse la dispoziția publicului, vor fi: depunerea și eliberarea online specializată a certificatelor fiscale, depunerea declaratiilor pentru cladiri, terenuri, mijloace de transport, depunerea de documente cu caracter general la registratura online.

Alte aspecte funcționale și non-funcționale îndeplinite prin intermediul acestei componente:

- Tehnologia utilizată va permite o afișare corectă și adaptată și pe diferite device-uri mobile (telefon mobil, tabletă, laptop);
- Va fi permisă afișarea diacriticelor limbii române;
- Vor fi disponibile mecanisme de căutare simplă/complexă;
- Pentru editarea textelor va fi folosit un editor de text de tip WYSIWYG (What-You-See-ls-What-You-Get) care permite formatarea complexă a textului;
- Va include un mecanism de recuperare a parolei;
- Va dispune de un mecanism de monitorizare și înregistrare a acțiunilor utilizatorilor;
- Accesul securizat va fi permis utilizatorilor prin intermediul unui cont bazat pe nume utilizator și parola, care are asociat un cont de e-mail pentru înregistrare;
- Oferă posibilitatea de încarcare (upload) în format electronic a documentelor;
- Permite vizualizarea documentelor incarcate deja si posibilitatea de a incarca altele;

- Ofera posibilitatea de completare si modificare a datelor personale pentru a putea fi folosite ulterior;

3.1.2. Funcționalități specifice componentei de back-office

3.1.2.1 Management al documentelor - DMS (Document management system)

Gestiunea documentelor trebuie să fie concepută pentru a menține o evidență centralizată a tuturor documentelor care intră sau ies din instituție. Prin implementarea acestui sistem se va permite alocarea automată a unui număr unic de identificare fiecărui document și distribuția sa oriunde în instituție, către compartimentul sau persoana responsabilă. Implementarea acestor funcționalități asigură o trasabilitate clară a documentelor și un control precis asupra fluxului acestora în organizație.

Funcționalitățile prevăzute a fi configurate în perioada de implementare includ înregistrarea versiunilor documentelor și păstrarea istoricului modificărilor, astfel încât să fie posibilă urmărirea fiecărui stadiu de modificare sau revizuire pe care un document l-a parcurs. În plus, controlul ciclului de viață al documentelor permite o gestionare mai eficientă a documentelor de la creare și până la arhivare, trecând prin diferitele etape de aprobare sau revizuire necesare în cadrul organizației.

Se vor defini fluxuri de lucru specifice tipurilor de documente, ceea ce înseamnă că traseul documentelor va fi configurat astfel încât să fie clar cine a avut acces la acestea, cine a introdus modificări și care sunt termenele asociate rezolvării fiecărui tip de document. Astfel, utilizatorii vor avea posibilitatea de a urmări atât parcursul documentelor, cât și acțiunile întreprinse asupra acestora de-a lungul timpului.

De asemenea, sistemul va fi configurat pentru a permite stocarea și accesul centralizat la documente prin intermediul unei interfețe web. Acest aspect facilitează o partajare rapidă a informațiilor și îmbunătățește comunicarea între angajați, oferindu-le acestora acces în timp real la documentele necesare.

Vor fi configurate drepturile de acces și acțiune în funcție de organigrama organizației și de rolul fiecărui angajat. Astfel, drepturile de aprobare, ștergere sau modificare pot fi configurate în funcție de responsabilitățile fiecărui utilizator, asigurând un control strict asupra accesului la informații. Managementul utilizatorilor, grupurilor, permisiunile, rolurile, politicile de acces, autentificarea și autorizarea vor folosi în mod exclusiv componenta de gestionare a identității.

Un alt aspect important al implementării acestui sistem este funcționalitatea de avertizare automată prin e-mail, care notifică utilizatorii atunci când le este alocată o activitate sau când se apropie termenul de rezolvare al unui document. Această funcție contribuie la o gestionare mai eficientă a timpului și la evitarea întârzierilor în rezolvarea sarcinilor.

Se vor configura registre de numere pe structuri organizatorice, ceea ce asigură o evidență clară a documentelor la nivelul fiecărui compartiment. De asemenea, se va configura și un registru de lucru specific în funcție de tipul documentelor, cum ar fi registrul general sau registrul de decizii, asigurând astfel o gestionare mai eficientă și mai organizată a documentelor în funcție de natura acestora.

Se va configura funcția de auditare a tuturor acțiunilor întreprinse în sistem, asigurând trasabilitatea completă a acțiunilor, precum cine a accesat documentele, ce

modificări au fost făcute și când au avut loc aceste acțiuni. Această funcționalitate este esențială pentru menținerea unui nivel ridicat de securitate și integritate a datelor gestionate în cadrul organizației.

3.1.2.2 Soluție software impozite și taxe locale

Modulul va contine toate funcționalitățile si procesele specifice unei institutii de stabilire, incasare si urmarire venituri la bugetul local, cu obligativitatea respectarii tuturor cerintelor legale in domeniu, inclusiv reglementarile impuse de Ministerul Finantelor pentru aplicatiile informatice și integrarea ei cu sistemul de Contabilitate Financiară a Primăriei Ploiești.

Prin proiectul curent se dorește implementarea unei aplicatii informatice care sa gestioneze pe baza rolului nominal unic toate categoriile de date si informatii existente la nivelul unei instituții ale administrației publice locale, cu specificul de lucru al SPFL Ploiești: stabilire, incasare, urmărire impozite si taxe locale. Aplicația va trebui sa răspundă cerințelor definite de toate compartimentele si sa asigure informarea corecta, completa si in timp util a factorilor de decizie.

Volumul foarte mare de date si informatii existente in compartimentele SPFL Ploiești face ca managementul datelor si informatiilor sa constituie o funcție centrala a instituției. Coordonarea si administrarea informațiilor constituie o problema strategica de importanta majora, SPFL Ploiești contribuind, prin natura activitatii, la colectarea veniturilor funcție de care se realizează sau nu, proiecția bugetului local.

Funcționalități minime:

– Sistemul trebuie sa conțină toate functionalitatile si procesele specifice unei instituții de stabilire, incasare si urmărire impozite si taxe locale cu obligativitatea respectării tuturor cerințelor legale in domeniu, inclusiv reglementările impuse de Ministerul Finanțelor pentru aplicațiile informatice;

– Aplicația va avea o arhitectura client server sau web si va putea fi administrata centralizat.

– Furnizorul trebuie sa asigure migrarea datelor existente din sistemul actual de impozite si taxe în noul sistem. Modelul de date va fi pus la dispoziție de către Beneficiar. *La finalizarea procesului de migrare furnizorul va trebui să genereze o listă cu rolurile care prezintă date eronate sau inconsistente, listă grupată pe tipuri de erori.*

– *Migrarea datelor va trebui să asigure inclusiv preluarea istoricului plăților, formelor de executare silită și modificărilor efectuate în perioada 2010-anul implementării astfel încât, ulterior migrării datelor, orice recalculare să poată fi efectuată cu respectarea prevederilor legale aplicabile în perioadele afectate de eventualele recalculări.*

– Furnizorul va trebui sa implementeze toate modificările din sistem impuse de schimbările cadrului legislativ in maxim 15 zile calendaristice de la data apariției acestora pe perioada garanției. In perioada de garanție, mentenanta si service-ul vor fi asigurate cu titlu gratuit.

– Pe durata implementării noii aplicatii nu se va perturba functionarea actualului sistem pana când acesta va fi înlocuit.

— Sistemul va asigura interfața cu SNEP (ghiseul.ro) si alti operatori economici cu care SPFL Ploiești are contract pentru realizarea de incasari de impozite si taxe (de exemplu Posta Romană, Oiwi, Printec, etc), inclusiv software-ul si licențele necesare interconectării.

— Sa aiba incorporat un generator de rapoarte care sa nu necesite intervenția furnizorului de aplicație; Generatorul trebui sa aibă ca si criterii minime de selecție și redare in conținutul raportului următoarele date : tip contribuabil, stare rol (activ, somat, insolvență, etc), debit total sau defalcat (curent, restanță, acesorii) mai mare decât „A" respectiv mai mica decât „A", tip bun detinut etc.

— Aplicatia trebuie sa fie conceputa pe baza rolului nominal unic al contribuabililor si a materiei impozabile avand posibilitatea declarării proprietăților multiple pe cote de deținere, pe clase de impozitare si la alta adresa decât aceea de domiciliu, rezultând obligatii pe fiecare proprietar/coproprietar. Aplicația trebuie sa permită adaugarea de coproprietari direct din matricola, iar la rolul nominal unic sa figureze fiecare cu cota parte deținuta din bunul impozabil, cu validare/atentionare ca suma cotelor sa fie egala cu 100 (sa nu permită utilizatorului introducerea de cote care insumate pentru matricola respectiva sa difere de 100).

— Aplicația trebuie sa permită identificarea facila a coproprietarilor si luarea in considerare a tuturor obligațiilor părților la emiterea certificatului fiscal.

— Aplicația trebuie sa permită evidențierea minim a următoarelor date de identificare sau corespondentă a contribuabililor: CNP, CUI, nume si prenume, denumire, act de identitate, sediu / domiciliu (strada, nr.postal, bloc, scara, etaj, apartament, sat, comuna, oraș, județ, tara), număr de telefon, e-mail, adresa pentru corespondenta (aceeași cu adresa de domiciliu sau alta adresa), date pe care să le preia automat în actele administrativ fiscale sau în corespondența dintre SPFL Ploiești și contribuabili.

— Aplicatia trebuie sa permită validarea CNP-ului la introducerea unui contribuabil persoană fizică in aplicație.

— Aplicația trebuie sa ofere posibilitatea unificării rolurilor de la momentul preluării (migrării datelor in forma actuala) din vechea aplicație pana la momentul realizării rolului nominal unic asa cum este definit de legislația in vigoare. In acest context va permite vizualizarea din istoric a rolurilor cu situația înainte de unificare, putând anula o operațiune de unificare eronata si revenirea la situația anterioara.

— Sa ofere pentru lucru un mecanism eficient de simulare a efectuării unor operatii pornind de la o situație existenta la un rol.

— Sa aiba istoric complet privind operațiile efectuate si datele din istoric, permițând, in cazul operării eronate, revenirea la forma inițiala sau vizualizarea acesteia, în acest sens aplicația trebuie să genereze un raport.

— Pentru gestionarea istoricului unui rol aplicația trebuie sa permită identificarea următoarelor aspecte: (istoric modificări adresa si istoric lucrări efectuate inspectori). La <istoric modificări adresa> trebuie sa fie evidențiat inspectorul care a făcut modificarea, data modificării, tipul de modificare (cnp, nume,prenume,adresa). La <istoric pentru lucrari> trebuie sa fie evidentiat inspectorul care a făcut modificarea, data modificării, iar pe fiecare cod de debit sa poata fi vizualizat istoricul complet (cladiri-suprafata,tip_cladire,tip utilitate,tip construcție,etc), teren (suprafața,etc), mijloace transport (istoric modificare tip vehicul, capacitate, serie motor, serie_sasiu).

– Aplicația trebuie să permită ca in cazul unor operări eronate sa fie posibila revenirea la forma inițiala.

– In aplicație trebuie sa poata fi cautata orice informație existenta dintr-un singur ecran care sa permită interogări după criterii multiple {ex: persoane (fizic/ juridic, nume, CNP, Cui etc.), clădiri (adresă poștală, matricola), teren (adresă poștală, matricola), auto (serie motor, serie șasiu, tip, capacitate cilindrică), plăți, somatii, documente (acte de proprietate, declaratii) după orice criteriu, iar in momentul regăsirii informației sa se poata naviga imediat la alte date legate de aceasta cerere;

– Aplicatia sa permită emiterea in bloc a deciziilor de impunere si a instiintarilor de plata la inceputul anului atât în format xls, cât si pdf direct din meniul aplicației fără intervenția furnizorului. Emiterea acestora trebuie sa fie posibila si pe coduri de debit sau după alte criterii suma debit, stare rol, etc. și în mod obligatoriu să țină cont de deciziile anterioare, oferind posibilitatea emiterii de decizii doar pentru diferențele de debit necuprinse în deciziile anterioare.

– Aplicatia sa permită emiterea in bloc a deciziilor de accesorii atât în format xls cât și pdf direct din meniul aplicației fără intervenția furnizorului. Emiterea acestora trebuie sa fie posibila si pe coduri de debit sau după alte criterii suma debit, stare rol, etc. și în mod obligatoriu să țină cont de deciziile anterioare, oferind posibilitatea emiterii de decizii doar pentru diferențele de accesorii necuprinse în deciziile anterioare.

– Tranzacțiile efectuate sa permită evidențierea lor in toate modulele la care se refera;

– Scutirile sau reducerile de impozite, trebuie reflectate prin borderouri de scădere, adica deschiderea anului fiscal se face pe toata suma datorata si imediat se aplica borderourile de scădere.

– Toate borderourile de debit generate de aplicație ca urmare a modificărilor efectuate de utilizatori, să fie reflectate într-o situație a borderourilor generate, situație pe care fiecare utilizator o generează după fiecare operațiune efectuată în vederea supunerii acestor borderouri verificării si aprobării de către șeful superior.

– Toate borderourile mai sus vor fi numerotate unic asigurându-se secvențialitatea acestora.

– Aplicația trebuie să permită emiterea proceselor verbale de contravenție, model 2016 - ITL 46, direct de pe rolul contribuabilului asigurând secvențialitatea numerelor si seriilor acestor procese verbale.

– Aplicația trebuie sa realizeze calcul automat si actualizarea informațiilor, in timp real avand viteza foarte buna in regim de lucru online cu un număr mare de roluri. Va asigura validarea datelor si calitatea introducerii acestora prin definirea câmpurilor obligatorii, a formatului acceptat, precum si prin atenționarea utilizatorului asupra incompatibilității sau contradicțiilor dintre înregistrări. Va atenționa utilizatorul in cazul datelor dublate, lipsa sau inconsistente in vederea limitării la maxim a apariției de date eronate. Trebuie sa folosească algoritmi rapizi pentru generarea/gestionarea debitelor si calculul obligațiilor, atat pentru anul fiscal curent, cât și pentru trecut.

– Aplicația va atenționa utilizatorul atunci când exista o neconcordanță între categoria de mijloace de transport selectată pentru debitare si valoarea capacitatii cilindrice a autovehiculul introdusă in baza de date de către inspector.

– Va asigura confidențialitatea, securitatea informațiilor si monitorizarea accesului la date printr-un sistem de drepturi si parole de acces la nivel de: utilizator, modul, functii, operatii;

– Trebuie sa fie parametrizabila la cel mai inalt grad astfel incat sa elimine, pe cat posibil, scrierea de programe si crearea de tabele specifice client;

– Sa permită valori inițiale pentru câmpuri prin selectare din liste sau preluare de valori de la înregistrări anterioare acolo unde acest lucru este posibil;

– Sistemul trebuie sa aiba interfața in limba romana si sa aiba asociat funcția help;

– Sa existe posibilitatea salvarii si arhivarii periodice a informațiilor din baza de date prin proceduri automate pentru acest gen de operațiuni;

– Sa permită aducerea informațiilor din arhive;

– Sa realizeze inchiderea de perioade calendaristice automat (închidere de luna, an) prin generarea de situatii legate de materia impozabila, necesare raportării veniturilor in evidenta Primăriei Municipiului Ploiești: incasari (numerar, Trezorerie, etc), debite, suprasolviri, bonificație, compensări, virări, solduri, lichidări poziții la rol etc.

– Închiderea și deschiderea anului fiscal prin generarea de rapoarte legate de materia impozabilă (clădiri, teren, auto), registrul rolurilor unice, majorări și restanțe la roluri și generarea borderoului pe debite curente, preluarea rămășițelor, majorărilor, suprasolvirilor. Funcția de deschidere an fiscal are ca scop preluarea materiei impozabile in noul an si pregătirea datelor necesare generării debitelor efectuând următoarele operațiuni: preluarea informațiilor fiscale din anul incheiat, introducere constante fiscale, debitare.

– In modulul debitare amenzi sa existe posibilitatea de a identifica procesele verbale achitate, prin orice forma (chitanța, ordin de plata, Snep, kiwi,etc) si sa nu permită debitarea acestora daca sunt deja debitate sau achitate. De asemenea, aplicația trebuie să permită modificarea oricărui camp in cazul constatării de erori in ceea ce privește debitarea amenzilor.

– Posibilitatea de a vizualiza procesele verbale pentru amenzile existente la un rol, asa cum figurează in momentul vizualizării, cele achitate prin orice forma.

– Modificările obiectelor impozabile trebuie sa se poata face retroactiv, cu ajustarea automata a nivelului creanțelor principale precum si a accesoriilor acestora. Calcularea creanțelor bugetare, în sensul majorărilor, scutirilor sau facilitatilor, pentru fiecare contribuabil în parte în funcție de încadrarea în anumite categorii. Aplicația sa permită definirea acestor parametrii pe perioada pentru care contribuabilul se încadrează în situația respectiva.

– Aplicația nu trebuie să permită compensarea automată a eventualelor suprasolviri apărute ca urmare a unor plăți eronate sau a modificărilor retroactive efectuate pe rolurile contribuabililor, suprasolvirile compensându- se numai de către inspectorii de sector. Aplicația trebuie sa permită emiterea deciziilor de compensare

– Sa se emită prin aplicație decizii de impunere, certificate de atestare fiscala, înștiințări de plata, adaptabile la legislația in vigoare;

– Sa existe un modul pentru compensări, virări si restituiri, care sa permită efectuarea acestor operațiuni, precum si un istoric al acestor operațiuni;

– Situația obligațiilor fiscale restante cu termene scadente expirate ce urmeaza a fi somate sa fie reflectate intr-o situație centralizatoare care sa poata fi identificata după mai multe criterii precum :

- sume restante cu termene scadente expirate mai mici de o anumita suma care sa poata fi inserata;
- sume restante cu termene scadente expirate la o anumita data care sa poata fi inserata;
- matricola centralizata cu toate persoanele restante indiferent de suma;
- matricola cu toate persoanele care înregistrează la data emiterii situației obligatii fiscale aflate la termenul de prescripție.

– Somația emisa prin programul informatic in funcție de criteriile de mai sus sa cuprindă toate elementele de identificare prevăzute de lege (inclusiv deciziile de impunere care stau la baza debitelor executate), iar titlul executoriu sa aiba definite natura sursei de impozitare, nominalizarea obiectului impozabil (adresa, nr. postal, etc.) cu toate caracteristicile sale, termenele scadente expirate, data emiterii, majorările calculate pana la data emiterii acesteia (cu precizarea ca accesoriile vor fi calculate pana la data platii inclusiv), totalul creanței bugetare iar pentru diferentele ramase după emiterea somației si titlului executoriu individualizarea lor sa fie posibila in aceleași condiții precizate mai sus ;

– Corelarea intre modulul de urmărire si executare silita si rolul debitorilor trebuie sa aiba in vedere orice modificări sau reglări ale situației fiscale, in sensul identificării diferentelor ramase din somație si titlul executoriu si posibilitatea emiterii unui act administrativ fiscal pe diferentele ramase in urma operării.

– După emiterea somației, sa fie individualizat automat pe rolul debitorului ca acesta este in curs de urmărire, iar după confirmarea somației si a titlului executoriu ca acesta este in curs de executare;

– Emiterea întregii documentatii de executare silita se va face prin programul informatic și va respecta întocmai prevederile legale cu privire la forma și conținutul tipizatelor utilizate în procedura de executare silită.

– Ulterior parcurgerii tuturor etapelor de executare silita care are drept consecința neidentificarea debitorului cu bunuri sau venituri urmaribile sa existe posibilitatea operării in evidente a stării de insolvabilitate a debitorului astfel:

- stare de insolvabilitate in evidenta curenta;
- stare de insolvabilitate in evidenta separata.

– In urma operării informatice a stărilor de insolvabilitate acestea sa poata fi vizualizate la rolul debitorului pe matricola/patrimoniul acestuia si calculul majorărilor de întârziere in funcție de cele doua categorii de încadrare mai sus amintite.

– Sa existe totodată si posibilitatea ca tot in categoria de stări speciale, sa fie introduse stările de insolventa, reorganizare judiciara, faliment, radiere, etc. prevăzută de mai multe reglementari legale (legea 85/2006,legea 85/2014, legea 314/2001, legea 31/1990, etc), iar operarea acestora in evidentele fiscale sa tina cont de prevederile legale in vigoare in acest domeniu fiscal. Încetarea unei astfel de stări trebuie sa poata fi operata in program, rezultând automat instituirea majorărilor de întârziere aferente reintrării in regim normal de activitate, daca e cazul.

– In momentul emiterii somației si a titlului executoriu sa se genereze automat numărul dosarului de executare, data acestuia si funcționarul operator de rol care sa poata fi identificat in registrul pf/ pj după caz, si care va trece in registru de soluționate momentul apariției acestei situatii fiscale a contribuabilului;

– In cazul in care exista mai multe roluri ale debitorilor, prin unificarea acestora sa se păstreze toate somațiile si titlurile executorii emise.

– Emiterea înscrisurilor de urmărire trebuie sa se faca la nivel de rol sau la nivel de grup de roluri după un set de caracteristici (ex.: stradal, valoric, etc.).

– Emiterea unei alte somatii trebuie sa se faca doar pentru sumele care nu au făcut obiectul executării silite.

– Descărcarea automata prin aplicație a platilor conform extrasului de cont preluat in format txt. de la trezorerie, pe fiecare plătitor in parte, conform clasificatiei bugetare și listei codurilor de debit, cu posibilitatea listării din modulul de extrase a oricăror informații;

– Aplicația trebuie sa permită gestionarea taxelor/impozitelor existente si a definirii de noi taxe si impozite fara necesitatea intervenției furnizorului, cu caracteristicile acestora: denumire, coeficienti/formule calcul, câmpuri specifice, termene de plata, observatii, etc.

– Aplicația trebuie sa ofere posibilitatea actualizării nomenclatoarelor de surse de obligatii de plata si descrierea acestora (conform legislației) fara intervenția furnizorului, actualizarea constantelor necesare calculului impozitului conform legislației în vigoare stabilita prin legi sau HCL, cu istoric pe ani, actualizarea formulelor de calcul (unde este cazul), actualizarea nomenclatorului de zone in funcție de perioada, artere, numere poștale, paritate, actualizarea nomenclatorului de artere și arondarea acestora pe zone, actualizarea arondării inspectorilor pe artere și intervale de numere, actualizarea tipului de clădiri, mijloace de transport, categorii de folosința terenuri;

– Aplicația trebuie sa permită accesul la structura datelor, cat si posibilitatea de export/import a datelor in alte formate de baze de date și integrarea cu alte sisteme, inclusiv cu noul sistem de tip DMS ce va fi implementat;

– Aplicația trebuie sa conțină rutine de validare a datelor introduse;

– Aplicația trebuie sa conțină rutine pentru verificarea consistentei si integrității datelor;

– Prin administrare sa se poata crea/suspenda utilizatori, sa se asigure generarea parolelor, acordare/suspendare drepturi de acces cu competențe pe fiecare modul si funcție in parte sau combinațiile pot da drepturi individual si la nivel de grup, cu posibilitate ca un utilizator sa faca sau nu parte dintr-un grup (EXEMPLU: utilizatorul sa poata accesa baza de date persoane fizice, persoane juridice sau combinatii (exemplu numai pf sau numai pj).

– Sesiunile de conectare ale utilizatorilor vor fi inchise după un timp de X minute.

– Sa poata audita operațiunile utilizatorilor prin vizualizarea operațiilor efectuate de utilizatorii aplicației (data modificării, utilizatorul care a făcut modificarea, modificările efectuate).

– Posibilitatea de a defini drepturi de acces de tip Read-Only pentru anumiti utilizatori.

– Aplicația va asigura posibilitatea supravegherii tuturor tranzacțiilor efectuate.

- Lucrul pe baza de date al utilizatorilor din diverse locații si consistenta datelor nu trebuie sa fie afectate de eventualele probleme de rețea (un trafic defectuos) sau alte cauze ce tin de aplicație (rulare rapoarte, accesare roluri cu un număr mare de matricole clădiri, teren,etc).

- Sa se efectueze backup complet al bazei de date in condiții de maxima siguranța si de asemenea backup zilnic al bazei de date având disponibile instrumente specializate și automate pentru acest fel de operațiuni.

- Aplicația va trebui să asigure refacerea rapidă și completă a informațiilor în caz de incidente (căderi de tensiune, deteriorări de mediu, manipulări accidentale etc.).

- Datele din sistem sa fie protejate împotriva încercărilor deliberate sau accidentale de acces neautorizat;

- Asigurarea securității tuturor interfețelor sistemului informatic, prevenind accesul utilizatorilor neautorizati la sistem;

- In cazul căderilor de sistem, toate tranzacțiile finalizate trebuie sa se regaseasca in sistem iar cele nefinalizate (datorita întreruperii accidentale a lucrului) trebuie anulate;

- Sa permită exportul datelor rezultate în urma oricărei raportări, în toate formatele enumerate : XLS, RTF, PDF, TXT, XML, DBF;

- Sa pună la dispoziție specificațiile pentru administrarea bazei de date;

- Sa prezinte flexibilitate crescută pentru adaptarea la cerințele care vor aparea;

- Sa asigure instruirea personalului care va exploata sistemul. Instruirea se va realiza inainte de intrarea in exploatare a aplicației si va include atat instruire generala pentru utilizatori cat si instruire specializata pentru administratorii aplicației (IT);

- Specialiștii IT ai beneficiarului vor fi astfel instruiti incat sa poata asigura functionarea sistemului cu o asistenta minima din partea furnizorului sau independent de contractant.

- Pe perioada utilizării aplicației, va fi nevoie de suport tehnic de la distanta pentru diagnoza si rezolvarea problemelor aparute in utilizare. Aceste servicii vor fi furnizate de către ofertant prin intermediul angajatilor sai.

- Sa furnizeze manuale de utilizare pentru aplicație la nivel de modul.

- Nota de plata cu obligațiile fiscale trebuie sa poata fi emisa in forma totala sau parțiala, in funcție de solicitarea contribuabilului. De asemenea trebuie ca în cazul amenzilor aplicația să permită casierului selectarea amenzii ce se dorește a fi plătită de contribuabil indiferent de vechimea acesteia.

- Emiterea chitanțelor in format ITL pentru pf/pj, cu sau fara rol definit (persoane care nu au domiciliul in localitate), cu sau fara debit;

- Emiterea borderoului de incasari pe casieri sau centralizat, zilnic sau pe o perioada, numerar/POS sau după alte criterii.

Rapoarte:

- Raport privind creanțele bugetului local pentru veniturile stabilite prin declarație fiscala (la deschidere an), pe conturi, conform clasificatiei bugetare;

– Raport - rulaj majorare si diminuare creanțelor conform declarațiilor de impunere depuse de contribuabil;

– Raport - rulaj incasari: virament, numerar, etc (din anul curent);

– Raport - rulaj incasari din an curent, ramasita si accesorii;

– Raport - rulaj bonificație acordata, compensări SSV (+/-), virări plati an curent (+/-, suprasolviri;

– Raport - rulaj facilitati acordate in baza cererilor;

– Raport - rulaj stingeri de creanțe pe alte cai (din anul curent si din anii precedenti);

– Raport - rulaj restituiri din plati an curent si din suprasolviri ani precedenti;

– Registrul veniturilor, centralizat pe conturi de trezorerie, conform clasificatiei bugetare;

Managementul declarațiilor online privind bunurile mobile

– documentele și datele descriptive asociate pentru declararea/modificarea/scoaterea din evidență de bunuri mobile vor fi depuse online prin intermediul unui serviciu public;

– solutia informatica va prelua datele necesare calculului impozitelor si taxelor locale din declaratia completata on-line de contribuabil, va transfera aceste date in aplicatie in vederea validarii acestor date de catre angajatii SPFL Ploiești; In urma validarii acestor date aplicatia va instiinta contribuabilul despre validarea datelor si va calcula impozitele datorate fara a mai fi necesar ca datele sa fie reintroduse in aplicatia de impozite si taxe;

– Soluția informatică va asigura preluarea automată si transferarea in aplicatia de impozite si taxe, a declaratiilor fiscale generate automat in urma scanarii cartii de identitate a vehiculului de catre contribuabil, privind mijloacele de transport prevazute in titlul IX "Impozite si taxe locale" din Codul Fiscal.

– in urma solicitarii online a scoaterii din evidenta a unui mijloc de transport de catre contribuabil se va genera automat si declaratia de scoatere din evidenta a mijloacelor de transport pe baza datelor existente in baza de date.

Identificarea contribuabililor la ghiseu prin scanarea documentelor de identitate

Prin intermediul componentei de scanare, recunoastere si inregistrare documente de identitate ale contribuabililor vor fi optimizate fluxurile specifice interactiunii cu publicul, atat in ceea ce priveste identificarea persoanei care se prezinta la ghiseu, cat si preluarea automata a informatiilor relevante pentru procesele asociate profilului de contribuabil aplicabil. Solutia va permite de asemenea validarea si interpretarea automata a unei game largi de documente de identitate (Carte de identitate/Pasaport/etc) conform standardelor ICAO/PRADO la nivel international, facilitand astfel interactiunea inclusiv cu cetateni straini ce pot avea obligatii de plata relevante.

Componentele solutiei

– Scanner: este dispozitivul care realizează activitatea de scanare prin: OCR, validarea elementelor de securitate si descifrarea zonelor MRZ si a cip-urilor de pe documentele de identitate.

– Server local: stație de lucru locala pe care se vor instala driverele scanerului si agentul local de monitorizare API. Scannerul va fi conectat prin cablu sau wireless la acest server local.

– Agent local de monitorizare API: componenta rezidenta pe serverul local, prin intermediul căreia se vor prelucra datele scanate si comunicate de către scaner. Aceste date sunt comunicate către serverul central.

– Stații de lucru: este orice stație de lucru pe care lucrează operatorii. Acestea vor avea acces la aplicația de scanare prin intermediul rețelei interne (intranet) sau retelei globale (internet). Din interfața aplicatiei de scanare, operatorul va selecta un scaner disponibil din locație. Conectarea stațiilor de lucru la serverul local se face prin LAN-ul local.

– Aplicatia de scanare: aplicație web, instalata pe un server central, care oferă un mediu prietenos si intuitiv de lucru utilizatorilor in vederea scanarii documentelor de identitate prin intermediul scannerului selectat.

– Componenta de administrare: modul de administrare a aplicației de scanare, prin intermediul căruia se gestionează relațiile utilizator/locație/scaner, statusul scanerelor, activarea si dezactivarea anumitor funcționalități din aplicație, gestionarea nomenclatorului tip operațiune, precum si istoricul tuturor actiunilor efectuate de catre utilizatori.

– Serviciu de auto-inregistrare: serviciu rezident pe masinile de tip „server local", ce verifica conectivitatea statiei cu un dispozitiv de scanare si efectueaza automat inregistrarea unui scanner nou, la detectia prezentei acestuia.

– Baza de date: în cadrul bazei de date sunt stocate informații precum date utilizatori, metadate asociate documentelor scanate

– Api-uri de comunicare: componenta de preluare a datelor unei scanari din aplicatia de scanare si comunicare către endpoint-uri externe.

3.1.2.3 Solutie call center avansat cu Inteligenta artificială

Call center-ul avansat cu Inteligenta artificială este o soluție avansată de call center pentru limba română, care îmbină tehnologia modernă cu inteligența artificială pentru a oferi servicii eficiente și personalizate cetățenilor vorbitori de limba română.

Componentele și funcționalitățile esențiale sunt:

Componente principale:

1. Hub central de control: Gestionează comunicarea între toate componentele și coordonează operațiunile.
2. Sistem de distribuție automată a apelurilor (ACD): Direcționează apelurile către agenții potriviți în funcție de criterii predefinite.

3. Sistem de răspuns vocal interactiv (IVR): Oferă un meniu vocal în limba română pentru ghidarea inițială a apelanților.
4. Platformă de inteligență artificială: Integrează capabilități de procesare a limbajului natural și învățare automată pentru limba română.

Funcționalități minime:

1. Sistem interactiv de răspuns vocal (IVR)
   - Oferă informații de bază și rezolvă probleme comune
   - Transferă apelurile complexe către agenți umani
2. Rutarea inteligentă a apelurilor
   - Direcționează apelurile către agenții cei mai potriviți în funcție de competențe și disponibilitate
   - Prioritizează apelurile în funcție de urgență și istoricul clientului
3. Recunoașterea și procesarea vorbirii în limba română
   - Transcrie automat conversațiile în text
   - Analizează tonul și sentimentul apelantului
   - Identifică cuvinte cheie și intenții
4. Automatizarea sarcinilor post-apel
   - Generează automat rezumate ale conversațiilor
   - Actualizează baza de date cu informații relevante
5. Analiza și raportare avansată
   - Generează rapoarte detaliate despre performanța call center-ului
   - Oferă insights despre tendințele clienților și ariile de îmbunătățire
6. Suport pentru munca la distanță
   - Permite agenților să lucreze de acasă cu acces complet la toate funcționalitățile
7. Integrare omnichannel
   - Sincronizează comunicarea între telefon, email, chat și rețele sociale
   - Oferă o experiență unitară clientului, indiferent de canalul ales
8. Securitate și conformitate
   - Asigură criptarea datelor și respectarea reglementărilor GDPR
   - Oferă funcții de monitorizare și înregistrare a apelurilor pentru control al calității
9. Inovație tehnologică continuă

Soluția va include toate licențele necesare pentru funcționare, inclusiv căști audio de tip call-center, nefiind nevoie de a se licenția alte module din soluție / alte terțe părți.

3.1.2.4 Funcționalități specifice componentei de contorizare folosire servicii publice

Pentru că acest proiect este propus a fi depus cu o cerere de finanțare pe 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, iar în ghidul de finanțare al acestui program este prevăzut ca indicator de rezultat obligatoriu "Utilizatori de servicii, produse și procese digitale publice noi și optimizate RCR11 - nr utilizatori/an", iar în cadrul auditurilor pe perioada de sustenabilitate a proiectului, este nevoie ca SPFL Ploiești să asigure crearea unei modalități facile de probare și contorizare a utilizatorilor care face obiectul acestui indicator.

Practic, acest modul va contoriza fiecare accesare de către utilizatori a serviciilor publice noi sau optimizate/actualizate semnificativ create prin intermediul acestui proiect. Prin utilizatori se înțelege clienții serviciilor, produselor publice digitale noi sau optimizate/actualizate semnificativ, precum și personalul instituțiilor publice care le utilizează.

Contorizarea folosirii serviciilor publice se va implementa folosind Soluția Portal.

3.1.3. Funcționalități specifice componentei de integrări externe și preluări de date

Un sistem informatic modern trebuie să fie capabil să preia și să transmită date către alte sisteme informatice, iar pentru acest lucru este nevoie de componente specializate care să poată să facă managementul acestor integrări și să asigure securitatea necesară. Se va încerca ca toate aceste integrări să se facă pe baza de API, în condițiile în care sistemele informatice corespondente o vor permite tehnic.

La acest moment au fost identificate următoarele integrări și surse de date necesare pentru operaționalizarea sistemului:

- PSCID-ROeID - pentru identificarea persoanelor fizice care interacționează cu serviciile publice. Cerințele tehnice privind interconectarea cu alte platforme are ROeID sunt disponibile la https://github.com/roeid-ro/integrare;
- Nodul eIDAS - pentru integrarea cu sistemele de identitate digitală din alte țări; detalii la https://eidas.gov.ro/;
- Sistemul național informatic de evidență a persoanelor, prevăzut în Ordonanța de urgență a Guvernului nr. 97/2005 privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români, republicată, cu modificările și completările ulterioare;
- Platforma Națională de Interoperabilitate (PNI) - viitorul sistem guvernamental, cf lg. 242/2022, care va asigura interoperabilitatea sistemelor informatice guvernamentale în România, pentru a trimite și primi date de la sistemele înrolate în acest sistem, dacă va fi implementat până la momentul implementării acestui proiect;
- Punctul de Contact Unic electronic sau Portalul Digital Unic din România (care dintre ele va fi disponibil la momentul implementării) - integrare necesară pentru punerea la dispoziție către acest sistem informatic a serviciilor publice electronice puse la

dispoziție de SPFL pentru punerea în aplicare a Regulamentului (UE) 2018/1724 și a aplicării principiului once-only;

- Platforma de Jurnalizare și Notificare (PJN) - Datele tranzacționate prin PNI vor fi jurnalizate prin Platforma de Jurnalizare și Notificare (PJN) și fiecare cetățean va putea fi informat/notificat atunci când datele sale sunt accesate, dacă va fi implementat PJN până la momentul implementării acestui proiect;
- Oficiul Național de Registru al Comerțului - pentru identificarea și extragerea informațiilor privind persoanele juridice supuse înregistrării în Registrul Comerțului;
- Ghiseul.ro - pentru efectuarea plăților pentru serviciile publice furnizate;
- Sistemul financiar contabil al Primăriei - integrare prin API Rest.

Pentru ca aceste integrări să fie posibile, este nevoie ca SPFL Ploiești să deschidă dialogul instituțional cu toate aceste instituții și să inițieze semnarea unor protocoale de colaborare, fără de care aceste integrări nu vor fi posibile sau să beneficieze de platforma PNI și să realizeze integrările prin acest cadru. Unele dintre sistemele enumerate mai sus sunt în curs de implementare la nivel guvernamental, integrarea cu ele se va face in măsura în care implementările vor fi finalizate până la finalizarea documentațiilor de tip caiet de sarcini ale acestui proiect. Sistemul va asigura respectarea standardelor de interoperabilitate prevăzute în NRRI (Ordinul MCID nr. 21286 din 26.10.2023) și Legea nr. 242/ 2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate (înlocuirea protocoalelor de transfer direct a datelor intre instituții cu mecanismele de transfer prin Platforma Națională de Interoperabilitate).

3.1.4. Servicii de implementare

3.1.4.1. Servicii de implementare IT

Analiza și proiectare

- Realizarea unei analize detaliate a cerințelor funcționale și tehnice pentru toate soluțiile propuse.
- Identificarea fluxurilor de lucru existente și proiectarea soluțiilor pentru a optimiza aceste procese.
- Elaborarea unui plan detaliat de implementare, incluzând etapele proiectului, termenele, resursele necesare și responsabilitățile părților implicate.
- Definirea arhitecturii tehnice, inclusiv integrarea soluțiilor software și hardware propuse.

Instalare și configurare hardware

- Achiziția și instalarea echipamentelor hardware, inclusiv calculatoare, echipamente de rețea și alte dispozitive necesare conform acestui proiect tehnic.
- Configurarea infrastructurii hardware pentru a susține funcționarea optimă a soluțiilor implementate.
- Implementarea unei rețele WiFi și cablări structurate, care să respecte standardele actuale de conectivitate și securitate.

Serviciile de cablare structurată la nivelul sediului central al SPFL Ploiești (clădire dispusă pe 4 niveluri: subsol, parter, 2 etaje) și la nivelul sediului secundar (clădire dispusă pe 2 niveluri: parter și 1 etaj). Activitățile necesare sunt:

- Planificare și proiectare:
  - Analiza spațiilor fizice și identificarea cerințelor specifice pentru rețea cablată și WiFi.
  - Elaborarea unui proiect detaliat care include traseele cablurilor, pozițiile echipamentelor de rețea și punctele de acces WiFi.
- Furnizare și instalare materiale:
  - Achiziționarea și instalarea cablurilor, panourilor de conexiuni (patch panels), prize de rețea și echipamentelor active (switch-uri, routere, puncte de acces WiFi), conform proiectului tehnic.
  - Utilizarea de cabluri și echipamente care respectă standardele actuale (ex. cabluri Cat 6 sau superioare).
- Montaj și configurare:
  - Instalarea și fixarea cablurilor în trasee sigure, utilizând canale dedicate pentru protecție.
  - Configurarea echipamentelor active pentru rețea cablată și WiFi, asigurând conectivitatea optimă.
- Testare:
  - Testarea fiecărui traseu de cablu pentru continuitate, pierderi de semnal și viteză.
  - Validarea acoperirii semnalului WiFi și ajustarea parametrilor pentru o acoperire uniformă.

În ceea ce privește rețeaua structurată și WiFi

- Rețea structurată:
  - Trebuie să permită transferuri de date la viteze ridicate.
  - Să fie scalabilă, cu posibilitatea de a adăuga noi echipamente sau utilizatori.
- Rețea WiFi:
  - Trebuie să acopere uniform toate spațiile de birouri și zonele publice.
  - Să suporte standardele actuale pentru viteze mari și capacitate crescută.
  - Să includă funcționalități de securitate avansate, cum ar fi autentificare prin certificate sau parole unice pentru utilizatori.
  - Să permită management centralizat pentru monitorizarea performanței și gestionarea punctelor de acces.

Instalarea și configurarea software în Cloud-ul Guvernamental

- Instalarea și configurarea tuturor soluțiilor software incluse in proiectul tehnic, inclusiv aplicația de impozite și taxe locale, sistemul de management al documentelor, portalul cetățenilor, call center, soluția de e-learning, soluțiile de securitate cibernetică, etc.
- Integrarea aplicațiilor software cu infrastructura hardware a Cloud-ului Guvernamental și cu sistemele SPFL Ploiești deja implementate.
- Asigurarea configurării inițiale și personalizării soluțiilor conform cerințelor SPFL.
- Configurarea mediului cloud pentru a susține toate aplicațiile, respectând cerințele de performanță și securitate.
- Realizarea efectivă a migrării datelor și instalarea în cloud și validarea funcționării acestora după instalarea lor și migrarea datelor.

Testare și validare

- Testarea tuturor soluțiilor implementate pentru a verifica funcționalitatea, performanța și integrarea corectă a acestora.
- Realizarea testelor de securitate pentru a asigura protecția datelor și a sistemelor.
- Validarea soluțiilor implementate conform cerințelor funcționale și tehnice definite în etapa de analiză.

Instruire

- Organizarea sesiunilor de instruire pentru personalul SPFL Ploiești privind utilizarea soluțiilor software și hardware implementate.
- Furnizarea de manuale de utilizare și ghiduri pentru a facilita adoptarea rapidă a noilor soluții.
- Crearea unor resurse educaționale pentru utilizatorii finali ai portalului cetățenilor.
- Operaționalizarea soluției de e-learning pentru angajații SPFL și înregistrarea lecțiilor video specific soluției implementate.

Garanție și mentenanță

- Oferirea de suport tehnic în perioada de implementare și post-implementare.
- Asigurarea unui serviciu de garanție și mentenanță pentru toate soluțiile hardware și software pe o perioadă de minimum 36 luni conform cerințelor.

Cerințe de securitate

- Furnizorul trebuie să implementeze soluții avansate de protecție, incluzând firewall-uri, soluții antivirus și sisteme de detectare a intruziunilor.
- Protecția datelor personale și conformitatea cu legislația GDPR trebuie să fie garantate prin toate soluțiile implementate.

3.1.4.2. Servicii migrare date

3.1.4.2.1. Migrarea datelor din aplicațiile existente în noua aplicație de tip Document Manager System (DMS)

Migrarea documentelor din aplicațiile existente (ELO, Atlas) către noul sistem de tip Document Management System (DMS) reprezintă o etapă critică în procesul de implementare. Este esențial ca toate documentele să fie transferate complet, corect și să fie accesibile în noul sistem conform cerințelor organizaționale și legale. Volumul de date care trebuie migrat este de aproximativ 1Tb de documente. Modelul de date va fi pus la dispoziție de către Beneficiar.

Obiectivele migrării

- Asigurarea transferului complet și corect al tuturor documentelor din sistemele existente.
- Păstrarea integrității datelor și a metadatelor asociate documentelor.
- Verificarea funcționalității documentelor migrate în noul sistem DMS.
- Minimalizarea timpului de indisponibilitate și a impactului asupra activității organizației.

Activități Necesare:

Analiza sistemului existent

- Realizarea unei analize detaliate a structurii aplicațiilor, incluzând:
    - Identificarea volumului de documente de migrat.
    - Evaluarea tipurilor de fișiere (începând de la formate standard, precum PDF, DOCX, și imagini, până la fișiere specifice aplicației).
    - Documentarea structurii folderelor și a metadatelor asociate.
    - Verificarea regulilor de acces și permisiunilor utilizatorilor din sistemul existent.

Proiectarea procesului de migrare

- Definirea unei strategii de migrare care să includă:
    - Etapele procesului de migrare.
    - Tehnologia și instrumentele utilizate pentru extragerea și importul documentelor.
    - Planul de gestionare a riscurilor asociate migrării (ex. pierderea de date, incompatibilitatea formatelor).
    - Procedura de validare a migrării.
- Crearea unui plan de backup pentru documentele existente în sistemele existente.

Extragerea datelor

- Extragerea documentelor din sistemele existente, incluzând:
  - Exportarea fișierelor în formatele lor originale.
  - Exportarea metadatelor asociate (nume, date de creare, autori, etichete, permisiuni, etc.).
  - Asigurarea că toate datele sunt complet exportate și structurate logic.

Transformarea și maparea datelor

- Realizarea conversiei formatelor de fișiere, dacă este necesar, pentru compatibilitatea cu noul sistem DMS.
- Maparea metadatelor din sistemele existente la structura de metadate definită pentru noul DMS.
- Aplicarea regulilor de securitate și permisiuni în funcție de cerințele organizaționale.

Importul datelor în noul sistem de tip DMS

- Importarea documentelor și a metadatelor asociate în noul sistem DMS.
- Asigurarea corectitudinii ierarhiei folderelor și a structurii organizaționale a documentelor.
- Configurarea permisiunilor utilizatorilor și a politicilor de acces pentru documentele migrate.

Verificarea și validarea migrării

- Verificarea completitudinii documentelor:
  - Compararea volumului de documente din sistemele existente cu cel din noul DMS.
  - Confirmarea prezenței tuturor fișierelor și metadatelor esențiale.
- Testarea funcționalității documentelor migrate:
  - Deschiderea și vizualizarea documentelor.
  - Validarea metadatelor asociate (ex. date corecte de creare, autor, etichete).
- Testarea politicilor de acces și permisiunilor.

Gestionarea erorilor

- Identificarea și rezolvarea erorilor apărute în procesul de migrare.
- Crearea unui raport detaliat al erorilor și a acțiunilor corective.

Validarea finală

- Organizarea unei sesiuni de validare cu echipa SPFL pentru a confirma corectitudinea și completitudinea migrării.
- Obținerea acordului formal pentru finalizarea procesului de migrare.

Măsuri de asigurare a calității

- Implementarea unui sistem de audit pe tot parcursul procesului de migrare.
- Documentarea și raportarea fiecărei etape a procesului către factorii de decizie.

3.1.4.2.2. Migrarea datelor din format letric în format digital

Migrarea datelor din format letric prin conversie digitala va viza pe de o parte realizarea unor copii fidele electronice ale documentelor din arhiva fizica, precum si atasarea acestora de campuri cheie, esentiale pentru regasirea ulterioara a documentelor in noul depozit electronic.

Obiective:

- Cresterea eficientei operationale: Simplificarea si accelerarea procesului de accesare si gestionare a informatiilor din arhiva.
- Transparenta: Crearea unui sistem accesibil si transparent pentru contribuabili, facilitand accesul la informatii relevante.
- Sustenabilitate: Reducerea utilizarii hartiei si contributia la protejarea mediului.
- Securitate: Protejarea datelor sensibile prin implementarea unor solutii digitale moderne si securizate.

Beneficii:

- Eficienta crescuta
- Reducerea timpului de cautare a documentelor
- Automatizarea proceselor administrative
- Costuri reduse pe termen lung
- Eliminarea costurilor de Intretinere a arhivelor fizice (spatiu, consumabile, Intretinere)
- Reducerea erorilor administrative cauzate de gestionarea manuala a documentelor
- Accesibilitate sporita
- Permite accesul rapid la informatii pentru angajati, cetateni si alte entitati
- Posibilitatea extinderii unor servicii online pentru contribuabili
- Protectie si siguranta a datelor
- Reducerea riscului de deteriorare, pierdere sau furt al documentelor fizice
- Backup automat si protectie cibernetica avansata
- Imbunatatirea imaginii institutiei
- Alinierea cu tendintele de modernizare digitala ale administratiei publice.

Conversia digitala va viza o volumetrie de aproximativ 3.000.000 pagini ce cuprinde documente preponderent de format A4 si un procent mic de documente de format mai mare (planuri format A2; A1) sau format atipic, mai mic de A4. Tinand cont de volumetria identificata, precum si de nivelul de calitate obtinut anterior in efortul sustinut in directia conversiei digitale al institutiei, se va avea in vedere scanarea documentelor la o rezolutie de 300 dpi, color, cu echipamente profesionale, de mare viteza. In ceea ce priveste documentele de format A2-A1, vor fi necesare echipamente de scanare format mare, planuri.

In etapa de clasificare si culegere cuvinte cheie a documentelor se vor avea in vedere urmatoarele activitati:

- Clasificarea documentelor electronice obtinute prin captura de date
- Atasarea de cuvinte cheie conform tipului de document. Pentru exemplificare, in cazul documentele auto se vor avea in vedere culegerea urmatoarelor cuvinte cheie: Serie Sasiu, Marca autovehicul, CNP. Pe langa aceste cuvinte cheie, fiecare document va avea atasata informatie cu privire la mapa/cutia fizica in care se regaseste corespondentul in format letric. Pentru toate categoriile de documente ce vor intra in procesul de conversie digitala s-a identificat necesitatea unui numar de 3 cuvinte cheie cu privire la continutul documentului, la care se adauga informatia de legatura cu documentul letric (cod unic de bare).

Rezultatul conversiei digitale si anume, colectia documentelor electronice va fi importata in sistemul centralizat de management de documente, completand astfel depozitul unic si centralizat de date al institutiei.

3.2. Arhitectura funcțională a sistemului

Sistemul propus presupune implementarea unui sistem informatic nou găzduit în Cloud-ul Guvernamental, Cloud-Native, actualizat la nivelul de evoluție tehnologică, cu o securitate informatică sporită, accesibil prin intermediul browser-elor web. Sistemul va fi compatibil din punct de vedere tehnic cu serviciile de stocare în cloud și cu serviciile de baze de date din cloud și va fi compatibil cu tehnologii de containerizare.

La proiectarea, realizarea și implementarea sistemului informatic, se va ține cont de următoarele principii generale:

- **Principiul legalității**: care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- **Principiul divizării arhitecturii pe nivele**: constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
- **Principiul arhitecturii bazate pe servicii**: constă în distribuirea funcționalității aplicației în unități mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic;
- **Principiul datelor sigure**: stipulează introducerea datelor în sistem doar prin canale autorizate și autentificate;

- **Principiul securității informaționale**: presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și acces nesancționat;
- **Principiul transparenței**: presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
- **Principiul expansibilității**: stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
- **Principiul scalabilității**: presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;
- **Principiul simplității și comodității utilizării**: presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor Sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
- **Principiul integrității, plenitudinii și veridicității datelor**: presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business ale sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte dintr-un sector concret al sistemului informatic.

Soluția va permite interoperabilitatea cu alte sisteme publice existente/viitoare. Toate activitățile tehnice privind integrarea cu aceste sisteme vor fi în sarcina viitorului prestator. Sistemul va fi, după caz, fie furnizor, fie consumator de date în raport cu sistemele altor instituții publice, permițând fie preluarea de date necesare, de exemplu din alte registre de bază, fie furnizarea de date către sistemele altor instituții publice pe bază de API. Categoriile de informații care vor fi folosite de către sistem din sistemele altor instituții publice se vor determina în etapa de analiză și proiectare.

Soluția va permite distribuția seturilor de date către alte instituții guvernamentale pe baza permisiunii de acces. Seturile de date disponibile terților vor fi stabilite în perioada de analiză a sistemului IT. De asemenea, sistemul va permite exportul de date ca date deschise spre portalurile dedicate, cu metadatele aferente.

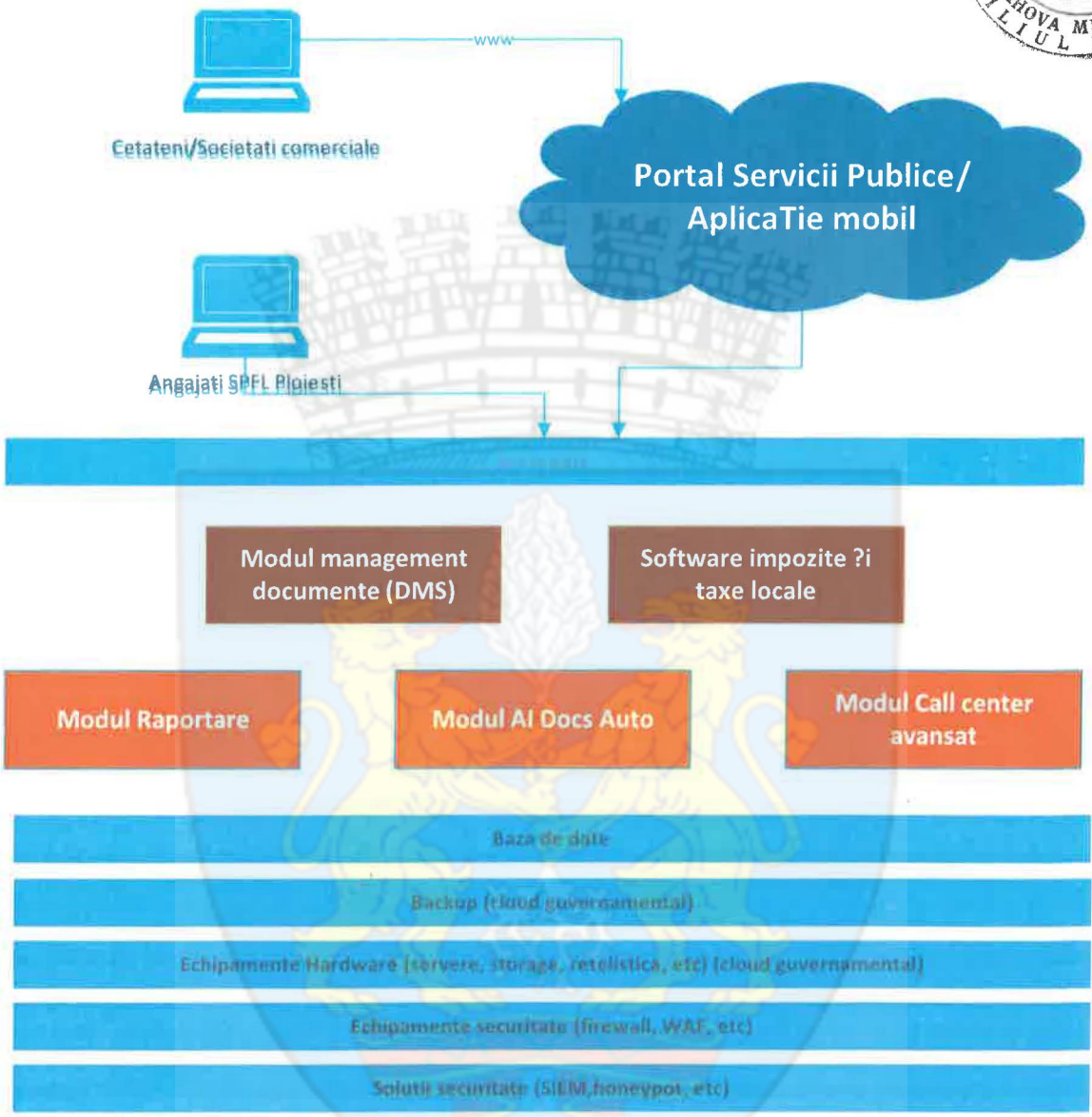
Sistemul va permite exportul de date (anonimizate după caz) pentru publicare ca date deschise pe portalul național sau portal de date deschise specific, în formate deschise, standardizate, cu metadatele aferente prin intermediul unui API.

Pentru serviciile, datele și documentele puse la dispoziție vor fi respectate standardele tehnice de interoperabilitate pentru modelele de date în conformitate cu standardele și practicile europene stabilite de Centrul European de Interoperabilitate Semantică - SEMIC.EU, prevăzute în Ordinul 21286 din 26.10.2023.

Modelele de date (logic și fizic) pentru sistemul integrat vor fi realizate în etapa de analiză și proiectare a sistemului.

Toate produsele și serviciile software de tip antivirus achiziționate prin intermediul acestui proiect vor respecta legea 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei.

Dispunerea componentelor funcționale și logice este reprezentată schematic în diagrama următoare:



3.2.1. Componente software de bază

3.2.1.1. Platformă de server web / reverse proxy

Server-ele web vor permite prezentarea conținutului sistemului către utilizatori și transferul de date dinspre client spre sistem prin intermediul browser-elor web. În același timp, server-ele web vor asigura primul nivel de securitate software din punct de vedere al accesului - configurare în mod reverse proxy.

Aceasta va oferi următoarele capabilități:

- va permite accesarea aplicației din browsere tradiționale (Microsoft Edge, Mozilla Firefox, Opera, Safari, Google Chrome etc.), cât și de pe dispozitive mobile Android, IOS, Microsoft;
- va asigura prin componentele software ale server-ului web funcționarea în cluster pentru a asigura balansarea încărcării și disponibilitatea maximă a aplicației;
- va dispune de funcționalități de rescriere a adreselor URL.

Platforma server web va putea rula pe toate distribuțiile majore de sisteme de operare prezente pe piață: Microsoft Windows, Linux.

3.2.1.2. Soluție pentru rularea aplicațiilor - Server de aplicații

Componenta software a serverelor de aplicații va trebui să ofere suport pentru asigurarea infrastructurii software necesară execuției aplicațiilor moderne bazate pe standarde deschise. Serverul de aplicații va asigura un set de servicii standard pe care toate aplicațiile dezvoltate și instalate să îl poată accesa și utiliza:

- servicii de clusterizare pentru o scalabilitate și disponibilitate ridicată;
- servicii de balansare și dirijare a încărcării;
- servicii de securitate pentru protejarea resurselor găzduite;
- servicii de definire și context de execuție pentru resursele de aplicație: conexiuni către baze de date relaționale;
- servicii de manipulare a datelor în format XML;
- servicii de management al tranzacțiilor la nivelul aplicației.

Pentru a asigura înaltă disponibilitate, soluția va include mecanisme de grupare a serverelor de aplicație în clustere în topologii de tip activ-activ, respectiv stoparea temporara a unui nod din cluster pentru mentenanță și suport, sistemul în acest timp fiind disponibil pentru activități normale.

Componenta server de aplicație va permite rularea serverului de aplicații pe sistemul de operare avut în vedere la definirea soluției.

Componenta server de aplicație va permite folosirea în conjuncție cu un cluster de servere proxy pentru serverele de aplicație în scopul realizării administrării traficului de date dintre serverele de aplicație având capabilități de balansare, caching, reverse-proxy.

Componenta server de aplicație va asigura funcționarea aplicației pe care o rulează în mod balansat între servere, cu continuarea sesiunii utilizatorului atât timp cât cel puțin un server din cluster este funcțional.

3.2.1.3. Sisteme de operare

Sistemele de operare vor asigura infrastructura software pentru rularea serviciilor și vor fi compatibile cu componenta de server de aplicații și cu platforma de server web. Sistemele de operare server vor oferi capabilități de virtualizare, capabilități de configurare cloud ready. Sistemele de operare:

- vor asigura un nivel ridicat de scalabilitate și fiabilitate;
- vor fi compatibile cu componentele software care vor rula pe acestea;
- vor rula pe 64 de biți;
- vor oferi suport pentru IPv6;
- vor putea fi configurate în topologii de tip cluster.

La implementare, din motive de securitate, serviciile care nu vor fi folosite la nivelul sistemelor de operare vor fi dezactivate.

3.2.1.4. Soluție de implementare servicii de directoare

În acest moment, la nivelul instituției este implementat un serviciu de directoare de tip Active Directory - Windows Server 2008 pentru 100 de conturi de utilizatori (Microsoft Windows Sever 2008 R2 CAL - 100 buc.).

Soluția viitoare va asigura implementarea de servicii de directoare bazate pe LDAP care să permită stocarea informațiilor despre obiectele din rețea și care să faciliteze regăsirea și utilizarea acestor informații de către administratori și utilizatori. Informația va putea fi organizată în mod ierarhic. Serviciul de directoare va asigura suport pentru minim 145 de conturi de utilizatori și va implica migrarea serviciului AD existent și extinderea până la noul număr de conturi utilizatori.

3.2.1.5. Soluție bază de date

Sistemul de gestiune al bazelor de date relaționale principal va fi un sistem de administrare a bazelor de date de tip relațional, va fi disponibil comercial (COTS - Commercial off the Shelf) și va oferi posibilitatea de a rula pe diverse platforme hardware, precum și pe sistemele de operare majore existente pe piață (Windows, Linux și Unix).

Dacă pe lângă acest sistem de baze de date principal care va fi achiziționat în cadrul proiectului vor exista componente care necesită și alte sisteme de gestiune a bazelor de date (de exemplu baze de date noSQL), implementatorul va avea obligația de a livra și implementa orice sistem de gestiune de baze de date suplimentar care să asigure funcționarea soluției, având și obligația de a integra bazele de date respective după cum va fi necesar.

Pentru a răspunde cerințelor de funcționalitate și performanță cerute, sistemul de baze de date relaționale principal va prezenta următoarele capabilități generale:

- va fi compatibil cu standardul ANSI SQL;
- va oferi suport Unicode UTF-8 sau echivalent;
- va oferi suport pentru date de tip multimedia, geo-spațiale și de tip graf;
- va permite nativ stocarea și gestiunea de structuri de date de tip XML și JSON;

- va oferi suport pentru proceduri stocate și triggeri;
- va permite accesul cât mai rapid la informații prin utilizarea diferitelor tipuri de indecși, cum ar fi B-Tree, function based, domain sau similari;
- va permite definirea de tabele de tip index pentru acces rapid la anumite tabele;
- va oferi suport complet pentru folosirea de expresii regulate, funcții analitice și algoritmi de machine learning;
- va oferi posibilitatea de interogare direct din baza de date a fișierelor text externe, fără a necesita în prealabil o operațiune de încărcare într-o tabela din baza de date;
- va permite definirea de tabele de tip index pentru acces rapid la datele din anumite tabele;
- criptarea transparentă a datelor stocate se va putea face atât la nivel de coloană, tabelă, cât și la nivel de fișier de date și va suporta cel puțin următorii algoritmi de criptare: 3DES (minim 168 bit) și AES (minim 256 bit);
- va permite criptarea transparentă, fără a necesita modificarea aplicațiilor, a informațiilor vehiculate în timpul sesiunilor între utilizatori/aplicații și baza de date folosind atât algoritmii criptografici AES și 3DES cât și protocoale criptografice specifice - SSL/TLS;
- va include capabilități de mascare transparentă, parțială sau totală la nivel de coloană, a datelor returnate utilizatorilor sau aplicațiilor, dacă aceștia nu sunt autorizați să le vizualizeze integral;
- va oferi posibilitatea autentificării utilizatorilor pe baza de certificate digitale;
- va permite restricționarea accesului la nivelul obiectelor bazei de date;
- va oferi o lista cu operațiile pe care un grup sau o clasa de utilizatori le poate executa;
- va permite operațiuni de backup și restaurare a datelor în regim de lucru online;
- va oferi posibilitatea de a realiza copii de siguranță (backup-uri) ale bazei de date și restaurarea acestora în mod incremental;
- va oferi mecanisme integrate în baza de date pentru recuperarea datelor modificate de o tranzacție care a fost comisă, fără a fi necesara întreruperea activității pe baza de date, restaurarea datelor dintr-un backup sau întreținerea prin proceduri de utilizator a unor copii ale datelor;
- va permite interogarea directă a tabelelor care să prezinte imaginea datelor exact așa cum erau acestea la un moment anterior în timp, chiar dacă acestea au fost modificate ulterior, fără a necesita restaurarea dintr-un backup sau efectuarea de snapshot-uri periodice;
- va avea capabilități de management al discurilor.

Arhitectura sistemului de gestiune a bazei de date va fi una de înaltă disponibilitate de tip cluster activ-activ, o singură baza de date să poată fi instalată pe cel puțin 2 noduri distincte, fiecare nod cu minim 4 nuclee de procesare. Din perspectiva disponibilității vor trebui asigurate următoarele funcționalități minime și obligatorii:

- toleranță la defecte hardware sau nefuncționare planificată astfel încât să fie oferită o disponibilitate de tip 24x7 în cazul apariției unei defecțiuni hardware sau software la unul din serverele cluster-ului de baza de date;
- balansarea încărcării între noduri la nivelul cererilor și execuțiilor pe baza de date cluster și posibilitatea de a interoga memoria cache de pe celelalte noduri, oferind o încărcare uniforma a clusterului;
- în cazul apariției unor erori hardware sau software, acestea trebuie sa fie tratate automat de mecanismele interne ale bazei de date astfel încât reconectarea la nodul sau nodurile ramase disponibile să se facă în mod transparent față de aplicații și utilizatori;
- posibilitatea de a adăuga la nevoie servere de baze de date suplimentare în cluster, servere care vor fi active imediat și vor prelua din încărcarea bazei de date, fără a necesita oprirea serviciilor la nivel de cluster;

Din punct de vedere al operațiunilor de administrare și monitorizare, soluția de baza de date va include minim următoarele funcționalități:

- o unealtă cu interfață grafică, accesibila web din care administratorii vor putea gestiona obiectele bazei de date și a proceselor uzuale dar și administrarea utilizatorilor, rolurilor, privilegiilor și a procedurilor de backup;
- un editor SQL inteligent cu sintaxa colorată și cu funcție de completare automata a frazelor prin sugestii automate în funcție de context care va permite posibilitatea reformatărilor interogărilor SQL în funcție de nevoie sau de utilizator și va permite proiectarea structurii bazelor de date prin vizualizarea și editarea în mod grafic a structurii bazelor de date;
- vizualizarea încărcării bazei de date, a activității utilizatorilor și a operațiilor mari consumatoare resurse precum și oferirea de sugestii pentru îmbunătățirea performanței generale și identificarea automata a cauzelor ce duc la degradarea acesteia;
- mecanisme interne de monitorizare și diagnosticare continuă, automatizând colectarea parametrilor de funcționare ai bazei de date (CPU Load, Sistem IO, Wait-uri, top sql, top sesiuni, consum resurse, interogări neoptimizate), precum și stocarea acestora într-un repository dedicat pentru a putea furniza o imagine pe termen lung a modului de funcționare al bazei de date.

3.2.1.6. Componenta de raportare și analiză avansată

Componenta de raportare și analiză avansată trebuie va fi disponibilă comercial (COTS - Commercial off the Shelf) și va oferi posibilitatea de a rula pe diverse platforme hardware, precum și pe sistemele de operare majore existente pe piață (Windows și Linux).

Această componentă va permite crearea și rularea de rapoarte, precum și efectuarea de analize și prezentare sub formă de dashboards pentru a constitui în orice moment o viziune de ansamblu asupra situației la zi din cadrul instituției. Se are în vedere un număr de 25 de utilizatori ce vor avea acces la această componentă.

Componenta de raportare și analiză avansată va oferi următoarele funcționalități majore:

- prezentarea datelor în formate variate (de exemplu tabele, tabele pivot, grafice, texte derulante);
- funcționalități de navigare ghidată pentru utilizatorii finali, cu posibilități multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât și pentru grafice;
- combinarea rezultatelor obținute de pe platforme diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
- salvarea rapoartelor în formate diferite (Excel, PDF, Word, HTML etc.);
- definirea de tablouri de bord și includerea rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
- modificarea tablourilor de bord sau a rapoartelor, posibilitatea de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
- accesul la informație se va realiza printr-un nivel de metadate care va ascunde utilizatorilor finali complexitatea structurilor fizice de date;
- nivelul de metadate expus utilizatorilor va fi comun la nivelul tuturor modulelor sistemului de raportare și analiză;
- utilizatorii își vor putea crea singuri propriile rapoarte (analize ad-hoc) fără să fie nevoiți să cunoască structurile fizice de date pe care le accesează;
- accesarea datelor de pe platforme relaționale, multidimensionale, foi de calcul sau din fișiere stocate în sisteme de fișiere distribuite de tip Big Data;
- interacțiunea utilizatorilor finali cu aplicația se va face într-o interfață de tip web, fără a necesita instalarea de componente software suplimentare pe calculatoarele utilizatorilor;
- va expune o interfață de administrare atât a drepturilor de acces la diferite zone, cât și a drepturilor de acces pe diferite tipuri de acțiuni;
- va permite facilități avansate de formatare a rapoartelor;
- va oferi posibilitatea de salva, organiza și partaja rapoartele cu alți utilizatori;
- va oferi capabilități de drill-down (navigare în adâncime) pe diferite nivele de agregate;
- va permite acces la surse de date multiple, în mod transparent pentru utilizatorul final;
- accesul utilizatorului final se va face dintr-o singură interfață web din care să aibă acces la toate componentele de analiză și raportare;
- va oferi utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât și în aplicația de analiză și raportare;
- rapoartele analitice să poată fi construite pe un număr variabil de interogări analitice. Instrumentul nu va limita numărul de astfel de interogări;
- este necesar ca aplicația de raportare să poată afișa anumite valori identificate ca fiind critice, să semnalizeze depășirea unor praguri ale acestor valori, să semnalizeze apariția unor evenimente. Astfel, va oferi utilizatorilor posibilitatea de formatare condiționată a valorilor prin setarea unor praguri, pentru a evidenția valorile excepționale;

- să nu necesite replicarea datelor pe un server separat, ci să folosească capabilitățile bazei de date sursă;
- mediul de lucru pentru utilizatorii finali sau alți dezvoltatori de rapoarte/analize să fie în mediu web pur, interacțiunea cu sistemul să se realizeze prin operațiuni de tip „point and click" și „drag and drop" (să nu necesite cunoștințe de programare din partea utilizatorilor);
- să ofere posibilitatea definirii de rapoarte înlănțuite, datele din raportul copil fiind filtrate pe baza rezultatelor din raportul părinte;
- să permită tuturor utilizatorilor crearea sau modificarea de rapoarte, analize ad-hoc și tablouri de bord, acordarea drepturilor specifice (consultare, creare de obiecte etc.) urmând a fi făcută de către administratori.

3.2.1.7. Soluție de gestiune a identității utilizatorilor

Soluția va include un sistem centralizat de management al accesului la aplicații și va oferi funcționalități de single sign-on, autentificare, autorizare, administrare centralizată, managementul politicilor de acces, management în timp real al sesiunilor de aplicații și audit. Platforma va dispune de interfață de utilizare în limba romană și va fi un instrument care să poată rula pe distribuții majore de sisteme de operare prezente în piață. Rolul acestui sistem este de creștere a securității sistemului informatic și eliminarea riscurilor potențiale, prevenirea accesului neautorizat la sistemele și aplicațiile beneficiarului, simplificarea operațiilor de administrare prin reducerea și automatizarea numărului de operațiuni administrative.

Platforma de control acces va identifica utilizatorul la începutul sesiunii de lucru prin redirectarea către un ecran de autentificare. Ca și mecanisme de autentificare, soluția va suporta minim următoarele:

- utilizator și parolă;
- certificate digitale X.509;
- Windows Native Authentication;
- token SAML (Security Assertion Markup Language);
- autentificare de tip multi-factor prin introducerea unui mecanism secundar de autentificare precum PIN sau cheie dinamică.

Operațiunile de autentificare efectuate de către utilizatori, precum și activitățile administrative de creare, modificare, vizualizare, ștergere scheme de autentificare, module și politici de acces vor fi auditate, platforma colectând minim adresa IP, data acțiunii și ID login.

Platforma va include o consolă web pentru crearea politicilor de acces, aceasta permițând definirea granulară de politici de acces la nivel de resursă web sau adresă URL. Politicile de acces vor fi definite în mod grafic, fără a necesita cunoștințe de programare sau rularea de scripturi. De asemenea, va permite definirea de politici de acces în funcție de atribute de utilizator, atribute cerere de acces, date de sesiune.

Platforma va oferi capabilități de grupare politici de acces pe zone funcționale.

Platforma va oferi administratorilor posibilitatea de a gestiona centralizat toate sesiunile deschise către aplicații, având vizibilitate în timp real asupra datelor de sesiune ale utilizatorilor.

Administratorii vor putea seta global numărul maxim de sesiuni pe o resursă, durata maximă a unei sesiuni și să poată căuta, termina și bloca sesiunile deschise de către un utilizator.

Pentru managementul și disponibilitatea ridicată a sesiunilor deschise de către utilizatori, platforma va implementa un mecanism de caching date sesiune utilizatori. Mecanismul de caching va asigura confidențialitatea datelor. Mecanismul de caching va asigura disponibilitate ridicată printr-o arhitectură de tip cluster activ-activ.

Soluția va include posibilitatea de fluxuri de autorizare de tip One Time Password - OTP prin aplicație mobilă sau SMS.

Soluția va include și un instrument grafic de testare politici de acces pe resursele protejate prin care administratorul platformei să identifice rapid politicile de autorizare aplicate pe fiecare adresă web.

Sistemul de raportare va oferi posibilitatea de a exporta rapoartele generate în formate diverse, minim HTML.

Soluția va permite accesarea simultană a mai multor surse de identitate pentru realizarea procesului de autentificare și autorizare, fără a implica duplicarea informației sau crearea unui meta director.

De asemenea, va include un modul de virtualizare a surselor de identitate din cadrul beneficiarului, minim server de tip LDAP, tabele profil utilizator stocate în baze de date și servicii web.

Soluția va include în mod standard o listă de rapoarte predefinite:

- rapoarte asociate procesului de autentificare grupate pe sistem, adresa IP sau utilizator;
- raport erori de autentificare.

3.2.1.8. Componenta de interoperabilitate

Componenta pentru interoperabilitatea cu alte sisteme va permite schimbul intern și direct de informații între componentele sistemului, precum și schimbul de date cu partenerii instituționali externi. Fiecare sistem/modul se va putea abona la unul sau mai multe tipuri de mesaje, astfel încât să primească direct informațiile de care are nevoie. Interoperabilitatea va asigura distribuirea mesajelor către abonații interni sau externi corespunzători. După consumare, mesajele vor putea fi șterse.

Fiecare sistem/modul va produce informații care vor fi încapsulate într-un mesaj intern. Mesajele vor putea fi păstrate pentru o perioadă, astfel încât acestea să rămână disponibile pentru un subsistem care nu a fost disponibil. Interoperabilitatea va asigura rapoarte de poziții ale elementelor de dispozitiv, achiziționate prin interfețele externe. Interoperabilitatea va asigura alerte cross-componentă funcționale în conformitate cu logica operațională implementată la nivel de sistem.

Distribuirea datelor va fi posibilă prin mai multe protocoale, cum ar fi HTTPS, FTP/FTPS și SMTP. Formatele suportate pentru distribuția de date vor fi XML, REST, TEXT și

VFS. Componenta va asigura interoperabilitatea aplicațiilor conform principiilor și conceptelor arhitecturilor "Service Oriented Architecture" și "Event Driven Architecture" a WS-I Basic Profile, WSDL, WS-*, XML și SOAP, prin intermediul unei magistrale de servicii de întreprindere (Enterprise Service Bus).

Componenta va oferi suport pentru soluții moderne și deschise de integrare conform principiilor și conceptelor arhitecturilor SOA. Interoperabilitatea va fi bazată pe standardele deschise de interoperabilitate a aplicațiilor WS-I Basic Profile, WSDL, WS-*, XML, JSON, SOAP și Restful. Componenta va permite comunicații sincrone și asincrone inter-aplicații. Interoperabilitatea va permite folosirea canalelor de notificare moderne (email, SMS) pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicații.

Componenta va include un modul de stocare și evaluare a regulilor de business, pe care personalul instituției le va putea accesa și modifica online prin intermediul unei console web. Interoperabilitatea va suporta transformări și manipulări de date complexe pentru implementarea logicii proceselor de integrare.

Componenta va suporta transformări și modificări de date prin utilizarea de șabloane de integrare conform standardelor disponibile (Enterprise Integration Patterns). Tipurile de mesaje transportate/suportate de magistrala de servicii de întreprindere vor fi JSON, XML, text, binar și attachment. Interoperabilitatea va include capabilități extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL), xQuery și xPath.

Componenta va oferi soluții de conectare predefinite la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje (JavaJMS, Oracle Advanced Queuing (AQ), IBM MQ, MS MQ etc.), sisteme de fișiere și servere FTP. Componenta va suporta soluții de conectare la principalele sisteme existente pe piață. Componenta va oferi un cadru de dezvoltare pentru noi soluții de conectare la sisteme externe bazat pe standarde deschise.

Componenta va oferi servicii de transport cu suport pentru persistența datelor și pentru garantarea livrării datelor. Componenta va asigura nativ următoarele capabilități de dirijare a mesajelor: conținut mesaj, tabele dinamice de dirijare, prioritate, performanța serviciilor, versiune serviciu, conținut header SOAP, originea mesajului, User ID și rol, retransmitere în caz de eroare.

Componenta va oferi servicii de securitate atât la nivel transport, cât și la nivel de aplicație. Pentru asigurarea securității la nivel transport, interoperabilitatea va permite utilizarea protocolului Secure Socket Layer (SSL) și a certificatelor compatibile X.509. Componenta va oferi servicii de securitate specifice lucrului cu serviciile web standard: autentificarea accesului la servicii și autorizarea accesului la servicii. Componenta va fi bazată pe standardele deschise de securitate a serviciilor web, precum WS-Security, Security Assertion Markup Language (SAML) etc.

Componenta va oferi suport pentru standardele deschise de securitate privind mesajele în format XML: XML Encryption pentru criptarea/decriptarea mesajelor XML în vederea asigurării confidențialității mesajelor transportate și XML Signature pentru semnarea/verificarea digitală a mesajelor XML în vederea asigurării integrității și non-repudierii mesajelor transportate.

Componenta va oferi suport pentru instalarea în configurație de înaltă disponibilitate, minim cluster activ-pasiv.

Componenta va permite rularea pe toate distribuțiile majore de sisteme de operare prezente pe piață: Windows, Linux și Unix. Specificarea și modificarea fluxurilor de mesaje să se poată face atât utilizând mediul de dezvoltare integrat al sistemului.

Componenta va oferi managementul încărcării livrării mesajelor către serviciile destinație înregistrate la nivelul magistralei de servicii de întreprindere folosind cozi de mesaje tampon care permit: definirea concurenței maxime admise de serviciul destinație, definirea unei perioade de expirare pentru mesajele trimise și definirea de priorități asociate mesajelor. Actualizarea informațiilor în panourile de bord se va face automat, în timp real, fără a fi necesar un "Refresh" manual din partea utilizatorului.

Componenta va oferi nativ următoarele capabilități de logging: stare endpoint serviciu, erori, apel serviciu, timp de răspuns etc.

Cu excepția limitelor impuse de infrastructura hardware, soluția propusă nu trebuie să aibă limitări în ceea ce privește numărul de aplicații/sisteme conectate sau caracteristici derivate.

Componenta va dispune de o componentă runtime integrator cu conectori de diferite tipuri: conectori de tip JMS, conectori care respectă WS-* (WS-Addressing, WS-Security) precum și conectori pentru formate de date ca CSV, XML, JSON, HTML. Interoperabilitatea va oferi posibilitatea dezvoltării de noi conectori și publicării acestora spre utilizare.

Componenta va permite gestionarea de servicii de acces date existente și construirea de servicii proprii de acces date pentru baze de date cu driver JDBC, dar și suport pentru colecții de date CSV, XML, JSON, Excel, sau NoSQL.

Componenta va poseda un modul de monitorizare a fluxurilor de mesaje și a fluxurilor de procese prin care se pot vizualiza activitățile de rutare a mesajelor, modul de lucru cu task-urile planificate, evoluția diferitelor evenimente de transport, recepție etc.

3.2.1.9. Soluție software de backup

Soluția propusă va îndeplini următoarele cerințe:

- Va proteja datele prin mecanisme de copiere (backup, replicare asincronă și continuă);
- Va oferi interfețe de administrare pentru administratori atât grafic (GUI), cât și linie de comanda (CLI);
- Va avea mecanisme de eficiență integrată, prin care se realizează stocarea datelor, prin compresie și deduplicare. Deduplicarea va avea opțiunea opțiunea de a utiliza blocuri de 1MB sau mai mici, sau lungime variabilă;
- Va permite crearea backupurilor incrementale și sintetice (synthetic full). Este obligatoriu ca backupurile sintetice să necesite timp minim de realizare, prin mecanisme de offloading către echipamentele de backup utilizate. Toate opțiunile de restaurare trebuie să nu fie condiționate de tipul backupurilor (incremental, sintetic etc.);
- Va include mecanisme de criptare (standardul AES 256 sau superior). Criptarea se va realiza la sursă, și va fi utilizată în tranzit și cât timp datele sunt stocate. Toate opțiunile de restaurare vor fi permise din backupuri cu sau fără criptare, iar prezența criptării nu va limita operațiile de restaurare;

- Va sigura inamovibilitatea datelor (mecanisme de garantare a datelor la scriere și ștergere);
- Va permite autentificarea administratorilor cu multifactor (MFA), iar pentru componentele de infrastructură va putea utiliza autentificarea Kerberos-only;
- Va include cel puțin 3 mecanisme de protecție: backup cu compresie și deduplicare, replicare utilizând snapshoturi și replicare continuă;
- Va implementa toate componentele (data mover, proxies, noduri de criptare etc) ca virtual și/sau fizice;
- Va permite backup către object storage, cu suport pentru compatibil S3 și suport pentru imuabilitate;
- soluțiile software vor oferi reziliența catalogului pentru metadate, astfel încât datele din backup sau replicile să poată fi utilizate în cazul defectărilor hardware și a pierderii cataloagelor interne;
- va putea virtualiza storageul de backup, prin unificarea mai multor spații de stocare de pe unul sau mai multe echipamente hardware, oferind capacitate nelimitată de stocare. Storageul virtual va permite mutarea backupurilor și eliberarea capacități de stocare pentru upgrade-uri ale echipamentelor sau alte operații administrative, fără impact în operațiile de backup și restaurare;
- va permite realizarea backupurilor consistente pentru aplicații, inclusiv pentru baze de date Oracle, Microsoft SQL, PostgreSQL și MySQL;
- va permite recuperarea granulară a fișierelor sau folderelor, prin extragerea lor din backup;
- din motive de securitate, mașinile virtualizate cu rol de baze de date nu permit instalarea de software sau agenți pentru operațiile de backup sau recuperare. Soluția va permite backupul și recuperarea datelor fără a fi nevoie de a instala software. Operațiile de restaurare granulară pentru fișiere, aplicații și baze de date (inclusiv baze de date Oracle, MS SQL și PostgreSQL) se vor realizeza direct, fără instrumente adiționale, agenți sau software ce se instalează pe aceste mașini;
- va oferi posibilitatea utilizatorilor să utilizeze un portal cu autoservire, pentru datele pe care doresc să le recupereze și au permisiunea administratorilor. În portalul de autoservire, administratorii vor putea delega restaurările de fișiere, aplicații, baze de date (SQL, Oracle), e-mailuri și mașini virtuale;
- va permite recuperări ultra rapide, prin pornirea imediată a acestora din backup, fără a fi necesară copierea datelor. Copierea datelor se va face după recuperarea mașinilor virtuale și se va face în background;
- recuperarea ultra rapidă va fi disponibilă din orice backup, din orice mașină (VMware, Hyper-V, mașini fizice) și va permite recuperarea inclusiv pe o altă platformă (prin mecanisme de conversie a formatului), inclusiv operații P2V (Physical-to-virtual), V2V (Hyper-V to VMware, VMware to Hyper-V) și C2V (AWS to VMware, AWS to Hyper-V, Azure to VMware);
- va include mecanisme de recuperare ultra rapidă pentru baze de date Oracle și Microsoft SQL, prin pornirea acestor baze din backup;

- soluția va avea posibilitatea setării parametrilor pentru resursele utilizabile în procesul de backup, pentru a minimiza impactul pe mediile de producție. Astfel, soluția va prezenta capabilitatea setărilor pentru a limita banda utilizabilă în rețea, iar pentru echipamentele de stocare va putea stabili praguri la care procesele de backup vor fi oprite în cazul utilizării intensive;
- va permite recuperarea instantanee a bazelor de date, prin tehnologii de tipul instant recovery, pentru baze de date Microsoft SQL, Oracle și PostgreSQL;
- va oferi posibilitatea restaurării numai a modificărilor față de versiunea ce rulează în producție. Astfel, se va oferi posibilitatea comparării cu producția, a identificării tuturor fișierelor ce sunt modificate, schimbate și șterse, de la momentul backupului până la versiunea curentă;
- va putea face backupul logurilor bazelor de date Microsoft SQL, Oracle și PostgreSQL astfel încât să poată restaura aceste aplicații la orice moment dat de timp;
- va include capabilități de a stoca backupurile pe medii inamovibile (protejate la scriere și ștergere), cât și offline;
- din rațiuni de securitate, operațiile de restaurare vor permite restaurarea cu opțiunea de scanare de securitate;
- va putea realiza testarea periodică prin recuperarea automată în medii de test a datelor. Jurnalul testelor va putea fi exportat și utilizat în scopuri de raportare și audit;
- va permite raportarea operațiilor de backup, situația mașinilor protejate, capacitatea de stocare utilizată, testele de recuperare efectuate și operațiile de verificare efectuate pentru aplicații;
- va permite generarea rapoartelor și trimiterea lor via e-mail;
- va permite generarea de rapoarte pentru o perioadă de timp aleasă;
- va avea rapoarte predefinite și va permitemodificarea acestora;
- va permite generarea de rapoarte pentru modul de funcționare a soluției de protecție a datelor;
- va avea rapoarte despre starea snapshoturilor mașinilor virtuale, cât spațiu consumă aceste snapshoturi și dacă există potențiale snapshoturi orfane;
- va include 36 de luni de suport de la producător de la punerea în funcțiune.

3.2.2. Componente software aplicative

3.2.2.1. Soluția de management de documente

Întregul sistem informatic va fi proiectat și realizat în jurul componentei de management de documente, aceasta reprezentând core-ul viitorului sistem informatic.

Componenta va include multiple funcționalități pentru managementul documentelor. Va fi o aplicație software integrată dedicată de tip COTS ce include subcomponente/module funcționale aparținând aceluiași producător, pentru asigurarea suportului avansat de la producător și eliminarea eforturilor de integrare și testare a infrastructurii.

- sistemul va oferi performanță optimă pentru minim 145 de utilizatori interni fără restricții în cazul creșterii numărului de utilizatori;
- toate documentele și înregistrările vor fi integrate dintr-un depozit central (Repository);
- aplicația va fi proiectată într-o arhitectura pe mai multe nivele;
- componenta „Server" va putea fi implementată pe următoarele platforme: Microsoft Windows, Linux sau similar;
- pentru a putea fi accesată de pe diferite dispozitive, soluția va oferi mai multe tipuri de componentă de tip „Client":
    - client „web" - care să ruleze cu aceleași funcționalități pe oricare din browserele uzuale, cum ar fi: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari și să fie optimizat pentru afișarea pe dispozitive mobile;
    - client „mobile" de tip PWA (Progresive Web Application), nativ sau hibrid pentru sisteme de operare ANDROID și iOS;
- suport pentru integrarea cu sistemul de e-mail, inclusiv a documentelor atașate la e-mail;
- va oferi suport pentru integrarea cu aplicațiile Microsoft Office;
- sistem independent din punct de vedere tehnologic în conformitate cu standardele sistemelor deschise, pentru a se conecta eficient cu alte sisteme informatice și pentru a partaja eficient informațiile și documentele necesare: sistemul va avea o interfață de programare a aplicațiilor (Restful API) pentru integrarea cu alte sisteme informaționale;
- pentru realizarea de personalizări sau pentru integrarea cu alte aplicații externe, soluția va pune la dispoziție un Restful API (Application Program Interface) detaliat și bine documentat (Ex. Swagger);
- aplicația va putea utiliza drept layer de persistență relațional fiecare din următoarele baze de date: Oracle Database, Microsoft SQL Server, PostgreSQL, MySQL, MariaDB;
- interfața de interoperabilitate Restful va fi independentă de Fluxurile de lucru și va aplica constrângerile formularelor de colectare de date;
- aplicația va permite notificarea prin e-mail și SMS referitor la apariția unei cereri și va conduce utilizatorul automat în pagina unde acesta poate aprobă sau refuză aceasta cerere;
- interfața va fi prietenoasă și customizată în funcție de tipul de utilizator care accesează platforma;
- caracterele românești vor fi suportate pentru toate ecranele, meniurile, mesajele de eroare, textele de ajutor online, rapoartele și datele;
- toate datele introduse să fie validate în timp real;
- aplicația va oferi o interfață comună pentru utilizatori care să aibă același "aspect și impresie" pentru toate modulele din cadrul platformei;

- aplicația va putea fi extinsă cu fluxuri, formulare de introducere de date, rapoarte operaționale și tablouri de bord;
- aplicația să afișeze o pagină de start caracteristică utilizatorului autentificat care va include informații de interes pentru acesta inclusiv tablouri de bord;
- aplicația va permite definirea de noi fluxuri conform nevoilor speciale ale beneficiarului, precum și acordarea drepturilor de accesare pentru utilizatori și grupuri;
- aplicația va permite definirea și gestionarea de noi entități de date cu nume intern, etichetă, tip de date, lungime, precizie, vizibilitate în listă, valoare implicită, opțiuni formulă de calcul, asigurând totodată persistența noii entități de date în baza de date;
- aplicația va permite definirea interfeței utilizator pentru noi entități de date (formulare), vizualizare listă, adăugare înregistrare nouă, editare, ștergere;
- interfața sistemului va fi disponibilă în limba română;
- canalele de comunicație pe care circula documentele și informațiile vor fi securizate utilizând protocoalele SSL și HTTPS;
- soluția se va integrarea cu LDAP, OpenID, OAUT2, SAML etc. pentru autentificarea și managementul centralizat al utilizatorilor;
- aplicația va permite resetarea parolei pentru utilizatori;
- aplicația va permite gestionarea numărului de încercări pentru introducerea greșită a parolei;
- sistemul va permite integrarea cu componente software pentru scanare și captarea documentelor;
- modulul va include funcționalități încorporate pentru gestionarea de calendare pentru planificarea sarcinilor;
- sistemul va oferi suport pentru semnarea digitală a documentelor portabile pdf cu ajutorul certificatelor calificate stocate pe USB Token sau din cloud, direct din interfața cu utilizatorul a componentei, și să permită arhivarea adecvată a acestor documente semnate în conformitate cu legile în vigoare;
- aplicația va putea să blocheze automat contul utilizatorului după introducerea numărului maxim de încercări (parolă greșită) pentru autentificare. Administratorul va avea posibilitatea de a scoate utilizatorii din lista de blocare și de a seta numărul de încercări la care se va bloca accesul, precum și timpul pentru care utilizatorul va fi blocat;
- aplicația să nu permită schimbarea datelor prin alte metode decât editarea autorizată;
- aplicația să nu permită utilizatorilor obișnuiți accesul la datele din baza de date decât prin intermediul funcțiilor incluse în sistemul informatic;
- în caz de avarii, vor exista înregistrate informații de diagnosticare pentru a ajuta la identificarea și soluționarea problemei. Toate modulele funcționale vor popula un jurnal centralizat (bază de date) disponibil pentru administratori. Administratorul va putea configura nivelul înregistrării: urmărire, depanare, informații, avertizare,

eroare (trace, debug, info, warn, error sau fatal), instalarea să se facă în mod containerizat (Docker sau similar);

- sistemul va permite auditarea utilizatorilor pe toate tranzacțiile din sistem, de exemplu, fiecare comandă care este efectuată într-un caz/acțiune va fi înregistrată, specificând cine și când a actualizat documentul și cu păstrarea tuturor versiunilor unui formular electronic. Toate măsurile de securitate vor fi implementate în cadrul sistemului pentru a preveni accesul accidental sau deliberat neautorizat la datele conținute în sistem;
- soluția va asigura capacitatea de restabilire în urma dezastrelor (asigurarea securității fizice și logice) ca parte componentă a planului de implementare.

3.2.2.1.1. Modul de gestionare a documentelor

Prin acest modul COTS se va asigura gestionarea documentelor în format electronic astfel, acesta va dispune de următoarele caracteristici:

- un depozit electronic central (Central Repository) al tuturor documentelor (primite, create intern, trimise, arhivate etc.). Utilizatorii vor avea posibilitatea de a încărca în sistem e-mailuri, faxuri, documente scanate, documente electronice etc.
- interfață web și mobile pentru accesarea documentelor;
- va permite conversia adreselor poștale în coordonate GPS prin conectarea la un sistem de tip GIS;
- disponibilitatea tuturor versiunilor documentului: urmărirea și verificarea versiunilor documentelor;
- acces direct la depozitul electronic central de documente și înregistrări prin aplicațiile Microsoft Office sau similare;
- eficientizarea modului de căutare și detaliere a conținutului documentelor prin posibilitatea adăugării de meta informații (cum ar fi numărul de identificare, data și ora primirii, crearea, modificarea, trimiterea, arhivarea, descrieri sumare, cuvinte cheie, utilizator responsabil, categorie, tip etc.), politici de securitate;
- notificări prin e-mail și SMS pentru toate acțiunile standard și modificările aduse documentelor și datelor;
- va asigura procesarea electronică a documentelor, astfel încât să se obțină varianta acestora sub formă de text, permițându-se indexarea conținutului acestuia;
- va asigura posibilitatea de a căuta un document după proprietățile acestuia sau de a căuta după un text din conținutul documentului;
- va asigura gestionarea și controlarea indexării conținutului documentelor și a cererilor de căutare;
- va permite stocarea unei game variate de conținut în format electronic, de la imagini scanate ale documentelor pe hârtie, la documente create cu editoare de text, foi de calcul tabelar, fișiere grafice: BMP, JPG, GIF, fișiere text: PDF, TXT, HTML. Documentele vor fi păstrate independent de sistemul de baze de date utilizat pentru a evita creșterea dimensiunii bazei de date și îngreunarea timpului de răspuns.

Astfel, în baza de date se vor păstra doar legături către documente/fișiere, alături de datele asociate specifice;

- va permite adăugarea de documente electronice printr-un mecanism de tip "drag-and-drop";
- va oferi posibilitatea alocării de numere de înregistrare fiecărui document, astfel:
    - înregistrarea directă a e-mailurilor sau a documentelor atașate la e-mailuri;
    - înregistrarea documentelor prin anexare la dosar;
    - înregistrarea documentelor prin anexare la alte documente electronice structurate (formulare) înregistrate;
- va permite definirea și validarea metadatelor obligatorii într-o etapa din fluxul de lucru;
- va permite organizarea documentelor într-o structura intuitivă. Această organizare va fi prezentată într-o structură similară dosarelor / cazurilor. Documentele trebuie să poată fi organizate în structuri care să simuleze modalitatea reală de organizare în dosare / cazuri;
- va oferi posibilitatea de organizare a documentelor pe dosare;
- va permite definirea de "liste filtrate" prin specificarea parametrilor utilizați la filtrare (exemplu: documente de un anumit tip, cu o anumită valoare într-un câmp de indexare sau create de un anumit utilizator sau free-text);
- "Listele filtrate" vor fi specifice numai unui anumit utilizator și pot fi numite sugestiv, utilizatorii își vor putea crea "Listele filtrate" și își vor putea configura coloanele de căutare;
- va oferi posibilitatea stocării documentelor într-un spațiu centralizat și organizat și posibilitatea de a asocia metadate pentru fiecare document în parte;
- va permite administratorilor definirea volumului de stocare a documentelor (locația fizică în care vor fi salvate documentele în sistem);
- va permite administratorului configurarea atributelor (câmpuri de date) fiecărui tip de document;
- va permite operații multiple executate asupra documentelor:
    - versionarea automată a documentelor, permițând păstrarea tuturor versiunilor prin care trece un document;
    - etichetarea fiecărei versiuni, pentru a permite utilizatorilor identifice facil versiunea căutată;
    - indexarea automată a documentelor;
- în ceea ce privește prelucrarea documentelor pe tipuri de documente și metadate specifice acestor tipuri, modulul va permite:
    - arhivarea electronică a documentelor;
    - definirea tipurilor de documente permise pentru fiecare flux de lucru;
    - predefinirea fluxurilor de lucru pentru orice tip de document;
    - indexarea automată a documentelor;

- va oferi suport pentru ciclul de viață al unui document (crearea, modificarea, validarea, aprobarea etc). În funcție de starea unui document sunt disponibile spre utilizare diferite acțiuni asupra documentelor;
- va permite urmărirea și trasabilitatea modificărilor efectuate pe un document;
- va permite versionarea documentelor. Formatul de stocare al documentelor electronice va fi cel nativ, astfel se exclude păstrarea documentelor în formatul propriu sistemului, pentru a asigura recuperarea facilă a datelor în caz de defecțiune;
- în ceea ce privește căutarea, platforma va asigura:
    - căutarea documentelor inclusiv după textul conținut cel puțin pentru: documentele scanate utilizând OCR, fișiere Office (Word, Excel), fișiere PDF și emailuri;
    - salvarea căutărilor ad-hoc pe parcursul unei sesiuni de lucru pentru utilizare ulterioară;
    - rafinarea rezultatelor unei căutări prin filtrări și ordonări suplimentare operate doar asupra rezultatelor căutărilor;
    - căutarea rapidă după valorile din oricare câmp de indexare (metadată), după titlul documentului și după conținutul acestuia (full text);
    - realizarea unui "scoring" al rezultatelor obținute în urma operației de căutare și să afișeze rezultatele ordonate conform acestui scoring; scoring-ul va ține cont de relevanța termenilor de căutare dar și de data de creare și accesare a documentelor;
    - exportarea listei de dosare / cazuri sau documente rezultată în urma operației de căutare, în formate standard, cum ar fi csv sau excel;
    - definirea de câmpuri care să fie văzute în lista de rezultate precum și ordinea acestora, va permite ordonarea rapidă a rezultatelor după orice câmp;
    - definirea de "liste filtrate" de documente, vizibile pentru utilizator, prin specificarea parametrilor utilizați la filtrare (exemplu: documente de un anumit tip, create de un anumit utilizator) și a modului de afișare a rezultatelor;
- va dispune de un cadru integrat de colaborare pe documente prin scrierea de mesaje de colaborare pe document adresate anumitor utilizatori și păstrarea istoricului;
- va permite integrarea cu alte sisteme informatice, astfel încât să schimbe informații cu acestea sub formă de documente. Această funcționalitate privește (și) interogarea (la nevoie a) arhivelor de către organizații externe;
- va dispune de integrare cu aplicații Microsoft Office (in vederea asigurării compatibilizării cu sistemele utilizate în prezent de Achizitor), astfel încât să permită:
    - editarea și/sau salvarea documentelor direct pe server;
    - pre-vizualizarea (preview) a documentelor direct în interfață, fără să fie nevoie să se deschidă documentele în aplicațiile native asociate, pentru toate tipurile uzuale (PDF, imagine, Word, Excel, Powerpoint etc.);

- salvarea din aplicațiile Word și Excel direct în depozitul de documente;
- definirea șabloanelor direct În aplicația Microsoft Word. Astfel, orice document existent în format Word va putea fi transformat în șablon, prin definirea zonelor în care vor fi precompletate valorile din metadate;
- funcționalitatea de tip „merge" a datelor introduse în formularele structurate cu șabloanele Word;
- conversia direct din aplicație a fișierelor Word în fișiere pdf;
- salvarea automată a e-mail-urilor și a atașamentelor în depozitele de stocare a documentelor, cu preluarea automată a câmpurilor de indexare specifice e-mail-urilor: expeditor, recipient, subiect și conținut e-mail;
- trimiterea prin intermediul motorului de flux de lucru notificări de tip email, sms sau nativ în care utilizatorul să poată accesa direct din corpul mesajului de email:
  - documentul aflat pe flux;
  - task-urile de flux de lucru specifice etapei în care se află documentul;

- va permite transmiterea prin email a documentelor sau a unui link către documentele stocate în depozitul de documente al soluției ("repository");
- va include un modul de captură a documentelor;
- va include un modul de management de fluxuri de lucru cu documentele;
- va asigura o securitate ridicată în ceea ce privește accesul la documente, astfel:
  - accesul la documentele gestionate este posibil exclusiv prin intermediul aplicației client și nu prin file-sharing;
  - permisiunile sunt: vizualizare date, editare date, ștergere și de modificare;
  - drepturile de acces se pot asocia la nivel de dosar / caz, utilizând utilizatori și grupuri de utilizatori;
- va oferi o consolă administrativă, punând la dispoziția administratorilor de sistem o interfață prietenoasă pentru administrare;
- va oferi posibilitatea creării structurii de date, utilizând o interfață grafică, astfel să permită:
  - configurarea facilă, direct în aplicația de configurare/administrare, la nivel de atribut pentru cel puțin următoarele caracteristici: eticheta afișată utilizatorilor, tipul de date permis (text, număr, data calendaristică, logic = adevărat sau fals), lungimea permisă, valoare implicită (exemplu: utilizator curent, data curentă), lista de valori, formula de calcul funcție de alte metadate;
  - definirea de noi formulare, liste, entități organizatorice, date, relații părinte-copil, relații cu subpagini mapate pe alte tipuri de documente, pe care să le poată publica direct în meniul aplicației pentru utilizatori;
  - administrarea șabloanelor;
- va permite aflarea numărului de documente gestionat de platformă;

- va oferi posibilitatea de a monitoriza și notifica evenimentele astfel:
    - monitorizarea fluxurilor de lucru active;
    - generarea de alerte și notificări din fluxuri de lucru;
    - monitorizarea și generarea de alerte pentru fluxurile de lucru care nu sunt executate în numărul de zile stabilit;
    - notificarea utilizatorilor privind modificările ce apar în sistem: a fost creat un nou document, documentul a ajuns într-un nou stadiu etc.
    - notificarea pe e-mail despre o sarcină de efectuat sau neefectuată;
- va permite auditarea operațiunilor de login, logout, acces la dosare. Informațiile de audit vor conține inclusiv data, ora, utilizatorul și acțiunea efectuată;
- va permite păstrarea istoricului activității prin intermediul configurărilor aferente proceselor precum introducerea documentelor, aprobări, printări etc;
- va fi de tip enterprise și va putea fi instalată pe toate tipurile de sisteme de operare Linux, Windows și Unix;
- va permite conversia fișierelor Word și a formularelor de introducere de date în fișiere pdf;
- va permite semnarea electronică a documentelor de tip pdf direct din aplicație, cu semnătură stocata pe token USB sau din cloud;
- va permite trimiterea documentelor pdf spre semnare, prin intermediul fluxurilor de lucru, către liste de utilizatori;
- utilizatorul va putea specifica locul în care se va aplica semnătura electronica;
- în situația în care un utilizator refuza semnarea electronică a unui document, va putea specifica motivul refuzului;
- va permite aplicarea de semnătură electronică pe documente, direct din cadrul sistemului fără a fi necesară extragerea și reîncărcarea acestora în sistem;
- modulul va include funcționalități de generare de documente;
- platforma va oferi funcționalități pentru gestionarea și configurarea de șabloane Microsoft Word pentru generarea rapidă și automată de noi documente în formate standardizate care să respecte politicile organizației;
- documentele generate de sistem vor putea fi salvate în platforma în formate ca MS Word sau PDF;
- platforma va permite popularea automată a documentelor generate cu valori ale indecșilor salvați în componentă;
- la generarea unui document în baza unui șablon, platforma va permite preluarea de informații din toate metadatele dosarului și includerea lor în documentul nou generat;
- platforma va permite generarea automată de documente prin intermediul unor task-uri de fluxurile de lucru;
- platforma va permite generarea manuală, la selecția șablonului, de documente și atașarea lor pe dosar sau pe document structurat;

- platforma va permite administratorilor să creeze, și/sau modifice un șablon existent;
- platforma va permite restricționarea folosirii șabloanelor doar la anumite tipuri de cazuri sau de documente structurate.

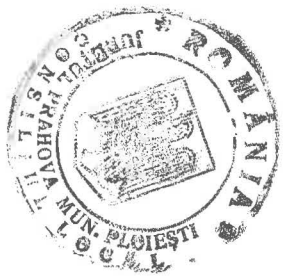
3.2.2.1.2. Modul Captură

Prin acest modul COTS se va realiza scanarea și OCR-izarea documentelor necesare la deschiderea unui dosar (în cazul documentelor depuse la registratură). Astfel, acesta va dispune de următoarele caracteristici:

- sistemul va facilita importul documentelor fizice în următoarele două moduri: de la stațiile de lucru ale utilizatorilor interni prin interfața web, cât și prin salvarea fișierelor pdf de către echipamentele de scanare de rețea;
- va permite scanarea asincronă și realizează legătura fișierului scanat la informațiile de înregistrare în funcție de codul de bare aplicat pe document;
- va dispune de capabilitatea de a imprima coduri de bare și numere de înregistrare cu imprimante de coduri de bare speciale și aplicarea pe documente;
- va realiza operațiuni automate de OCR pentru toate fișierele de tip imagine și PDF. În plus, va permite indexarea și căutarea automată a documentelor inclusiv după textul conținut cel puțin pentru: documentele scanate utilizând OCR, fișiere Office (Word, Excel), fișiere PDF și emailuri;
- va dispune de integrare nativă cu modulul de registratură permițând înregistrarea și direcționarea fișierelor către compartimentul de destinație;
- indexarea documentelor electronice va fi realizată atunci când imaginile scanate sunt convertite în documente .pdf în care se pot efectua căutări;
- va permite pre-vizualizarea (preview) documentelor direct în interfață, fără să fie nevoie să se deschidă documentele în aplicațiile native asociate, pentru toate tipurile uzuale (PDF, imagine, Word, Excel, Powerpoint etc);
- modulul de captură avansată va permite verificarea manuală pentru acuratețea rezultatului și actualizarea conținutului indexat.

Componenta de management de documente va încorpora un motor de indexare și de căutare distribuit, accesibil printr-o interfață Restful sau echivalent. Componenta va oferi următoarele caracteristici principale:

- capabilitate de căutare full-text;
- suport pentru expresii de căutare complexe;
- indexare text și cuvinte cheie;
- clasificarea și gruparea rezultatelor căutării;
- căutare geospațială;
- căutare distribuită pentru scalabilitate ridicată;
- metode de stocare redundantă a datelor pe mai multe noduri;
- consistență într-un sistem distribuit;
- suport pentru date persistente;



- suport pentru manipularea concomitentă a datelor;
- scripting și câmpuri calculate;
- stocare de documente;
- API Java și RESTful;
- multi-platformă;
- interfață de monitorizare;
- capabilități de analiză și machine learning;
- funcționalități de colectare automată de date din diverse surse;
- funcționalități de transformare de date.

3.2.2.1.3. Modul Registru electronic

Prin acest modul COTS se va realiza gestionarea interacțiunilor directe și indirecte (email și pagina web) dintre beneficiar cu entitățile externe.

Modulul va asigura următoarele funcționalități:

- păstrarea înregistrărilor și procesarea tuturor documentelor primite și care ies, inclusiv primirea, deschiderea, vizualizarea și atribuirea dosarelor / cazurilor și documentelor, introducerea în evidențele dosarelor și documentelor, împerecherea cazurilor și documentelor, livrarea cazurilor și documente pentru procesarea, procesarea cazurilor și documentelor, inclusiv producerea și depunerea automată a unei varietăți de documente electronice predefinite în cadrul fluxurilor de lucru, distribuirea cazurilor și documentelor, procesarea rezultatelor către destinatarii din afara organizației, calendarul cazurilor, plasarea cazurilor și documentelor în arhivă (arhivare electronică) și păstrarea acestora;
- înregistrarea și prelucrarea electronică a registrelor;
- etichetarea cazurilor, documentelor, corespondenței, bonurilor de livrare interne etc.;
- înregistrarea tuturor documentelor de intrare și de ieșire;
- înregistrarea directă a e-mailurilor sau a documentelor atașate la e-mailuri;
- client e-mail integrat direct în modulul de registratură, configurarea unui cont de e-mail de registratură per utilizator;
- posibilitatea generării, tipăririi și aplicării de coduri de bare pe documentele înregistrate pentru regăsirea facilă ulterioară a acestora în cadrul sistemului utilizând coduri de bare;
- posibilitatea scanării și indexării documentelor pe suport hârtie de către registrator. Registratorul va putea indexa documentul, utilizând indecșii definiți în platformă, cu tipurile de date și meta date asociate;
- posibilitatea definirii unui număr nelimitat de registre de documente. Pe fiecare registru de documente va exista posibilitatea definirii drepturilor de înregistrare a documentelor și tipurile de documente permise pentru înregistrare, având ca scop

minimizarea greșelilor umane de înregistrare sau după cuvinte din textul documentelor scanate;

- salvarea automată în aplicație și indexarea fișierelor scanate într-un folder preconfigurat;
- căutarea rapidă a documentelor după numărul de înregistrare sau după cuvinte din textul documentelor scanate;
- posibilitatea definirii de către administrator sau direct de către utilizator a coloanelor care să apară în fiecare registru. Completarea acestora se va putea face fie manual, fie prin preluare automată din metadatele documentelor înregistrate;
- inițierea fluxurilor de lucru la înregistrarea documentelor pentru transmiterea acestora către compartimentele responsabile (de exemplu, la recepția și înregistrarea unei petiții aceasta trebuie să poată fi transmisă automat pe flux către un anumit compartiment);
- va permite înregistrarea documentelor prin anexare la documente structurate (formulare) înregistrate;
- va asigura identificarea și urmărirea oricărui document folosind scannere de coduri de bare unice, număr de serie sau de înregistrare;
- va asigura crearea unui număr nelimitat de înregistrări și definirea de coloane personalizate;
- va asigura existența unor coloane standard pentru registre, cum ar fi: data înregistrării, numărul, sursa, de la - la, persoane, departament, descriere, număr de pagini, număr de înregistrare și data de primire de la cealaltă parte;
- va asigura atașarea documentelor la anumite numere ale unui registru;
- va asigura definirea drepturilor de editare/vizualizare pentru fiecare registru;
- va asigura exportarea conținutului registrelor în fișiere XLS sau CSV;
- va asigura imprimarea codurilor de bare și numerelor de înregistrare cu imprimante de coduri de bare speciale și aplicarea pe documente;
- va asigura configurarea drepturilor pentru fiecare registru de utilizatori și grupuri;
- va permite alocarea numărului de înregistrare fără fișier;
- va permite atașarea fișierelor la un număr de înregistrare existent;
- va fi integrat cu modulul de captură;
- odată înregistrate documentele în platforma de document management, în funcție de tipul de document înregistrat, precum și în funcție de indecșii și meta-datele asociate, documentele vor fi automat rutate de către platforma document management pe traseele electronice (fluxuri de lucru) definite și asociate acestora în sistem, precum și către destinatarii/departamentele asociate documentului în procesul de înregistrare.

3.2.2.1.4. Modul de fluxuri de lucru

Sistemul va include un motor de fluxuri de lucru COTS care asigură capabilitatea de gestiune a proceselor cu documente asigurând circulația documentelor pe trasee ierarhice sau definite de autorul documentului, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea și circulația informațiilor și a documentelor interne în cadrul beneficiarului, precum și a celor generate în relația cu terții.

Modulul va include atât instrumentele pentru dezvoltare, cât și mediul de rulare pentru proiectarea, execuția și monitorizarea fluxurilor de documente.

Modulul de fluxuri de lucru cu documente va asigura următoarele funcționalități:

- automatizarea managementului cazurilor în conformitate cu procedurile interne predefinite pentru fiecare categorie de cazuri;
- generarea automată a numerelor unice de dosare pe baza etichetei de clasificare, departamentul/compartimentul/direcția căruia îi sunt alocate dosarele, anului în care au fost instituite, precum și contorului secvențial automat.
- va permite autorilor de procese definirea și întreținerea vizuală, a fluxurilor de lucru aplicabile documentelor înregistrate;
- va permite autorilor de procese proiectarea fluxurilor de lucru bazate pe rolurile din organigramă;
- va permite autorilor de procese să definească termene limită pentru fiecare etapă a fluxului de lucru;
- va permite autorilor de procese să proiecteze fluxuri de lucru cu sarcini singulare sau sarcini paralele;
- va permite autorilor de procese să proiecteze fluxuri de lucru cu sarcini iterative, secvențiale sau paralele;
- va permite autorilor de procese să definească condițiile de terminare pentru o activitate paralelă;
- va permite autorilor de procese să definească comenzi condiționale în cadrul fluxurilor de lucru;
- va permite autorilor de procese definirea variabilelor pentru fluxurile de lucru sau pentru o sarcină;
- va permite autorilor de procese modificarea cu ușurință a fluxurilor de lucru, regulilor și logicii de rutare, drag and drop;
- va permite autorilor de procese să aloce drepturi de executare pentru fiecare flux de lucru;
- va permite autorilor de procese să definească tipuri de documente permise pentru fiecare flux de lucru și fluxuri de lucru specifice;
- va permite autorilor de procese să programeze declanșarea schimbului de date cu sistemele externe prin API (Application Programming Interface), înainte și după inițierea unui flux de lucru, și de asemenea, pentru orice pas al fluxului de lucru, minim conectori Java, Restful și SOAP;

- pentru orice flux de lucru va oferi posibilitatea să se definească un set de documente structurate și un set de documente nestructurate, relaționate direct la flux sau la documentele structurate. Componenta va permite ca pentru orice etapă a fluxului de lucru să se definească un set de documente nestructurate obligatorii / necesare etapei respective. În cazul în care unul din documentele respective nu este încărcat în sistem, platforma DMS va afișa/alerta în mod vizual către utilizator faptul că respectivul document lipsește. Mai mult decât atât, motorul de flux de lucru va permite prin configurare ca în cazul în care unul din documentele nestructurate obligatorii nu este încărcat, utilizatorul să nu poată trece în etapa următoare fără să încarce documentul respectiv;
- va permite autorilor de procese să programeze un timp de expirare o sarcină sau pentru flux de lucru;
- va permite autorilor de procese blocarea editării documentelor după anumite etape a fluxului de lucru - de exemplu: nepermiterea editării unui document după aprobare;
- va permite autorilor de procese să utilizeze grupuri și roluri pentru definirea fluxurilor de lucru;
- va permite autorilor de procese punerea în aplicare a oricărui tip de acțiune înainte sau după orice etapă a fluxului de lucru;
- va permite autorilor de procese definirea și validarea metadatelor obligatorii într-o etapa din fluxul de lucru;
- va permite autorilor de procese să programeze escaladarea automată a pașilor dacă nu există un răspuns într-un anumit număr de zile;
- va permite autorilor de procese exportul definiției fluxurilor de lucru în format de tip imagine, pentru a-l putea prezenta spre avizare;
- va permite autorilor de procese exportul și importul definiției fluxurilor de lucru într-un format standardizat recunoscut la nivel internațional;
- va sigura redirecționarea automată a sarcinilor în cazul în care utilizatorul și-a delegat sarcinile;
- va sigura informarea utilizatorilor prin e-mail, SMS și aplicație despre o nouă sarcină primită pe un flux de lucru;
- va asigura notificarea utilizatorilor pe e-mail, SMS, aplicație despre o sarcină de efectuat sau neefectuată;
- va asigura deschiderea sarcinilor de către utilizatori din notificări primite pe e-mail, aplicație;
- va permite utilizatorilor să scrie un comentariu asociat unei sarcini / document al unui flux de lucru;
- va permite administratorului să genereze un raport cu toate fluxurile de lucru și toate informațiile necesare;
- va permite utilizatorilor să creeze filtre de căutare care să se aplice fluxurilor de lucru;
- va permite administratorilor să oprească un flux de lucru;

- să asigura administrarea de delegații pentru utilizatorii în concediu de odihnă;
- să asigura notificarea utilizatorilor prin mesaje implicite pentru inițializarea fluxului de lucru și pentru acțiuni;
- va permite editarea documentelor structurate și nestructurate de către utilizatorii din fluxul de lucru;
- va permite manipularea automată a fișierelor într-un dosar /caz pre-selectat, după o etapă a fluxului de lucru;
- va permite utilizatorilor întoarcerea la un pas anterior în cazul în care documentul este returnat prin respingere;
- va permite utilizatorilor selectarea persoanei responsabile cu întocmirea din grupul de lucru, pentru ca documentele să nu fie trimise întregului grup;
- va permite generarea unui istoric al fluxurilor de lucru pentru utilizatori individuali sau grupuri și întreaga structură;
- va asigura monitorizarea fluxurilor de lucru active prin intermediul unei console web (definiții de flux, instanțe de flux, variabile, sarcini executate, erori etc.);
- va asigura generarea de alerte și notificări din fluxuri de lucru;
- va asigura monitorizarea și generarea de alerte pentru fluxurile de lucru care nu sunt executate în numărul de zile stabilit;
- va oferi posibilitatea unui utilizator să consulte în același ecran documentele structurate sau nestructurate ale unui dosar în același timp cu editarea unui document nou;
- va oferi suport pentru crearea și utilizarea formularelor electronice fără a fi necesară achiziția sau integrarea cu un alt software. Pentru crearea de formulare electronice, componenta va oferi un designer integrat de formulare electronice care va permite:
    - definirea de noi formulare și personalizarea ulterioară a acestora;
    - utilizarea în formulare a unor metadate existente la nivel de dosar;
    - posibilitatea adăugării unor atribute/câmpuri specifice doar formularelor (nu metadate) a căror valoare să fie salvată în baza de date și disponibilă pentru raportare sau acțiuni/reguli de flux de lucru;
    - posibilitatea de configurare a unor reguli inteligente de validare, de afișare dinamica a unor informații, în baza unor elemente existente (metadate, etape de flux, grup de utilizatori);
    - posibilitatea de creare a unor expresii prin opțiuni de calcul bazat pe formule și funcții predefinite în sistem;
    - posibilitatea utilizării unor controale/componente vizuale predefinite de tip secțiune, coloane, secțiuni repetitive, adăugarea de atașamente, semnătură olografă, hyperlink, imagini, câmpuri calculate;
    - posibilitatea de dezvoltare de noi controale care să poată fi adăugate în formulare;
    - posibilitatea de publicare a acestor formulare electronice;
    - exportul formularelor într-un format interoperabil.

3.2.2.1.5. Modul de Raportare

Platforma trebuie să includă un modul integrat de raportare care va permite realizarea prin configurare a unor rapoarte sau tablouri de bord care să afișeze în format tabelar sau grafic informații despre documentele și fluxurile de lucru din sistem. De exemplu:

- tipuri de documente per grupuri de documente și grupuri și sau utilizatori care le-au introdus;
- analize ale informațiilor stocate în metadatele documentelor;
- rapoarte de utilizare sistem și documente;
- timpul mediu de procesare a documentelor per proces/workflow;
- încărcarea zilnică per proces/workflow;
- timpul de procesare per etapă/coadă de workflow;
- documente procesate per etapă/coadă de workflow;
- documente rezidente per etapă/coadă de workflow;
- identificarea documentelor procesate intens sau încet (raportat la KPI prestabiliți);
- timpul de procesare per utilizator per etapă/coadă de workflow (în minute).

Rapoartele și analizele vor putea fi clasificate pe diferite categorii. Sistemul va permite ce grupuri de utilizatori și sau utilizatori pot accesa anumite categorii de rapoarte.

Modulul de raportare va permite prin configurare facilă, de exemplu de tip „drag and drop":

- crearea prin configurare de surse de date către baze de date relaționale și NoSql:
  - fie prin utilizarea unor surse de date predefinite în Platforma de management documente;
  - fie prin crearea de noi surse de date externe;
- crearea de rapoarte afișate în format tabelar sau pivot;
- crearea de analize afișate în formate grafice de tip: pie chart, bar chart, trend, map etc;
- posibilitatea de creare de analize de tip drill-down, inclusiv cu opțiunea de a deschide înregistrările sursă din analize sau de a lansa noi procese pe înregistrările din tabloul de bord sau de a accesa interfața de workflow și etapele în care sunt înregistrările respective;
- opțiunea de analiză multiplă a unor „slice" -uri de informații delimitate prin simpla selecție a unor segmente de date;
- utilizarea de formule (sum, min, max etc).

Modulul de raportare va fi disponibil din interfața soluției de management de documente, cu posibilitatea de a genera rapoarte pentru afișare pe ecran sau imprimare, în funcție de drepturile de acces ale utilizatorilor, va oferi suport pentru rapoarte analitice avansate și prezentări de ansamblu și va putea exporta date din rapoarte în diverse formate, cum ar fi Word, PDF, Excel (tabele de foi de calcul) și afișare grafică printr-o simplă acțiune cheie.

Componenta va permite producerea de rapoarte și tablouri de bord disponibile direct din soluția aplicativă, fără dezvoltare, inclusiv, dar fără a se limita la: data de aprobare a unor documente/etape, ștampilele/notele adăugate de utilizatori pe parcursul unei tranzacții, data creării, data modificării unui document.

Atât rapoartele operaționale, cât și tablourile de bord vor putea fi publicate în componenta de management de documente. Modulul de rapoarte va ține cont de contextul utilizatorului și va filtra datele afișate în funcție de context (ex: per departament).

Sistemul va furniza funcționalități de tip Business Intelligence, în timp real, fără necesitatea construirii de procese de tip ETL.

3.2.2.1.6. Modul de administrare

Modulul de administrare va sprijini gestionarea ușoară a taxonomiilor, utilizatorilor, drepturilor utilizatorilor și fluxurilor de lucru, inclusiv, cel puțin, următoarele:

- modificări ale aplicației fără a fi nevoie de a schimba codul sursă sau orice programare suplimentară;
- editor de flux de lucru ca instrument vizual pentru avizare/flux de lucru: modificarea și editarea fluxurilor de lucru - drag and drop și adăugarea de noi fluxuri de lucru ar trebui să fie posibilă fără o intervenție a Furnizorului și fără a avea abilități tehnice și de dezvoltare speciale;
- capacitatea de a defini date suplimentare (câmpuri, adică metadate) și entități suplimentare (noi forme de metadate) pentru fiecare tip de caz;
- sistemul va oferi suport pentru autentificarea de la distanță, care garantează identitatea subiecților în comunicarea acestora cu posibilitatea de a seta de către administratorul local parametrii de securitate precum:
    - administrarea permisiunilor individuale de acces la date și documente, definirea dreptului de acces (la nivel de înregistrări și documente individuale) de către utilizatori și grupuri de utilizatori. Drepturile de vizualizare, adăugare, modificare și ștergere a datelor și documentelor trebuie să fie diferențiate;
    - administrarea parolelor și a procedurilor de autentificare pentru sistem;
    - posibilitatea de a transfera propriile drepturi către alt utilizator în caz de absență. Perioada drepturilor transferate ar trebui să fie limitată și, prin urmare, ar trebui să aibă un termen limită de expirare, dar este necesar să se permită ștergerea drepturilor transferate anterior. Pentru transparență, este necesar să se păstreze transferurile de drepturi în evidențe.

3.2.2.1.7. Modul de ajutor

Sistemul va dispune de un modul de ajutor care să conțină informații explicative pentru fiecare modul în parte cu privire la instrucțiunile de utilizare a acestuia. Modulul va fi capabil să furnizeze explicații inclusiv pentru formularele de introducere de date.

Modulul de ajutor va fi parte integrantă a sistemului și:

- va fi adaptat contextului și situației (particularizat modulului în care utilizatorul solicită ajutor);
- va prezenta fiecare modul / parte a sistemului în detaliu cu instrucțiuni privind utilizarea corectă a acestuia.

Totodată, în cadrul fiecărui modul vor fi disponibile butoane de ajutor, a căror activare va avea drept rezultat furnizarea în mod automat a informațiilor de ajutor relevante contextului/situației/ecranului în care se află utilizatorul, precum si, la solicitarea utilizatorului, furnizarea informațiilor generale necesare prin raportare la cerința anterioară.

3.2.2.1.8. Alte precizări

Deoarece soluția de management de documente reprezintă nucleul în jurul căruia se va dezvolta întregul sistem și, deoarece, se preconizează că această componentă, alături de portal sunt cele mai predispuse modificărilor și adaptărilor continue la nevoile beneficiarului ulterior implementării, pe lângă faptul că pentru acestea vor fi achiziționate licențe de tip perpetuu, se vor achiziționa și codul sursă pentru soluția de management de documente și pentru portal în integralitatea sa, nu doar pentru eventuale dezvoltări și customizări realizate în cadrul proiectului. De asemenea, aceste componente se vor achiziționa cu posibilitatea ca pe toată perioada de garanție și suport ale sistemului, implementatorul să facă upgrade la versiunile noi lansate pe piață de către producătorul componentelor software de aplicație incluse în ofertă. Upgrade-ul la versiunile noi de produs se vor face fără niciun cost adițional pentru beneficiar.

3.2.2.2. Soluție Portal

Portalul Web va reprezenta un punct unic de acces la sursele de informații și servicii. Acesta va fi realizat pe o platformă flexibilă și scalabilă, capabilă să asigure standardizarea și reutilizarea resurselor și serviciilor, să furnizeze permanent conținut și informații noi, precum și acces rapid la informații și servicii (componente ale soluției).

De asemenea, interacțiunea cu cetățenii și companiile, precum și colaborarea va fi asigurată prin intermediul platformei de portal și a componentelor sale.

Platforma de portal va permite actualizarea rapidă a conținutului fără a necesita resurse de dezvoltare, distribuirea conținutului, stabilirea rolurilor și a drepturilor de acces.

Platforma va trebui să asigure accesul estimat a minim 145 de utilizatori interni și număr nelimitat de utilizatori externi ai sistemului.

Platforma portal va oferi următoarele funcționalități generale:

- interfață web, facilă pentru prezentare și navigare rapidă și simplă;
- posibilitatea de a personaliza conținutul;
- caracteristici pentru securitate ridicată;
- configurare în regim de înaltă disponibilitate;
- să poată fi configurat astfel încât să permită crearea de zone securizate pe care utilizatorii să le poată accesa din interiorul și exteriorul organizației, în conformitate cu matricea drepturilor de acces;

- va fi un sistem deschis bazat pe standardele existente în domeniu;
- va permite administrarea facilă;
- dezvoltarea aplicațiilor se va face ușor, respectând standardele în domeniu;
- portalul va oferi un punct centralizat de lucru pentru utilizatori și o interfață unică;
- este necesar ca interfața portalului să fie separată, din punct de vedere logic, de codul aplicațiilor integrate, astfel încât în cazul actualizării unei aplicații, să se păstreze toate particularizările ce au fost efectuate asupra interfeței;
- conținutul accesat prin portal va putea fi automat afișat sau ascuns, pe baza rolurilor utilizatorilor, roluri care sunt predefinite;
- administratorii vor putea controla drepturile utilizatorilor în funcție de rolul acestora sau în funcție de regulile definite;
- posibilitatea de integrare și comunicare în timp real cu o soluție de Management al identității externă portalului sau cu o soluție de servicii de directoare LDAP oferind inclusiv posibilitatea de sincronizare în timp real cu soluția respectivă; posibilitatea de a folosi o bază de date externă cu utilizatori;
- sistemul portal va permite utilizarea de mecanisme pentru autentificare, autorizare SSO și SSL; de asemenea, trebuie să permită și integrarea cu soluții de securitate;
- pentru aplicațiile care nu pot fi modificate (aplicații găzduite de alt provider) soluția va oferi posibilități de SSO prin rescrierea de header web, servicii web, cookie-uri sau dezvoltare de agenți sau procese de autentificare custom;
- nicio resursă web din interiorul sistemului nu va putea fi accesată direct din exterior, orice acces realizându-se prin intermediul serverelor web proxy;
- va integra controlul accesului pentru componentele sistemului;
- va cere utilizatorilor să introducă date de identificare pentru accesul la aplicații;
- va permite impunerea unor filtre de acces (operațiuni de autorizare) - cel puțin interval orar și locație de rețea de unde s-a inițiat cererea de acces;
- va permite administratorului sistemului să aleagă mai multe metode de autentificare și autorizare diferite pentru fiecare grup de resurse în parte;
- va oferi o interfață de administrare de tip web pentru accesul facil la configurări, care să poată fi accesată doar de către administratorii de securitate ai soluției;
- va oferi SSO - autentificare unică pentru accesul la resurse; pe parcursul unei singure sesiuni de lucru utilizatorul va fi autentificat o singură dată, după care va putea accesa fără reautentificare toate aplicațiile web pentru care are drept de acces;
- fiecare utilizator să fie identificat de sistem pe baza unei sesiuni;
- soluția va oferi și proceduri de autentificare pentru serviciile web și aplicații ce depind de parteneri sau provideri folosind mecanisme SAML 1.0, 1.1, 2.0, ADFS, and WS-Federation;
- soluția va asigura funcționalități de management al utilizatorilor și de control a drepturilor de acces:

- autentificarea unică a utilizatorilor prin servicii de tip Single Sign-On (SSO) și autorizarea acestora în sistem pe baza rolurilor și privilegiilor definite;
- utilizatorii vor avea acces numai la aplicațiile și documentele pentru care li s-a acordat dreptul de acces;
- va oferi un mod flexibil și unitar de gestiune a drepturilor și politicilor de acces ale utilizatorilor la toate resursele sistemului;
- va permite supravegherea cererilor de servicii și operațiilor executate de o persoană care a generat, a modificat sau a șters o informație;

- va permite deconectarea automată - va oferi un mecanism prin care un utilizator să fie deconectat în cazul în care nu a mai efectuat nicio tranzacție într-o anumită perioadă de timp;
- va permite utilizarea profilelor de utilizatori, administratorul putând seta astfel preferințele atât la nivel de profil, grup, cât și la nivel de utilizator. Aceste preferințe specifică atât accesul pe care îl vor avea la diverse secțiuni ale portalului, cât și drepturile asupra acestor zone;
- va asigura SSO de tip federație pentru a extinde procesele de SSO între aplicații interne sau externe;
- va avea o arhitectură deschisa;
- va oferi suport pentru XML și pentru servicii web;
- va fi flexibil din punct de vedere al clientului, putând fi accesat de pe majoritatea browserelor web existente pe piață și va respecta specificațiile WCAG;
- va permite folosirea de politici (colecții de setări) pentru administrarea următoarelor componente: utilizatori, grupuri, aplicații;
- va oferi nativ mecanisme de salvare și restaurare;
- va oferi posibilitatea de a recupera rapid informații dintr-o bază de date de conținut, fără a fi necesară restaurarea întregii soluții din care face parte acea bază de date;
- va asigura un asistent de creare de site-uri ce permite setarea permisiunilor, crearea de șabloane de conținut și adăugarea de teme personalizate;
- va permite dezvoltarea de aplicații bazate pe standarde web;
- va pune la dispoziție un mecanism robust de monitorizare a încărcării și performanței sistemului;
- va pune la dispoziție un mecanism de configurare/scripting de tip command-line;
- va oferi capabilități de clustering și load balancing;
- va oferi nativ următoarele funcționalități specifice pentru gestiune conținut:
- platforma va permite funcționalități avansate pentru gestionarea documentelor de orice tip, precum și lucrul colaborativ pe documente și proiecte;
- va asigura utilizatorilor posibilitatea de a crea moduri personale de vizualizare a informațiilor publicate;
- va permite managementul versiunilor de conținut;
- va permite implementarea de politici de retenție a conținutului;

- va oferi un mecanism de clasificare și rulare automată a conținutului către spațiile de stocare aferente;
- va permite definirea de seturi de documente (stocate în locații diferite) care să permită tratarea lor ca o singură entitate.

3.2.2.2.1. Automatizare a comunicării cu cetățenii

Componenta va dispune de un sistem de automatizare a comunicării cu cetățenii care să permită următoarele:

- să permită implementarea unui modul extern chatbot, bazat pe inteligență artificială și programat să desfășoare conversații într-un mod cât mai asemănător comportamentului uman, prin metodele de recunoaștere text și voce;
- să funcționeze integral on premise, fără a depinde de servicii externe;
- să ofere capabilitatea de integrare cu mai multe canale de comunicare;
- să permită integrarea cu soluțiile LLM consacrate: LLAMA, OpenAI, Gemini;
- să includă un modul predefinit LLM;
- pentru canalul de chat web va fi disponibilă o aplicație web care poate fi inclusă în orice pagină html;
- să conțină un modul predefinit de înțelegere a limbajului natural bazat pe inteligență artificială care să îi permită recunoașterea intențiilor și entităților exprimate liber de către utilizatori;
- să permită integrarea cu soluții de e-mail și sms cu posibilitatea de extindere pentru alte canale;
- să permită configurarea și administrarea conținutului asistentului în mod ușor, fără a scrie cod;
- să includă un modul de întrebări și răspunsuri prin intermediul căruia administratorii de conținut să poată configura o lista de întrebări și răspunsuri;
- să permită platformei moduri diferite de interacțiune pentru utilizatorii interni și externi.
- să permită fiecărui utilizator extern să creeze un cont ce poate fi atât anonim, bazat pe cookie-ul din browser, cât și pe bază de autentificare cu user și parolă proprie;
- să permită sincronizarea cu sistemul de SSO pentru a nu menține mai multe conturi utilizatorilor interni;
- să permită funcționalitatea de creare chatbot nou (proiect nou) disponibilă administratorului principal al platformei;
- să permită administratorului proiectului să activeze și să configureze integrări cu alte sisteme precum canale de social media;
- să pună la dispoziție utilizatorilor o serie de instrumente pentru testarea chatboților, respectiv testarea fluxului conversațional, inclusiv al intențiilor și entităților;
- să permită interacțiunea cu soluția DMS prin intermediul serviciilor web ale acesteia;
- să permit fluxuri de tipul "Human în the loop" (HITH);

- să permită configurarea unui mesaj de întâmpinare ce se va trimite automat la deschiderea ferestrei de chat.

3.2.3. Echipamente și soluții de securitate

În cadrul proiectului vor fi achiziționate echipamente și appliance-uri virtuale de comunicații și securitate care vor fi instalate atât în centrul de date cloud guvernamental (CG), cât și la nivelul sediilor SPFL Ploiești.

Nr. crt.	Echipament/appliance virtual	Cantitate	Locație implementare
1.	Appliance firewall aplicații web	2	Centrul de date
2.	Appliance honeypot	1	Centrul de date
3.	Appliance management centralizat rețea	1	Centrul de date
4.	Soluție pentru managementul evenimentelor și informațiilor de securitate	1	Centrul de date
5.	Echipament next generation firewall	2	Sediu central SPFL
6.	Switch acces	6	Sediu central SPFL Sediu secundar SPFL
7.	Switch PoE	5	Sediu central SPFL Sediu secundar SPFL
8.	Access point	10	Sediu central SPFL Sediu secundar SPFL
9.	Scânner citire/verificare documente identitate	10	Sediu central SPFL
10.	Infokiosk	5	Sediu central SPFL Sediu secundar SPFL Alte locații din municipiu determinate ulterior
11.	Laptop	45	Sediu central SPFL Sediu secundar SPFL
12.	Sistem desktop de tip All-in-One	100	Sediu central SPFL Sediu secundar SPFL
13.	Soluție ticketing ghiseu	1	Sediu central SPFL

3.2.3.1. Echipamente și soluții pentru centrul de date

3.2.3.1.1. Appliance firewall aplicații web

Soluția va fi implementată ca appliance virtual redundant cu suport pentru VMware, Hyper-V, KVM și va fi destinată protecției aplicațiilor web HTTP/HTTPS. Se va instala într-o configurație redundantă HA cu suport pentru minim 4 vCPU și va avea următoarele caracteristici:

- capacitate de procesare
  - Trafic procesat HTTP: 500 Mbps;
  - Domenii Administrative: până la 64.
- moduri de instalare în rețea
  - Reverse proxy;
  - Inline transparent;
  - True Transparent Proxy;
  - Offline sniffing;
  - WCCP.
- opțiuni de definire a politicilor și profilelor de securizare
  - politici de securitate predefinite;
  - opțiuni de partajare al accesului administrativ pentru configurația profilelor și politicilor de securizare pentru aplicațiile web protejate, prin utilizarea de domenii administrative.
- va include mai multe opțiuni pentru autentificarea utilizatorilor;
- va avea suport pentru High Availability cu sincronizare de configurație între două echipamente;
- va oferi protecție la nivel de aplicație împotriva atacurilor de tip:
  - OWASP Top 10;
  - Cross Site Scripting;
  - SQL Injection;
  - Cross Site Request Forgery;
  - Session Hijacking.
- controlul accesului clienților de aplicație HTTP după blacklist-uri și whitelist-uri configurabile de adrese IP;
- funcționalitate de scanare programabilă și raportare automată a vulnerabilităților aplicațiilor web protejate;
- posibilitatea de a defini manual semnături de atac noi;
- blocare pe bază de reputație a surselor cu potențial malițios de tip malware, spam, phishing, DDoS, proxy anonim
- protecție împotriva botnet, crawler, scraper

- posibilitatea de a monitoriza și bloca traficul provenit dintr-o anumită regiune geografică sau țară;
- protecție împotriva scanării fișierelor de conținut malițios (scanare antivirus)
- va oferi opțiuni de procesare a traficului
- va beneficia de minim 3 ani de sport, din momentul instalării ce va include:
    - suport tehnic din partea vendorului 7 zile pe săptămână, 24 ore pe zi;
    - update firmware versiuni minore și majore.
- va beneficia de minim 3 ani update-uri automate de semnături de securitate pentru IP Reputation, WAF, Antivirus, Sandbox în cloud producător, Analiza în cloud a amenințărilor, Baza de date credențiale compromise, din momentul instalării.

3.2.3.1.2. Appliance honeypot

Această componentă va fi un appliance integrat de protecție în rețea cu capabilități de expunere a unor servicii cu scopul de a atrage atacatorii în exploatarea acestor sisteme în vederea descoperirii tehnicilor, uneltelor și metodelor de penetrare folosite asupra organizației, atât din exteriorul rețelei, cât și din interiorul ei.

Scopul soluției este să inspecteze comportamentul atacatorilor și să valideze intențiile malițioase, în timp ce direcționează aceste activități către un mediu sigur, aflat în afara sistemelor de producție.

Pentru a asigura acuratețe și performanță, toate modulele de protecție ce alcătuiesc modulele de securitate trebuie să funcționeze având la baza un sistem de operare dedicat, dezvoltat de către producătorul echipamentului. Nu este permisa folosirea unui sistem de operare comercial, pentru uz general.

Appliance-ul honeypot va avea următoarele caracteristici:

- va fi instalabil ca appliance virtual cu suport pentru VMware, Hyper-V, KVM;
- va avea suport pentru minim 12vCPU;
- implementarea unor instanțe VM/sisteme de operare care să atragă atacatorii în vederea interacțiunii și exploatării acestor capcane virtuale;
- implementarea instanțelor capcană va putea fi efectuată și controlată dintr-o locație centrală;
- implementarea de instanțe reale virtuale pentru sistemele de operare Windows și Linux, în aceleași segmente de rețea cu stațiile reale;
- implementarea de servicii capcana de tip SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP and TCP port listener, SMTP, RADIUS, Mysql, MQTT, SIP, XMPP;
- descoperirea activității de exploatare cu detecție și alertare timpurie;
- depistarea și corelarea activității atacatorilor în interiorul segmentelor de rețea monitorizate;

- eliminarea amenințărilor prin direcționarea atacatorilor către sistemele capcană, deviind atacatorii (in mod automat, fără intervenția operatorului uman) de la sistemele de producție (ex. utilizând agenți/clienți/token-uri locale);
- monitorizarea:
    - evenimentelor de tip login și logout;
    - accesului la partajarea Windows;
    - încercărilor de intruziune;
    - accesului către anumite pagini web.
- soluția va beneficia de minim 3 ani de suport, din momentul instalării, direct de la producător și va fi licențiată pentru a asigura:
    - conectare a cel puțin 4 VLAN-uri în regim de deception;
    - 4 instanțe capcană de tip Windows;
    - subscripții pentru activarea funcționalităților de anti-evaziune, anti-exploatare, IPS, AV și web filtering, precum și pentru implementarea instanțelor / mașinilor capcană și serviciilor capcană, în cadrul VLAN-urilor de deception;
    - suport tehnic 7 zile pe săptămână, 24 ore pe zi;
    - update firmware versiuni minore și majore;
- soluția va beneficia de update-uri automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților cerute mai sus timp de minim 3 ani, din momentul instalării.

3.2.3.1.3. Appliance management centralizat rețea

Aceasta va reprezenta o soluție de tip platformă de management centralizat al echipamentelor de securizare a rețelei, aplicații și acces LAN și va îndeplini următoarele caracteristici:

- va avea același producător ca echipamentele de tip firewall, switch acces, switch PoE, access point, și va putea administra toate aceste echipamente;
- va putea distribui update-uri de semnături de securitate, va putea realiza logarea evenimentelor și va putea genera rapoarte pentru appliance-urile firewall aplicații web redundant;
- va putea distribui update-uri de semnături de securitate pentru appliance-ul honeypot;
- soluția va fi achiziționată ca mașină virtuală / appliance virtual compatibilă cu platformele de virtualizare VMware, Hyper-V, KVM sau echivalent, cu minim 8 GB memorie și minim 4vCPU;
- va permite configurarea colectivă a politicilor de securitate de pe echipamentele gestionate;
- va permite managementul capabilităților de tip SD-WAN;
- va permite managementul conexiunilor VPN dintre echipamentele gestionate;

- va permite monitorizarea în timp real a incidentelor survenite pe echipamentele gestionate;
- va permite personalizarea raportării incidentelor;
- capacitate log-uri pe zi de minim 6 GB;
- număr minim de echipamente administrate în mod licențiat: 30;
- soluția va avea asigurate serviciile de suport de tip 24x7 din partea producătorului pentru o perioadă de 3 ani, din momentul instalării. Serviciile de suport vor include update gratuit la noile versiuni ale software-ului pe toată durata perioadei de garanție, posibilitate de ridicare de incidente către centrul de suport al producătorului;
- după expirarea serviciilor de suport tehnic și de actualizare software, platforma trebuie să funcționeze, să permită atât administrarea, cât și fluxurile de date.

3.2.3.1.4. Soluție pentru managementul evenimentelor și informațiilor de Securitate

Soluția va îndeplini următoarele caracteristici:

- alertare automată în situația în care (datorita unor defecțiuni, erori umane sau atacuri cibernetice) anumite conexiuni, sisteme sau aplicații devin inaccesibile sau nefuncționale;
- colectarea și stocarea log-urilor (aferente echipamentelor și aplicațiilor IT&C), pentru perioade îndelungate de timp: atât online, cât și offline prin arhivare;
- corelarea automata între logurile și alertele predefinite sau definite de către administrator;
- detectarea anomaliilor comportamentale (detectarea abaterilor de la valorile statistice de referință) și alertarea automata în cazul producerii acestora;
- posibilitatea de rulare automată a unor scripturi de remediere (predefinite sau definite de către administrator) în cazul producerii unor incidente de: securitate, disponibilitate, performanță;
- posibilitatea de investigare cât mai rapidă a unor eventuale tentative de încălcare a securității datelor, atacuri cibernetice sau probleme de performanță/disponibilitate prin analizarea în timp real a log-urilor și evenimentelor colectate;
- instalare ca soluție software putând rula pe platformele de virtualizare VMware ESX, Microsoft Hyper-V, KVM;
- colectarea de informații în mod pasiv (fără interogarea dispozitivelor sau a aplicațiilor existente), prin captarea mesajelor/log-urilor: Syslog, NetFlow, sFlow, SNMP Traps;
- colectarea de informații (de Securitate, Performanta, Disponibilitate și Modificare), în mod activ, fără agenți, prin interogarea dispozitivelor și aplicațiilor existente utilizând protocoalele standard: SNMP, WMI, VM SDK, OPSEC/CheckPoint LEA, JDBC, Telnet, SSH, JMX;

- monitorizarea stării și nivelului de răspuns al serviciilor DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH și Web (HTTP, HTTPS). Rezultatul acestei monitorizări poate fi utilizat în calcularea nivelelor de disponibilitate aferente serviciilor respective;
- definirea de rapoarte complexe care cumulează/conțin la rândul lor mai multe rapoarte distincte/individuale;
- posibilitatea de a exporta un raport în format PDF sau CSV;
- posibilitatea de a transmite un raport prin email în mod manual sau automat (programat pentru anumite momente de timp prestabilite: de ex. zilnic, săptămânal, lunar);
- posibilitatea de a corela, la nivelul unei reguli de alertare, a următoarelor tipuri de evenimente:
    - securitate: IPS, AntiVirus, erori de autentificare, exploituri, vulnerabilități etc.;
    - performanță: nivel încărcare CPU, RAM, spațiu de stocare, conexiuni/throughput;
    - disponibilitate: restartarea sau întreruperea unor aplicații/servicii/echipamente);
    - modificare: modificare unor fișiere, modificarea configurațiilor unor echipamente, adăugarea/ștergerea unor utilizatori etc.;
- soluția va asigura integrarea a cel puțin 75 dispozitive IT&C și a cel puțin 1.000 de evenimente pe secundă;
- soluția va beneficia de support 24x7 din partea producătorului pentru o perioadă de 3 ani, din momentul instalării, inclusiv accesul la update-urile de firmware (OS, patch-uri);
- soluția va beneficia de update-uri pentru baza de date cu indicatori de compromis (IOC) pentru o perioadă de 3 ani, din momentul instalării.

3.2.3.2. Echipamente și soluții sedii SPFL Ploiești

Echipamentele prevăzute în această secțiune sunt destinate instalării și utilizării la nivel local, în cadrul sediului central SPFL Ploiești și în cadrul sediului secundar al SPFL Ploiești.

La nivelul sediului central vor fi instalate următoarele echipamente:

- 2 echipamente redundante de tip Next-Generation Firewall;
- 1 soluție ticketing pentru 10 ghișee
- La subsol va fi instalat un access point;
- La parter vor fi instalate 2 switch-uri acces, 1 switch PoE și 2 access point-uri;
- La etajul 1 vor fi instalate 2 switch-uri acces, 1 switch PoE și 2 access point-uri;
- La etajul 2 vor fi instalate 2 switch-uri acces, 1 switch PoE și 2 access point-uri.

La nivelul sediului secundar vor fi instalate următoarele echipamente:

- La parter vor fi instalate 1 switch PoE și 2 access point-uri;
- La etajul 1 vor fi instalate 1 switch PoE și 1 access point.

La nivelul celor 2 clădiri se va realiza și cablarea structurată.

5 sisteme de tip infokiosk cu posibilitatea de plata a taxelor vor fi instalate la Sediul Central/Sediul secundar si in alte locații larg utilizate din Municipul Ploiești, locații ce vor fi determinate ulterior.

3.2.3.2.1. Echipament next generation firewall redundant

Vor fi implementate la nivelul sediului central SPFL Ploiești (principal) 2 echipamente redundante de tip Next-Generation Firewall care vor avea următoarele caracteristici:

- firewall de tip stateful;
- router cu suport pentru protocoale de rutare dinamice;
- securitate: IPS, antivirus, filtrare Web, control aplicații, antispam;
- IPSec VPN și SSL VPN;
- suport pentru QoS și Traffic Shaping;
- suport pentru SD-WAN;
- update-uri automate și în timp real;
- suport pentru IPv6 UTM;
- server token OTP;
- minim 8 x 10 GE SFP+;
- minim 4 x 1 GE SFP;
- minim 8 x 1GE RJ45;
- trafic firewall (1518/512/64 byte pachete UDP): 39/39/26 Gbps;
- trafic Firewall măsurat în pachete per secundă: 39 Mpps;
- număr de sesiuni concurente TCP: 11.000.000;
- IPSec VPN la pachete 512 byte: 36 Gbps;
- SSL VPN Throughput: 3 Gbps;
- IPS Throughput: 9 Gbps;
- NGFW Throughput: 7 Gbps;
- SSL Inspection Throughput: 7 Gbps;
- capabilități de Explicit Proxy;
- capabilități VPN precum: PPTP, L2TP, IPSec, L2TP over IPSec, SSL-VPN, criptare: DES, 3DES, AES128. AES192, AES256;
- soluția va beneficia de minim 3 ani de suport din momentul instalării ce va include:
    - înlocuirea echipamentului în caz de defecțiune hardware;

- Suport tehnic din partea producătorului 7 zile pe săptămână, 24 de ore pe zi;
- update firmware versiuni minore și majore;
- update-uri automate de semnături de securitate pentru îndeplinirea funcționalităților de Antivirus, Web Filtering, Antispam, Application Control și IPS.

3.2.3.2.2. Switch acces

Vor fi implementate la nivelul sediului central și al celui secundar al SPFL Ploiești 6 echipamente de tip switch acces care vor avea următoarele caracteristici:

- 48 interfete GE RJ45;
- 4 interfete 10Gbps SFP+;
- 1 port consola;
- echipamentul va putea funcționa în mod independent, administrat din Cloud, cât și de către un echipament cu facilitate de Switch Controller;
- arhitectura non-blocking (capacitate switching: 176 Gbps);
- capacitate de procesare (pachete pe secunda): 260 Mpps;
- stocare Adrese MAC: 32K Adrese MAC;
- VLAN-uri suportate: 4K;
- protocoale și standarde:
  - Securitate: 802.1X (port Based, Mac Based), 802.1X MAB, DHCP Snooping, Dynamic ARP Inspection, IEEE 802.1X Open Auth, IPv6 RA Guard, LLDP-MED ELIN support, RADIUS Accounting, RADIUS CoA, sFLOW Sticky MAC, asignare VLAN dinamica, Reliable Syslog, Packet Capture, ACL;
  - Layer 2: IGMP Snooping, IGMP Querier, IGMP proxy, MSTP, integrare Rapid PVST, Storm Control, Per-Port Storm Control, Loop Guard, SPAN, MAC Notification Trap;
  - Layer 3 (facilitățile de Layer 3 pot fi oferite de switch în mod de operare standalone, fie asigurate de Switch Controller): Static Routing, Static BFD, DHCP Server, DHCP Relay;
  - QoS: 802.1p, priority queuing trunk și WRED, Taildrop Policy;
  - Suport RFC.
- soluția va beneficia de minim 3 ani de suport din momentul instalării ce va include:
  - înlocuirea echipamentului în caz de defecțiune hardware;
  - suport tehnic din partea vendorului 7 zile pe săptămână, 24 ore pe zi;
  - update firmware versiuni minore și majore.

3.2.3.2.3. Switch PoE

Vor fi implementate nivelul sediului central și al celui secundar al SPFL Ploiești 5 echipamente de tip switch PoE care vor avea următoarele caracteristici:

- 24 interfețe GE RJ45, unde toate cele 24 de interfețe vor putea oferi alimentare PoE, cu suport atât pentru 802.3af cât și 802.3at
- buget PoE minim 370W;
- 4 interfețe 10Gbps SFP+;
- 1 port consolă;
- arhitectura non-blocking (capacitate switching: 128 Gbps);
- capacitate de procesare (pachete pe secunda): 190 Mpps;
- stocare Adrese MAC: 32K Adrese MAC;
- VLAN-uri suportate: 4K;
- protocoale și standarde:
    - Securitate: 802.1X (port Based, Mac Based), 802.1X MAB, DHCP Snooping, Dynamic ARP Inspection, IEEE 802.1X Open Auth, LLDP-MED ELIN support, RADIUS Accounting, RADIUS CoA, Sticky MAC, Asignare VLAN dinamica, ACL;
    - Layer 2: IGMP Snooping, IGMP Querier, IGMP proxy, MSTP, Integrare Rapid PVST, Storm Control, Per-Port Storm Control, Loop Guard, SPAN;
    - Layer 3 (facilitățile de Layer 3 pot fi oferite de switch în mod de operare standalone, fie asigurate de Switch Controller): Static Routing, Static BFD, DHCP Server, DHCP Relay;
    - QoS: 802.1p, priority queuing trunk și WRED;
    - Suport RFC.
- soluția va beneficia de minim 3 ani de suport din momentul instalării ce va include:
    - înlocuirea echipamentului în caz de defecțiune hardware;
    - suport tehnic din partea vendorului 7 zile pe săptămână, 24 ore pe zi;
    - update firmware versiuni minore și majore.

3.2.3.2.4. Access point

Vor fi implementate la nivelul sediului central și al celui secundar al SPFL Ploiești 10 echipamente de tip access point care vor avea următoarele caracteristici:

- Access Point de interior, 802.11ax/WiFi 6E;
- Posibilitatea de administrare din wireless controller-ul integrat în soluția de firewall implementată;
- Moduri de operare suportate: Centralizat, Distribuit, Mesh;
- Benzi frecvente: 2.4GHz, 5Ghz și 6GHz simultan pentru acces;
- Antene: 2 x Dual Band Interne, 2 x Tri Band Interne, 1 x BLE Internă;

- SSID-uri suportate: 16;
- Securitate: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST, WPA PSK, WPA2 PSK, WPA3 PSK, WPA cu 802.1X, WPA2 cu 802.1X, WPA3 cu 802.1x, filtrare MAC;
- Standarde IEEE: 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az, 802.3bz;
- Interfețe/porturi: 1 x RJ45 (100/1000/2500Mbps), 1 x RJ45 (10/100/1000Mbps), PoE, 1 x Console RJ45.
- soluția va beneficia de minim 3 ani de suport din momentul instalării ce va include:
    - acces la suportul tehnic al producătorului (include acces la upgrade/update de firmware);
    - înlocuire hardware avansată.

3.2.3.2.5. Laptop

Vor fi achiziționate 45 de laptopuri care vor avea următoarele caracteristici:

Componenta	Specificatii
Procesor	Din cea mai recenta generație lansată de producător, de tip Intel Ultra 5, sau echivalent
Ecran	Diagonala 16", tehnologie WVA / IPS, 165Hz refresh, rezolutie FHD+, rabatabil 180⁰
Carcasa	Metalica (A, C si D), rezistenta la socuri, lovituri si la uzura - validare MIL-STD-810H
RAM	Instalata 16GB LPDDR5X, 8533 MT/s
Stocare	1TB, SSD M.2 NVMe PCIe Gen 4
Video	Intel Arc Graphics, sau echivalent
Cameră Web	Integrată, 5.0MP cu TNR si Human Presence Detection
Audio	Doua boxe integrate - High Definition Audio
Conectivitate	Wi-Fi 7, Bluetooth 5.4
Porturi (integrate)	1 x Thunderbolt (cu functie de alimentare a laptopului) 3 x USB 3.2 (din care cel putin unul Type C) 1 x HDMI 1 x Audio jack (casti si microfon) 1 x Slot SIM
Card Reader	MicroSD
Securitate	Windows Hello Camera cu modul SecureBIO si modul integrat TPM 2.0
Tastatura	Tastatura iluminata cu num pad integrat
Acumulator	Minim 70Wh
Alimentator	Minim 65W
Portabilitate	Greutate mai mica de 1.5 kg
Sistem de operare	Windows 11 PRO - preinstalat si preactivat, cu cheie inserata in BIOS sau echivalent
Expandabilitate	Posibilitatea de a monta intern un modem 5G intr-un slot M.2 dedicat
Pachet Office	Licenta Microsoft Office Home & Business 2024 preinstalat, licenta perpetua sau echivalent
Antivirus	Solutie antivirus ce va asigura protecție completă împotriva tuturor tipurilor de malware: ransomware, phishing, viruși, spyware etc. - cu o valabilitate de 3 ani Solutia va fi disponibil într-o singură platformă ușor de utilizat, care acoperă toate echipamentele de tip statie personala.
Certificari si conformitate	Certificare Microsoft Windows 11 Professional (listare pe Microsoft WCPL https://partner.microsoft.com/en-us/dashboard/hardware/search/cpl)
Garantie	36 luni (3 ani) garantie de la data receptiei, sustinuta si certificata de producatorul echipamentelor.

3.2.3.2.6. Stații de lucru de tip All-in-One

Vor fi achiziționate 100 de complete de lucru de tip All-in-One care vor avea următoarele caracteristici:

Componenta	Specificatii
Carcasa	Tip AIO (nu se accepata solutii VESA PC pe Monitor)

Componenta	Specificatii
Ecran	Minim 27" FHD (1920 x 1080) 16:9, Anti-glare display, tehnologie IPS Stand cu functie de inclinare (Tilt) -5° to 25°, rotire (Swivel), reglare pe inaltime
Placa de baza	Cu chipset din seria 800, compatibil cu procesorul
Procesor	Minim clasa Intel Ultra 5 din cea mai recenta generație lansată de producător, sau echivalent
Memorie	minim 16 GB DDR5 instalat instalabil 128 GB DDR5
Stocare	minim: 1TB, SSD M.2 NVMe PCIe Gen 4 minim cu posibilitatea de a monta inca 2 unitati de stocare de 2.5"
Cameră Web	Camera WEB 8MP integrata, cu obturator mecanic integrat microfon Dual integrat
Audio	placă audio integrată boxe stereo integrate, minim 2 x 1.5W
Portui integrate	minim: 1 x HDMI In 1 x HDMI Out 1 x RJ45 Gigabit Ethernet 5 x USB 3.2 (din care minim 3 x USB Type-C) 4 x USB 2.0 3 x Audio jacks
Comunicații fară fir	Wi-Fi 7 Bluetooth 5.4
Sursa de alimentare	Sursa interna de minim 250 Watt, eficienta de 80%
Securitate si protectie	Modul TPM 2.0 Sistem de blocare a accesului in interiorul AiO-ului, pentru persoanele neautorizate Permite securizarea echipamentului cu cablu de securitate (de tip Kensington lock)
Certificari si conformitate	Certificare minim Microsoft Windows 11 Professional (listare pe Microsoft WCPL https://partner.microsoft.com/en-us/dashboard/hardware/search/cpl)

Componenta	Specificatii
Mouse si tasatatura	Mouse si tastatura cu fir, conector USB, cu acelasi brand cu cel al sistemului;
Sistem de operare	Windows 11 PRO - preinstalat si preactivat, cu cheie inserata in BIOS sau echivalent
Pachet Office	Licenta Microsoft Office Home & Business 2024 preinstalat, licenta perpetua sau echivalent
Antivirus	Solutie antivirus ce va asigura protecție completă împotriva tuturor tipurilor de malware: ransomware, phishing, viruși, spyware etc. - cu o valabilitate de 3 ani Solutia va fi disponibil într-o singură platformă ușor de utilizat, care acoperă toate echipamentele de tip statie personala.
Garantie	36 luni (3 ani) garantie de la data receptiei, sustinuta si certificata de producatorul echipamentelor.

3.2.3.2.7. Sistem ticketing ghișee

Funcționalitățile minimale necesare pentru automatizarea și eficientizarea preluării solicitărilor la ghișeu sunt următoarele:

- Componenta trebuie să includă minimal următoarele module hardware la nivel de locație:
  - Terminal self-service de emitere tichete care să cuprindă ecran de tip touchscreen, imprimantă termică, PC încorporat, UPS;
  - Afișoare centrale cu led-uri: 1 x afișor cumulativ central, 10 x afișor ghișeu;
  - TV LCD pentru afișare coadă clienți și materiale publicitare;
  - Unitate redare conținut video;
- Va permite ca, la sosire, clienții să intre într-o coadă de așteptare, corespunzător nevoilor lor.
- Clienții care solicită servicii complexe trebuie să poată fi gestionați separat, pentru a reduce riscul de "blocare" a altor clienți, cu un impact negativ asupra experienței lor în relația cu SPFL;
- Pentru emiterea de tichete de ordine, componenta trebuie să ofere o interfață în limba română și în limba engleză.
- Pe tichet se va tipări numărul de ordine, denumire operațiune, ora la care a fost tipărit,
- Chemarea clienților se va face cu ajutorul ecranului LCD, acesta va permite afișarea ultimelor tichete chemate, afișarea numărului tichetului nou distinct, alertă la o noua chemare.

3.2.3.2.8. Sistem infokiosk

Vor fi achiziționate 5 sisteme infokiosk cu următoarele specificații:

Componenta	Specificatii
Infochiosc tip totem	-toate componentele sistemului trebuie sa fie integrate in carcasa infochioscului -carcasa din otel de minim 1.5mm grosime, antivandal -usa securizata acces monitor / calculator -conceput pentru indoor - utilizare in interior -ventilatoare răcire echipamente comandate de thermostat -conector LAN RJ45 extern
Monitor touchscreen profesional - functionare 24/7	-diagonala 32" (80 cm) -rezolutie: 1920x1080 -luminozitate monitor: 500 nits -timp de raspuns maxim: 8 ms -unghi vizualizare minim: h/v 178/178 -MTBF minim: 50000 h -integrat in carcasa metalica a infochioscului -tehnologie touch projective capacitive cu finisare Anti-glare
Sistem PC	-sistem de operare: Licenta Windows 11 Pro preinstalata sau echivalent -procesor: Intel Core i5 Gen. 12 sau echivalent -memorie 16GB memorie instalată, DDR4 -unitate de stocare minim: 240 GB SSD -rețea Lan: 1 x 10/100/1000 integrată -USB: 5x USB 3.2 +2x USB 2.0 +1x USB 3.2 Type C -Conexiuni: WiFi, 4G
Cititor carti identitate simple/biometrice	Capabilitati de citire: -detectare automata a documentului -cotrol adaptiv al iluminarii -inlaturarea reflectiilor -compatibil ICAO 9303 specificatie patea 1-Part 1v2, Part 2, Part 3 , Part 3v2 pentru Type ID-1, ID-2 si ID-3 MRZ Optical Character Recognition -software de ocr pentru extragere nume, prenume, adresa cnp, serie CI, data expirarii. -recunoaste codurile de bare 1D și 2D - citeste noile documente de identitate contactless ICs conforme cu ISO 14443 Type A & B, BSI TR-03105
Cititor coduri de bare 1D/2D/QR	- CMOS 640x480 - QR Code, Aztec, PDF417, Micro PDF417, Data Matrix - Interfata USB HID
Imprimanta termica pentru chitante	- Direct termic rezolutie 203 dpi - Rola hartie cu latimea de 83mm - Diametru exterior rola 130 mm - Printeaza 1D și 2D
EFT POS bancar neasistat: PIN PAD+ cititor carduri bancare	- Pinpad carcasa ABS - 16 taste numerice+functii - Afisor grafic LCD 2.27" color IPS - 640 x 240 pixeli - Protectie: IP 44 - Camera integrata 2MP
Camera WEB	Full HD integrata in partea superioara a carcasei infochioscului
Garantie	36 luni (3 ani) garantie de la data receptiei, sustinuta si certificata de producatorul echipamentelor.

3.2.3.2.9. Scanner citire/verificare documente identitate

Este dispozitivul care realizează activitatea de scanare prin: OCR, validarea elementelor de securitate si descifrarea zonelor MRZ si a cip-urilor de pe documentele de identitate. Acesta va avea următoarele caracteristici:

- rezoluție de 900 dpi;
- conectivitate pentru transfer de date și alimentare prin conexiune USB 3.0;
- va permite scanarea in spectru vizibil, UV si IR in vederea identificarii elementelor de siguranta de pe documentele de identitate (zonele dedicate citirii automate ISO/IEC 7501-1 si ICAO 9303, documente RFID conform ISO 14443, ISO 7816, ICAO 9303, ISO 18013, PKI, carduri cu chip ISO 7816, ISO 7810);
- va fi protejat fizic la deschidere cu etichete ce contin elemente de siguranta.

3.3. Managementul utilizatorilor și accesul la sistem

Sistemul va permite managementul utilizatorilor utilizând un sistem bazat pe roluri astfel încât accesul la sistem să fie controlat și auditat. Va fi implementat un sistem centralizat de management al accesului la aplicații care va oferi funcționalități de single sign-on, autentificare, autorizare, administrare centralizată, managementul politicilor de acces, management în timp real al sesiunilor de aplicații și audit. Rolul acestui sistem este de creștere a securității sistemului informatic și eliminarea riscurilor potențiale, prevenirea accesului neautorizat la sistemele și aplicațiile beneficiarului, simplificarea operațiilor de administrare prin reducerea și automatizarea numărului de operațiuni administrative.

Platforma de control acces va identifica utilizatorul la începutul sesiunii de lucru prin redirectarea către un ecran de autentificare, conform politicilor de acces definite. Pentru detalii privind capabilitățile soluției de management al utilizatorilor și accesul la sistem, a se vedea cap. Soluție de gestiune a identității utilizatorilor.

Din punct de vedere operațional, toți noii utilizatori vor beneficia de instruire înainte de a fi autorizați să acceseze sistemul informatic nou creat. Sistemul nou creat va fi accesat numai de utilizatorii autorizați pe bază de conturi individuale de acces. Toate conturile de acces se vor crea numai în concordanță deplină cu politicile de acces stabilite la nivelul instituției. Toate conturile de acces vor fi administrate și drepturile de acces vor fi date pe nivele de autorizare, limitându-se accesul utilizatorilor la funcțiile și datele necesare în funcție de apartenență la grupuri/roluri.

3.4. Securitatea sistemului

Din punct de vedere al datelor gestionate, sistemul va trebui să asigure respectarea următoarelor principii:

- **Confidențialitate** - asigurarea protecției datelor împotriva accesărilor neautorizate.
- **Integritate** - asigurarea protecției, exactității și completitudinii datelor atât la nivelul modalității de stocare și gestionare a acestora, cât și pentru asigurarea împotriva manipulării frauduloase a datelor/informațiilor.
- **Disponibilitate** - prin asigurarea redundanței tuturor componentelor sistemului pentru păstrarea coerenței și necoruperii datelor.

Securitatea sistemului va urma principiile modelului de securitate „apărare în adâncime". Vor fi avute în vedere tehnologii ce ar trebui să asigure:

- securizarea serviciilor web utilizând tehnologii de tip web application firewall;
- protecția și securizarea comunicațiilor utilizând soluții firewall;
- managementul rețelei, analiza și raportarea logurilor de securitate provenite de la echipamentele de securizare a sistemului;
- managementul vulnerabilităților și al actualizărilor (de ex. identificarea vulnerabilităților înainte de a fi exploatate de către utilizatori malițioși, aplicare automată a actualizărilor de securitate, dezactivarea serviciilor sistemului de operare care nu sunt utilizate etc.);
- actualizarea permanentă și în mod automat a aplicațiilor;
- implementarea unui sistem anti-malware care să asigure implementarea politicilor de securitate în mod centralizat pentru end-point-uri și mașini virtuale;
- implementarea unui sistem de control acces care permite autentificarea utilizatorilor și administratorilor conform zero-trust security model;
- auditarea activităților realizate în sistem și a solicitărilor de acces la serviciile expuse prin intermediul platformei.

Noul sistem va implementa toate măsurile de securitate necesare în vederea protejării acestuia conform legislației naționale în domeniu precum și a standardelor internaționale specifice.

3.4.1. Cadrul legislativ aplicabil în domeniul securității cibernetice

În concepția, analiza și proiectarea sistemului informatic trebuie să se ia in calcul:

- respectarea Regulamentului general de protecția datelor (UE) 2016/679, a Directivei (UE) 2016/680 și a legii 190/2018 și a legii 363/2018
- respectarea Directivei europene de securitate cibernetică (UE 2022/2555) privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniunea Europeană (Directiva NIS 2), precum și a actelor normative naționale de transpunere a acesteia. OUG 155/2024;
- respectarea legii nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei
- Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148
- Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019R0881

- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. https://legislatie.just.ro/Public/DetaliiDocument/209670
- Ordonanță de Urgență nr. 119 din 22 iulie 2020 pentru modificarea și completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. https://legislatie.just.ro/Public/DetaliiDocument/228369

Legislație secundară

- HG nr.963/2020 pentru aprobarea Listei serviciilor esențiale. https://legislatie.just.ro/Public/DetaliiDocument/233193, https://dnsc.ro/vezi/document/hg-963-2020
- HG nr. 976/2020 privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale. https://legislatie.just.ro/Public/DetaliiDocument/233298 https://dnsc.ro/vezi/document/hg-976-2020
- HG nr. 1003/2020 NORME TEHNICE de stabilire a impactului incidentelor pentru categoriile de operatori de servicii esențiale și furnizori de servicii digitale. https://legislatie.just.ro/Public/DetaliiDocument/235108 https://dnsc.ro/vezi/document/hg-1003-2020-norme-tehnice-stabilire-impact-incidente
- Ordinul nr. 600/2019 privind aprobarea Normelor metodologice de organizare și funcționare a Registrului operatorilor de servicii esențiale. https://legislatie.just.ro/Public/DetaliiDocument/215629 https://dnsc.ro/vezi/document/ordin-mcsi-600-2019
- Ordinul nr. 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale. http://legislatie.just.ro/Public/DetaliiDocument/216121 https://dnsc.ro/vezi/document/ordin-mcsi-599-2019
- Ordinul nr. 601/2019 pentru aprobarea Metodologiei de stabilire a efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale. https://legislatie.just.ro/Public/DetaliiDocument/216151 https://dnsc.ro/vezi/document/ordin-mcsi-601-2019
- Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale. https://legislatie.just.ro/Public/DetaliiDocument/233775 https://dnsc.ro/vezi/document/osgg-1323-2020
- Ordinul nr. 559/2021 559 privind aprobarea Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică. https://legislatie.just.ro/Public/DetaliiDocument/240988 https://dnsc.ro/vezi/document/ordin-sgg-nr-559-2021-regulament-asc
- Ordinul nr. 105/11.10.2022 pentru aprobarea Normelor de aplicare a dispozițiilor privind verificarea și controlul îndeplinirii obligațiilor de securitate cibernetică

pentru spațiul cibernetic național
https://legislatie.just.ro/Public/DetaliiDocumentAfis/260933
https://dnsc.ro/vezi/document/ordin-dnsc-nr-105-2022-norme-control

- Ordinul nr. 106/14.10.2022 pentru aprobarea Normelor privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică. https://legislatie.just.ro/Public/DetaliiDocument/261244
https://dnsc.ro/vezi/document/ordin-dnsc-nr-106-2022-norme-furnizori-de-servicii-de-formare
- Decizia 88/30.04.2020 privind aprobarea Listei standardelor și specificațiilor europene și internaționale
https://legislatie.just.ro/Public/DetaliiDocument/226520
https://dnsc.ro/vezi/document/decizia-dnsc-nr-88-2020-lista-standarde-si-specificatii-europene-si-internationale
- Decizia nr. 301/22.12.2021 pentru aprobarea Listei cuantumului tarifelor pentru servicii din activitățile prevăzute la art. 22 alin.(1) lit. l), art. 32 alin. (2) lit. c) și e) și la art. 33 alin. (2) lit. c) și e) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare. https://legislatie.just.ro/Public/DetaliiDocument/250129
https://dnsc.ro/vezi/document/decizia-dnsc-nr-301-2021-lista-cuantum-tarife-activitati-dnsc

Reglementări/ghiduri/cerințe specifice

- Ghid practic identificarea operatorilor de servicii esentiale. https://dnsc.ro/vezi/document/cert-ro-ghid-identificare-ose
- Ghid practic identificarea furnizorilor de servicii digitale. https://dnsc.ro/vezi/document/ghid-practic-identificare-fsd

3.5. Confidențialitatea datelor

Confidențialitatea este o activitate de bază pentru furnizarea serviciilor publice.

Accesul la datele stocate în sistem va fi protejat corespunzător, iar accesul va fi auditat permanent.

Sistemul de gestiune a bazelor de date va oferi facilități de criptare pentru anumite câmpuri.

Orice conexiune cu sistemul va fi realizată prin metode securizate (SSL) sau canale de comunicație criptate (VPN). De asemenea, fișierele de tip log vor fi analizate periodic în vederea identificării posibilelor intruziuni.

În cadrul proiectului se vor respecta următoarele principii:

- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- respectarea Regulamentului general de protecția datelor (UE) 2016/679, a Directivei (UE) 2016/680 și a legii 190/2018 și a legii 363/2018
- respectarea Directivei europene de securitate cibernetică (Directiva NIS2 EU 2022/2555) și transpunerea ei în România prin OUG 155/2024;

- că respectă cerințele și obligațiile juridice privind **protecția și confidențialitatea datelor** recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

De asemenea, se va asigura respectarea legislației privind protecția datelor, prin:

- **„Planuri de gestionare a riscurilor"** pentru identificarea riscurilor, evaluarea potențialului impact al acestora și planificarea intervențiilor cu măsuri tehnice și organizatorice adecvate. Pe baza ultimelor evoluții tehnologice, aceste măsuri trebuie să asigure un nivel de securitate proporțional cu gradul de risc;
- **„Planuri de continuitate a activității"** și **„planuri de rezervă și de redresare"** pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucerea tuturor funcțiilor la situația normală cât mai curând posibil;
- Un **„plan de acces la date și autorizare"** care stabilește persoanele care au acces la date, datele care sunt accesibile și condițiile accesării datelor, pentru a asigura confidențialitatea. Accesul neautorizat și încălcarea normelor de securitate trebuie monitorizat, și măsurile corespunzătoare pentru a preveni orice repetare a încălcărilor trebuie documentate și planificate.

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

Nr. Crt.	Proiect	Obiective specifice	Plan de acțiune	Lista indicativă de intervenții complementare
1.	"Soluții informatice integrate pentru optimizarea activității administrative, creșterea competențelor și a nivelului de calitate a serviciilor publice pentru cetățeni și mediul de afaceri la nivelul municipiului Ploiești", cod proiect 129737, cofinanțat din Fondul Social European prin Programul Operațional Capacitate Administrativă 2014 - 2020 (proiect finalizat)	1. Implementarea unor mecanisme și proceduri standard - Plan Strategic Instituțional 2020 - 2024, pentru a crește eficiența acțiunilor administrative la nivelul Municipiului Ploiești; 2. Optimizarea proceselor administrative ale Primăriei prin implementarea unui sistem informatic integrat de management al calității și performanței care să asigure gestiunea, monitorizarea și evaluarea continuă a calității și performanței administrației Municipiului Ploiești; 3. Simplificarea furnizării serviciilor către cetățeni și mediul de afaceri, prin implementarea unui sistem informatic/platforme integrate de tip portal web Centru de Inovare și Inițiativă Civică pentru creșterea implicării funcționarilor primăriei și a transparenței actului	1. Realizarea unui Plan Strategic Instituțional aferent perioadei 2020 - 2024; 2. Implementarea unei Platforme informatice integrate de management al calității și performanței și un sistem informatic/platformă integrată de tip portal web Centru de Inovare și Inițiativă Civică; 3. Instruirea a 50 de persoane din cadrul grupului țintă în ceea ce privește utilizarea soluțiilor informatice implementate în cadrul proiectului, respectiv instruite și certificate pe teme specifice ale administrației publice locale; Echipamente achiziționate: server, sistem de stocare centralizat, switch, firewall, rack cu UPS.	➢ Simplificarea furnizării serviciilor către cetățeni și mediul de afaceri, prin implementarea unui sistem informatic/platforme integrate de tip portal web Centru de Inovare și Inițiativă Civică pentru creșterea implicării funcționarilor primăriei și a transparenței actului administrativ și îmbunătățirea mecanismelor de control; ➢ Îmbunătățirea abilităților și cunoștințelor personalului Municipiului Ploiești în domeniul utilizării sistemelor informatice dezvoltate prin proiect și, totodată, îmbunătățirea competențelor profesionale ale unui număr de 50 de persoane din diferite niveluri ierarhice din cadrul Municipiului Ploiești pe teme specifice;

Nr. Crt.	Proiect	Obiective specifice	Plan de acțiune	Lista indicativă de intervenții complementare
		administrativ și îmbunătățirea mecanismelor de control; 4. Îmbunătățirea abilităților și cunoștințelor personalului Municipiului Ploiești în domeniul utilizării sistemelor informatice dezvoltate prin proiect și, totodată, îmbunătățirea competențelor profesionale ale unui număr de 50 de persoane din diferite niveluri ierarhice din cadrul Municipiului Ploiești pe teme specifice;		➢ Achiziția de echipamente TIC: server, sistem stocare centralizat, switch, firewall, rack cu UPS.
2.	"Investiții integrate și complementare în măsuri de planificare strategice și măsuri de simplificare la nivelul Municipiului Ploiești", cofinanțat din Fondul Social European prin Programul Operațional Capacitate Administrativă 2014 - 2020, Cod SMIS 136182 (proiect finalizat)	1. Definirea politicii locale a Municipiului Ploiești cu concursul tuturor factorilor cu aport în dezvoltarea locală, concretizată prin adoptarea a 2 documente strategice: Strategia Integrată de Dezvoltare Urbană pentru perioada 2021 - 2027 și Planul de Mobilitate Urbană Durabilă 2021 - 2030, corelat cu SIDU. 2. Implementarea de măsuri de eficientizare a proceselor de lucru specifice domeniului asistenței sociale atât din perspectivă back-office, cât și front-office. 3. Dezvoltarea abilităților personalului din cadrul Primăriei	1. Implementarea unei aplicații software de arhivare electronică și de managementul documentelor ELO DMS; 2. Crearea unui portal de servicii pentru cetățeni; 3. Instruirea a 20 de persoane din grupul țintă în domeniul SMART CITY MANAGEMENT, inclusiv prin abordarea temelor de dezvoltare durabilă, egalitate de șanse, nediscriminare și egalitate de gen;	1. Implementarea unei aplicații software de arhivare electronică și de managementul documentelor ELO DMS; 2. Crearea unui portal de servicii pentru cetățeni; 3. Instruirea a 20 de persoane din grupul țintă în domeniul SMART CITY MANAGEMENT, inclusiv prin abordarea temelor de dezvoltare durabilă, egalitate de șanse, nediscriminare și egalitate de gen;

Nr. Crt.	Proiect	Obiective specifice	Plan de acțiune	Lista indicativă de intervenții complementare
		prin formarea a 20 de persoane in domeniul SMART CITY MANAGEMENT.		
3.	Proiectul propus la finanțare "TIMPUL TĂU E PREȚIOS, NU-L PIERDE LA COZI ȘI GHIȘEE! DIGITALIZAREA ESTE SOLUȚIA!"	1. Optimizarea serviciilor publice electronice oferite cetățenilor și mediului de afaceri de către SPFL Ploiești; 2. Creșterea gradului de maturitate digitală a Municipiului Ploiești cu peste 60% față de situația inițială (momentul Raportului auditului inițial)	1. Dezvoltarea de servicii digitale publice optimizate: depunerea și eliberarea online specializată a certificatelor fiscale, înregistrări privind impunerea clădirilor, terenurilor, mijloacelor de transport, eliberarea de documente din arhivă către entitățile interesate; 2. Crearea unui portal de servicii publice ca poartă unică de acces a cetățenilor și societăților comerciale către serviciile publice oferite de SPFL Ploiești.	1. Portal de servicii publice furnizate cetățenilor și mediului de afaceri de către SPFL Ploiești; 2. Instruirea angajaților SPFL Ploiești pentru utilizarea și administrarea sistemului informatic integrat propus; 3. Achiziții de echipamente hardware și software;

Totodată, menționăm faptul că proiectul propus la finanțare este complementar și cu Cloud-ul Guvernamental care va reuni într-o singură arhitectură informatică întreaga administrație publică din România.

Principalele beneficii ale operaționalizării cloud-ului guvernamental pentru cetățeni sunt:

1. ***One-stop shop*** - acces direct la toate serviciile publice, prin folosirea formularelor electronice disponibile în cloud;
2. **Statul român - accesibil la un click distanță** - pentru că toate instituțiile vor fi interconectate în cloud, cetățeanul va putea solicita și primi documente de oriunde, oricând;
3. **Economie de timp** - fără cozi, fără nicio deplasare fizică la instituțiile publice;
4. **Trasabilitate** - cetățeanul va putea avea un istoric al interacțiunilor sale cu administrația;
5. **Siguranță** - cloud-ul guvernamental va beneficia de **cele mai avansate sisteme de securitate cibernetică** disponibile.

Cloud-ul va aduce beneficii concrete și pentru activitatea administrativă:

1. va asigura interoperabilitatea sistemelor publice;
2. va reduce birocrația, prin eliminarea proceselor administrative redundante sau perimate;
3. va asigura o mai bună colaborare și o partajare rapidă a informațiilor între toate instituțiile guvernamentale;
4. va eficientiza costurile - instituțiile publice nu vor mai fi nevoite să asigure mentenanța pentru echipamentele hardware și software.

De asemenea, Cloud-ul Guvernamental va produce beneficii și pentru mediul privat:

1. antreprenorul va putea găsi într-un singur loc toate serviciile publice electronice, precum și toate avizele și autorizațiile care îi sunt necesare, integrate cu platforma care procesează plățile pentru aceste servicii (Ghișeul.ro), cu platforma de autentificare a identității digitale (PSCID) și cu platforma de gestionare electronică a achizițiilor publice (SEAP) - Ghișeul.ro, SEAP și PSCID sunt platforme informatice administrate de ADR;
2. creșterea eficienței aparatului administrativ va determina creșterea încrederii antreprenorilor în performanța statului și va genera creștere economică.

Sistemul informatic propus prin proiect va fi găzduit în Cloud-ul Guvernamental, astfel că toate soluțiile software incluse în proiectul tehnic, inclusiv aplicația de impozite și taxe locale, sistemul de management al documentelor, portalul cetățenilor, call center, soluția de e-learning, soluțiile de securitate cibernetică, etc, vor fi instalate și configurate în Cloud-ul Guvernamental

4. RESURSE

4.1. Personal și instruire

4.1.1. Personal

Echipa de proiect este formată din 7 membri, componența fiind stabilită în baza **Dispoziției nr. 3688/03.10.2024** privind nominalizarea membrilor Unității de Implementare a Proiectului **"TIMPUL TĂU E PREȚIOS, NU-L PIERDE LA COZI ȘI GHIȘEE! DIGITALIZAREA ESTE SOLUȚIA!", Cod SMIS 336834:**

1. **Irina Elena NĂSTASE** - Consilier Serviciul Relații Internaționale, proiecte cu finanțare internațională, ONG și implementare proiecte, având calitatea de **Manager de proiect;**
2. **Bianca Mariana PASCU** - Referent Serviciul Relații Internaționale, proiecte cu finanțare internațională, ONG și implementare proiecte, având calitatea de **Asistent manager;**
3. **Sorina NĂSTASE** - Consilier Direcția Tehnic-Investiții, având calitatea de **Responsabil tehnic;**
4. **Ileana SIMION** - Consilier Direcția Economică, având calitatea de **Responsabil economic;**
5. **Ioana Geanina SERBINOV** - Consilier juridic Direcția Administrație Publică, Juridic-Contencios, Achiziții Publice, Contracte, având calitatea de **Responsabil juridic;**
6. **Mariana NAE** - Consilier Serviciul Informatică, având calitatea de **Responsabil IT;**
7. **Iuliana RĂDULESCU** - Consilier Direcția Administrație Publică, Juridic-Contencios, Achiziții Publice, Contracte, având calitatea de **Responsabil achiziții.**

Rolul **Managerului de proiect** (*Cod COR 242101 - Manager proiect*) va consta în:

- Asigurarea managementului general al proiectului, urmărind îndeplinirea obiectivelor acestuia, cu respectarea activităților proiectului și a prevederilor contractului de finanțare;
- Organizarea și coordonarea echipei de proiect;
- Cooperarea în scopul atingerii obiectivelor proiectului, a tuturor factorilor implicați;
- Monitorizarea și controlarea modului de realizare a etapelor proiectului, a modului de desfășurare a fiecărei activități în conformitate cu graficul planificării activităților;
- Supervizarea modului de întocmire a dosarului proiectului care conține toate documentele generate în cadrul proiectului, inclusiv documentația tehnică, documentele livrate în cadrul proiectului, contractele încheiate cu furnizorii/prestatorii, corespondența purtată pe perioada derulării proiectului, înregistrările efectuate în derularea proiectului;

- Evaluarea modului în care fiecare membru al echipei de proiect își desfășoară activitatea;
- Monitorizează măsurile de informare și publicitate;

Rolul **Asistentului manager de proiect** (*Cod COR 334303 - Asistent manager*) va consta în:

- Participă la ședințele lunare de progres în cadrul cărora se va analiza evoluția proiectului din punctul de vedere al cheltuielilor, utilizării resurselor, implementării activităților, obținerii rezultatelor și managementul riscurilor;
- Oferă suport în pregătirea vizitelor în teren ale reprezentanților ADR;
- Asigură activități de secretariat în pregătirea dosarelor de rambursare;
- Asigură activități de secretariat în pregătirea dosarelor de plată;
- Asigură activități de secretariat în pregătirea documentelor pentru audit;
- Oferă asistență în implementarea unui sistem de arhivare și management al documentelor aferente proiectului;
- Asigură suport pentru întocmirea notelor;
- Asistă ceilalți membri UIP în vederea respectării regulilor privind măsurile de identitate vizuală în conformitate cu contractul de finanțare;
- Asigură suport pentru întocmirea notelor informative, comunicărilor oficiale, respectiv a actelor adiționale ale contractului de finanțare încheiat între beneficiar și finanțator;
- Participă la ședințele de monitorizare a progresului proiectului;

Rolul **Responsabilului tehnic** (*Cod COR 112024 - Director tehnic*) va consta în:

- Oferă input tehnic pentru pregătirea documentației de atribuire a contractului de achiziție servicii informatice implementare sistem informatic integrat de gestionare a activității SPFL Ploiești, licențe, echipamente hardware, servicii de instalare, configurare și PIF, securitate cibernetică, inclusiv instruire personal;
- Participă la identificarea cerințelor tehnice și funcționale ale sistemului informatic integrat de gestionare a activității SPFL Ploiești;
- Participă la recepția finală a sistemului informatic integrat de gestionare a activității SPFL Ploiești, a infrastructurii hardware și software aferente, precum și a serviciilor de instruire a personalului care va utiliza și administra soluția software rezultată prin proiect;

Rolul **Responsabilului economic** (*Cod COR 331302 - Contabil*) va consta în:

- Asigură îndeplinirea tuturor obligațiilor de natură financiară, rezultate ca urmare a derulării proiectului în cauză;
- Urmărește și verifică eligibilitatea tuturor cheltuielilor efectuate, asigură controlul costurilor proiectului;
- Verifică și avizează rapoartele de natură financiară trimise de contractori și, pe baza acestora, pregătește cererile de prefinanțare/rambursare/plată adresate finanțatorului;
- Supraveghează și certifică încadrarea în bugetul proiectului a tuturor acțiunilor generatoare de cheltuieli aferente proiectului;
- Asigură din punct de vedere financiar respectarea obligațiilor asumate prin contractul de finanțare încheiat cu autoritatea de management;
- Asigură coerența financiară a proiectului;
- Verifică asigurarea realizării cash-flow-ului pentru toată durata de implementare a proiectului;
- Participă la ședințele de monitorizare a progresului proiectului;
- Participă, la solicitare, la vizitele de monitorizare ale reprezentanților finanțatorului;

Rolul **Responsabilului juridic** (*Cod COR 261103 - Consilier juridic*) va consta în:

- Participă, alături de ceilalți membri ai UIP-ului, la elaborarea unor instrucțiuni privind modul de desfășurare a activității UIP cu privire la aspectele nereglementate de legislația în vigoare;
- Aduce la cunoștința managerului de proiect orice modificări legislative ce intervin în domeniul în care se implementează proiectul, ca urmare a informării transmise de către Serviciul Relația cu Consiliul Local, Reglementare;
- Verifică legalitatea documentelor cu caracter juridic primite spre avizare;
- Acordă asistență, consultanță și reprezentare juridică reprezentanților Solicitantului implicați în implementarea proiectului;
- Propune soluții de rezolvare a cererilor cu caracter juridic referitoare la activitățile derulate în cadrul proiectului;
- Redactează și/sau verifică documente juridice pe parcursul derulării proiectului;
- În îndeplinirea atribuțiilor sale, consilierul juridic are obligația de a respecta prevederile art. 4 din Legea nr. 514/2003;

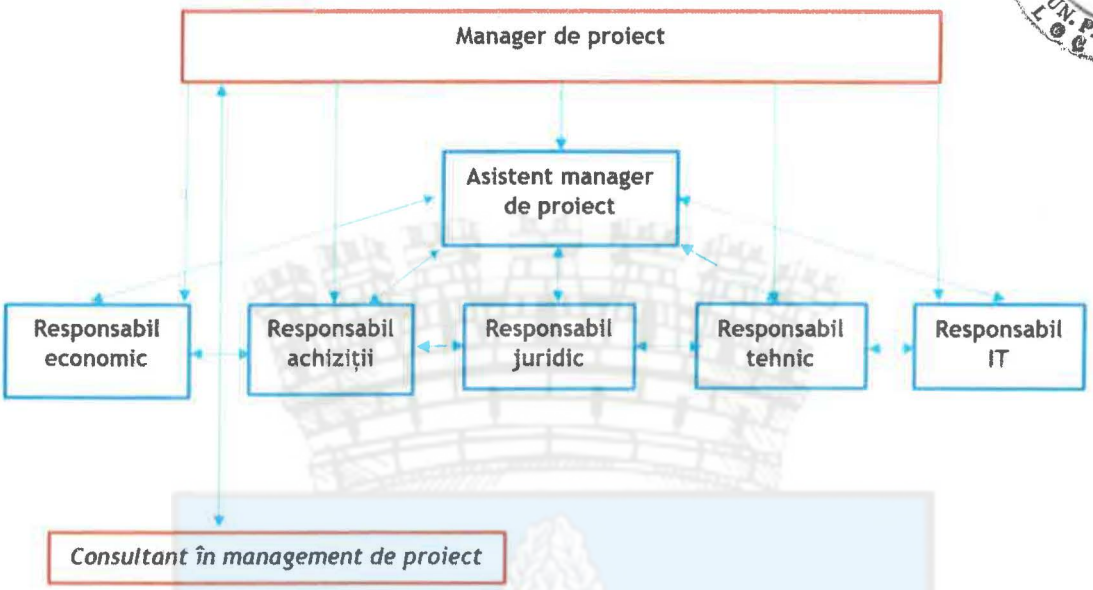
Rolul **Responsabilului IT** (*Cod COR 251206 - Manager proiect informatic*) va consta în:

- Furnizează informații privind sistemul informatic existent în vederea extinderii coordonate a acestuia cu noile soluții introduse în proiect;
- Validează livrabilele IT din proiect;
- Asigură asistență de specialitate IT echipei de proiect;

Rolul **Responsabilului achiziții** (*Cod COR 214946 - Expert achiziții publice*) va consta în:

- Asigură parcurgerea tuturor etapelor și operațiunilor desfășurate în procesul de achiziție publică în conformitate cu legislația în vigoare;
- Întocmirea programului achizițiilor publice;
- Chemarea la competiție; publicarea invitației/anunțului de participare, punerea la dispoziție a documentelor de atribuire;
- Atribuirea contractului de achiziție publică;
- Realizarea dosarului de achiziție publică;
- Întocmirea de acte adiționale, dacă este cazul;
- Furnizarea informațiilor necesare în scopul întocmirii și transmiterii documentelor de achiziție atașate dosarelor de plată/rambursare;
- Face parte din comisia de evaluare a ofertelor depuse în cadrul procedurilor de achiziții publice și asigură verificarea, completă și corectă, a îndeplinirii criteriilor de calificare/selecție și a cerințelor privind modul de elaborare a ofertei tehnico-financiare;

Organigrama proiectului



Solicitantul are o **strategie clară** pentru monitorizarea implementării și post-implementării proiectului, după cum urmează:

I. Monitorizarea implementării proiectului:

1. **Definirea indicatorilor de performanță:**
   - ✓ **Indicatori cantitativi:** Progresul activităților (% finalizat), costurile (% din buget utilizat), numărul de utilizatori implicați.
   - ✓ **Indicatori calitativi:** Gradul de satisfacție a beneficiarilor, nivelul de conformitate cu specificațiile.
2. **Stabilirea responsabilităților:**

✓ Echipa de management (Manager de proiect și Asistent manager) monitorizează activitățile curente.

✓ Responsabilii de arii specifice (financiar, tehnic, legal) furnizează rapoarte regulate.

3. **Implementarea instrumentelor de monitorizare:**

✓ Software-uri de management de proiect (ex. Microsoft Project);

✓ Rapoarte de progres săptămânale sau lunare;

✓ Ședințe regulate pentru actualizarea situației;

4. **Audituri și verificări periodice:**

✓ Controale interne pentru conformitate cu planul și reglementările.

✓ Audit financiar pentru verificarea eligibilității cheltuielilor efectuate în cadrul proiectului.

5. **Comunicare constantă:**

✓ Menținerea unei linii deschise între echipa de proiect și părțile interesate.

Monitorizarea implementării proiectului va fi realizată de Managerul de proiect, conform următorului calendar:

Activități de monitorizare	Perioada de monitorizare (fiecare celulă reprezintă 1 lună calendaristică)																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Ședințe de monitorizare																								
Controlul costurilor																								
Rapoarte de activitate întocmite de consultant																								
Rapoarte de progres fizic și valoric intermediar																								

II. Monitorizarea post-implementării proiectului:

1. **Evaluarea performanței rezultatelor:**

✓ Măsurarea utilizării platformei sau serviciului creat.

✓ Colectarea datelor privind impactul asupra grupurilor țintă.

2. **Feedback de la utilizatori:**

✓ Chestionare online, focus-grupuri, interviuri pentru a înțelege gradul de satisfacție și problemele întâmpinate.

3. **Mentenanța și suportul tehnic:**

✓ Asigurarea funcționării continue a platformei sau serviciului.

✓ Rezolvarea problemelor raportate de utilizatori.

4. **Actualizări și îmbunătățiri:**

✓ Implementarea modificărilor în baza sugestiilor și a noilor cerințe.

5. **Raportarea rezultatelor:**

✓ Rapoarte finale către finanțator, evidențiind impactul și eficiența proiectului.

Monitorizarea post-implementării proiectului se va realiza, anual, de către Managerul de proiect prin urmărirea realizării obiectivelor strategice menționate anterior.

Plan de acțiuni pentru monitorizare:

Etapă	Activități cheie	Responsabil	Instrumente
Monitorizare implementare	Colectarea datelor de progres, verificarea conformității activităților	Manager de proiect	Gantt chart, Rapoarte de progres trimestrial
Monitorizare utilizare	Analizarea traficului platformei și a numărului de utilizatori	Responsabil IT, Responsabil tehnic	Google Analytics, Feedback utilizatori
Gestionarea riscurilor	Monitorizarea incidentelor tehnice și aplicarea soluțiilor rapide	Responsabil IT, Responsabil tehnic	Loguri de erori, Rapoarte de securitate
Îmbunătățiri post-lansare	Actualizarea funcționalităților pe baza feedback-ului primit	Furnizor sistem informatic integrat Responsabil IT, Responsabil tehnic	Sisteme de suport tehnic
Evaluarea impactului final	Raportarea indicatorilor de rezultat și analiza sustenabilității	Manager de proiect, Auditor financiar, Auditor de maturitate digitală	Raport de progres final, Rapoarte anuale de durabilitate

O strategie clară de monitorizare a implementării și post-implementării proiectului garantează controlul asupra progresului și asigură succesul pe termen lung al rezultatelor. Cheia este utilizarea unor instrumente adecvate, raportarea regulată și implicarea tuturor actorilor relevanți în procesul de evaluare și ajustare.

În vederea asigurării unei implementări adecvate cu prevederile contractului de finanțare și din dorința de a asigura o implementare de succes a proiectului, Solicitantul a decis contractarea unui furnizor cu experiență în derularea proiectelor cu finanțare europeană. Decizia de contractare a unui consultant în management de proiect este susținută și de faptul că Municipiul Ploiești deține un portofoliu vast de proiecte și un număr limitat de angajați, o repartizare echitabilă a sarcinilor acestora conform fișelor de post făcând necesară și asigurarea unor resurse externe pentru a reduce presiunea asupra echipei interne astfel încât proiectele să se poată derula conform termenelor agreate prin contractele de finanțare, fără întârzieri datorate supra-alocării angajaților în condițiile în care aceștia sunt nevoiți să gestioneze mai multe sarcini sau proiecte, ceea ce poate conduce la suprasolicitare și, implicit, la scăderea productivității.

Consultantul în management de proiect va avea următoarele sarcini:

- → monitorizează derularea activităților din cadrul proiectului conform prevederilor contractului de finanțare;
- → asigură interfața de comunicare dintre solicitant și finanțator;
- → întocmește rapoartele trimestriale de progres privind stadiul fizic și valoric realizat, comparativ cu cel estimat, în scopul urmăririi progresului proiectului și al stadiului îndeplinirii indicatorilor de realizare și rezultat, al respectării planului de monitorizare a proiectului și al realizării indicatorilor de etapă din plan; încarcă raportul de progres în aplicația MySmis 2021 împreună cu documentele justificative la intervale de 3 luni calendaristice;
- → urmărește îndeplinirea indicatorilor de etapă din planul de monitorizare a proiectului;
- → verifică eligibilitatea cheltuielilor, în conformitate cu prevederile legale privind eligibilitatea;
- → verifică plata efectivă de către Beneficiar a sumelor incluse în cererile de rambursare/plată;
- → întocmește cererile de rambursare/plată/prefinanțare;
- → actualizează graficul cererilor de rambursare/plată/prefinanțare în funcție de sumele decontate;
- → întocmește documentația aferentă propunerilor de notificări/acte adiționale, după caz;
- → verifică păstrarea de către Beneficiar a tuturor documentelor originale legate de proiect;
- → verifică atingerea rezultatelor și obiectivelor asumate prin proiect;
- → verifică finalizarea tuturor activităților proiectului;
- → întocmește rapoartele de durabilitate pe perioada post-implementare;

Activitățile de management ce vor face obiectul contractului de servicii de management al proiectului (delegate contractantului):

1. elaborare rapoarte de progres trimestrial/durabilitate;
2. întocmire cereri de plată/rambursare/prefinanțare;
3. întocmire notificări/acte adiționale, după caz;
4. verificarea eligibilității cheltuielilor, în conformitate cu prevederile legale privind eligibilitatea;
5. verificarea bunurilor/serviciilor/lucrărilor - dacă au fost livrate/prestate în conformitate cu contractele de achiziții;
6. verificarea utilizării de către beneficiar a conturilor contabile analitice (cu codificarea proiectului);

7. verificarea finalizării tuturor activităților proiectului,
8. verificarea atingerii țintelor indicatorilor în conformitate cu valorile asumate prin contractul de finanțare (cu modificările ulterioare, dacă este cazul);
9. verificarea atingerii rezultatelor și obiectivelor asumate prin proiect;
10. urmărirea și validarea îndeplinirii indicatorilor de etapă din planul de monitorizare a proiectului.

Modul în care va fi monitorizată și controlată activitatea contractantului care va furniza servii de management de proiect

Monitorizarea consultantului în management de proiect va include următoarele aspecte, fără a se limita doar la acestea:

- livrarea documentelor și a rapoartelor de progres trimestrial la intervale de 3 luni calendaristice, în termen de 30 de zile de la finalizarea perioadei de raportare. Primul Raport de progres trimestrial se va întocmi pentru trimestrul calendaristic următor semnării contractului de finanțare în cadrul PR SM 2021 - 2027;
- autorizarea rapoartelor de progres de către ADR SM;
- verificarea respectării și autorizării de către ADR SM a indicatorilor de etapă menționați în planul de monitorizare;
- autorizarea cererilor de rambursare/plată/prefinanțare de către ADR SM;
- calitatea transferului de know-how către membrii echipei de proiect propuse de Solicitant, prin evaluarea conținutului materialelor transmise beneficiarului și a temelor propuse spre rezolvare membrilor echipei de proiect, precum și prin evaluarea post-implementare a prestației echipei consultantului în cadrul proiectului;
- calitatea și transparența sistemului de arhivare și înregistrare a informațiilor, va fi monitorizată prin ușurința accesului specialiștilor care vor efectua auditurile la nivel de proiect la documente;
- verificarea atingerii țintelor indicatorilor în conformitate cu valorile asumate prin contractul de finanțare (cu modificările ulterioare, dacă este cazul);
- verificarea atingerii rezultatelor și obiectivelor asumate prin proiect;

Monitorizarea consultantului de management de proiect se va face atât prin prisma calității și a conformității documentelor de proiect transmise, cât și în cadrul întâlnirilor organizate la nivelul proiectului în vederea monitorizării progresului acestuia, prin aprecierea coerenței și a corectitudinii informațiilor transmise.

Calendarul activităților de monitorizare a activității derulate de consultantul în management de proiect:

Activități de monitorizare	Perioada de monitorizare (fiecare celulă reprezintă 1 lună calendaristică)																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Ședințe de monitorizare																								
Controlul costurilor																								
Rapoarte de activitate întocmite de consultant																								
Rapoarte de progres fizic și valoric intermediar																								

Monitorizarea consultantului în management de proiect va fi realizată de Managerul de proiect, Responsabilul economic și de către Responsabilul juridic.

Managerul de proiect va monitoriza următoarele aspecte:

1. atingerea țintelor indicatorilor în conformitate cu valorile asumate prin contractul de finanțare (cu modificările ulterioare, dacă este cazul);
2. atingerea rezultatelor și obiectivelor asumate prin proiect;
3. finalizarea tuturor activităților proiectului;
4. respectarea planului de monitorizare a proiectului și îndeplinirea indicatorilor de etapă;
5. întocmirea rapoartelor de progres trimestrial la intervale de 3 luni calendaristice, în termen de 30 de zile de la finalizarea perioadei de raportare, precum și autorizarea acestora de către AM;
6. conformitatea activităților obligatorii de comunicare și vizibilitate aferente proiectului cu prevederile contractului de finanțare și ale Ghidului de Identitate Vizuală al PRSM 2021-2027;
7. calitatea informației furnizate de consultant.

Responsabilul economic va monitoriza următoarele aspecte:

1. gestionarea bugetului proiectului;
2. pregătirea documentelor necesare pentru cererile de plată/rambursare;
3. asigurarea trasabilității tuturor cheltuielilor și justificarea lor în raport cu activitățile proiectului;
4. asigurarea respectării regulilor privind eligibilitatea cheltuielilor, conform ghidului solicitantului și altor reglementări europene;
5. respectarea procedurilor financiare și a termenelor stabilite în contractul de finanțare;

6. autorizarea cererilor de rambursare/plată/prefinanțare de către ADR SM;
7. măsurile propuse pentru minimizarea impactului riscurilor financiare care ar putea afecta implementarea proiectului.

Responsabilul juridic va monitoriza următoarele aspecte:

1. Conformitatea întocmirii notificărilor și a actelor adiționale la contractul de finanțare cu anexele specifice propuse de ADR SM în Manualul Beneficiarului, respectiv cu prevederile contractului de finanțare și ale legislației naționale și europene relevante pentru proiect;
2. Capacitatea de identificare a riscurilor juridice potențiale în derularea proiectului;
3. Capacitatea de a elabora documente clare, precise și conforme cu cerințele legale;

Predarea livrabilelor de management către Beneficiar (rapoarte de progres, cereri de rambursare/plată/prefinanțare, notificări, acte adiționale, orice alt document necesar în cadrul proiectului) se va face în baza unui proces verbal de predare - primire și a unui raport de activitate întocmite de consultant și acceptate de Beneficiar.

4.1.2. Instruire

Prin proiect, va fi asigurată creșterea capacității administrative a Solicitantului în domeniul digitalizării prin:

1. pregătirea personalului care va utiliza sistemul informatic integrat propus pentru gestionarea activității SPFL Ploiești, precum și echipamentele hardware achiziționate prin proiect (utilizatori);
2. pregătirea personalului care va asigura administrarea și mentenanța echipamentelor achiziționate prin proiect și a sistemului informatic integrat propus prin proiect (administratori).

Sesiunile de instruire a utilizatorilor și administratorilor vor fi asigurate de furnizorul sistemului informatic integrat și al echipamentelor hardware.

Beneficiarul, împreună cu furnizorul, vor stabili de comun acord datele de început ale cursurilor de instruire pe baza planificării proiectului și disponibilității cursanților, durata acestora, precum și locația de desfășurare.

Beneficiarul va stabili, la nivel intern, lista participanților la cursurile de instruire și va comunica Managerului de Proiect din partea Furnizorului lista de cursanți.

În funcție de tipul și caracteristicile utilizatorilor sistemului informatic, se vor desfășura următoarele categorii de cursuri:

Tip instruire	Număr utilizatori	Durată instruire
Instruire administratori sistem informatic integrat și echipamente hardware, instruire privind egalitatea de șanse și nediscriminarea	3	Sesiune în clasă dedicată cu o durată de o zi, minim 4h/zi
Instruire utilizatori cheie sistem informatic integrat, instruire privind egalitatea de șanse și nediscriminarea	17	Sesiune în clasă dedicată cu o durată de 2 zile, minim 4h/zi
Instruire online a utilizatorilor prin cursuri video înregistrate pentru principalele module ale proiectului, instruire GDPR, instruire pentru securitate cibernetică și instruire privind egalitatea de șanse și nediscriminarea	125	30 module video cu o durată de maxim 10 minute fiecare

Tipuri de instruire:

- **Cursuri destinate administratorilor** - vor cuprinde tematici precum administrarea sistemului, administrarea bazelor de date, monitorizarea performanțelor, securitatea sistemului (inclusiv securitate cibernetică), asistența utilizatorilor etc. Echipa de administrare a beneficiarului va fi instruită de către furnizor astfel încât să poată asigura funcționarea sistemului cu o asistență minimă din partea furnizorului sau independent de acesta, începând cu perioada post-implementare. În urma instruirii administratorilor, aceștia trebuie să dobândească toate competențele necesare bunei gestiuni a sistemului și asigurării capacității acestora de a transfera, la rândul lor, informațiile necesare către noi utilizatori sau administratori care pot interveni în exploatarea sistemului IT.
- **Cursuri destinate utilizatorilor cheie** - acest tip de instruire este destinat utilizatorilor sistemului informatic și se va derula după finalizarea testării funcționale a sistemului implementat, incluzând tematici cu privire la utilizarea noului sistem implementat. Instruirea va cuprinde și un modul cu privire la securitatea informației și a sistemului informatic, precum și la protejarea datelor cu caracter personal și la legislația aplicabilă, instruire privind egalitatea de șanse și nediscriminarea. Instruirea va fi de tip „train the trainer", utilizatorii instruiți de către Prestator asigurând, la rândul lor, instruirea celorlalți utilizatori.
- **Cursuri destinate instruirii online** - acest tip de instruire **online** este destinat utilizatorilor sistemului informatic și se va derula după finalizarea testării

funcționale a sistemului implementat, incluzând tematici cu privire la utilizarea noului sistem implementat. Această instruire se va realiza prin cursuri video înregistrate pentru principalele module ale proiectului, instruire GDPR, instruire pentru securitate cibernetică și instruire privind egalitatea de șanse și nediscriminarea.

Resurse materiale necesare instruirii

Instruirea se va face pe baza suportului de curs, livrat de furnizor, în format fizic sau electronic, fiecărui participant. Acest suport de curs va conține exemple practice pentru o mai bună înțelegere a modului de funcționare și administrare a sistemului, precum și alte detalii legate de acesta.

Manuale și documentație

Prestatorul va pune la dispoziția beneficiarului toate manualele și documentațiile în limba română, cu excepția documentațiilor tehnice ale echipamentelor și software-ului de bază, furnizate de producători, care pot fi în limba engleză.

Întreaga documentație de utilizare și administrare a sistemului, va fi livrată în format electronic odată cu produsul în sine. De asemenea, acestea vor fi incluse și în portal pentru a facilita accesul la respectivele documente.

La sfârșitul fiecărei sesiuni de instruire se vor elabora documentele:

- prezență la curs/diplomă de participare;
- raport activitate de instruire realizat de către instructor.

Numărul mare de utilizatori (145) din cadrul SPFL Ploiești a făcut necesară instruirea acestora, în etape, cu ajutorul unei platforme online de instruire, rațiunea alegerii unei astfel de metode de instruire fiind dată de faptul că nu toți angajații din cadrul SPFL Ploiești pot întrerupe programul de lucru pentru activități de formare în regim clasic. Instruirea online a utilizatorilor prin elearning se adaptează programului acestora, permițând învățarea în ritm propriu, atunci când programul de lucru o permite. Suplimentar, s-a avut în vedere instruirea de tip „train the trainer" a unor utilizatori cheie care vor asigura la nevoie suport celorlalți utilizatori.

4.1.2.1. Platforma instruire video utilizatori

Aplicația va fi instalată pe mașinile virtuale puse la dispoziție de Cloudul Guvernamental și va permite instruirea utilizatorilor online prin cursuri video înregistrate pentru principalele module ale proiectului, instruire GDPR, instruire pentru securitate cibernetică și instruire privind egalitatea de șanse și nediscriminarea..

Funcționalități minime:

- Aplicația va permite integrarea cu servicii director și/sau cu soluția de management a autentificării utilizatorilor (identity managment);
- Aplicația va permite adăugarea de materiale de curs in diverse formate și a chestionarelor de evaluare și organizarea acestora pe categorii și fluxuri de instruire;
- Aplicația va fi achiziționată cu conținut video pentru protecția datelor cu caracter personal minim 10 module în limba Română;

- Aplicația va fi achiziționată cu conținut video pentru egalitatea de șanse și nediscriminarea minim un modul în limba Română;
- Aplicația va fi achiziționată cu conținut video pentru securitate cibernetică, minim 15 module în limba Română;
- Aplicația va fi achiziționată cu chestionare online de evaluare a cunoștințelor cu minim 3 întrebări pentru fiecare modul de instruire în parte, în limba Română;
- Aplicația va permite generarea de rapoarte de instruire a utilizatorilor;
- Aplicația va permite instruirea periodică a tuturor utilizatorilor;
- Vor fi achiziționate servicii pentru crearea a cel puțin 30 module video suplimentare cu o durată de maxim 10 minute fiecare pentru aplicațiile livrate în cadrul proiectului către beneficiar. Acestea vor fi însoțite de chestionare de evaluare a cunoștințelor. Instruirile și chestionarele vor fi în limba română.

4.2. Resurse materiale

Pentru buna implementare a proiectului, solicitantul va asigura la sediul său din Piața Eroilor, Nr. 1 A din Municipiul Ploiești, Județul Prahova capacitatea operațională și administrativă necesară implementării proiectului propus la finanțare. Resursele materiale deținute și utilizate de Solicitant pentru buna implementare a proiectului sunt reprezentate de:

- sediul solicitantului, precum și dotările necesare pentru întâlnirile echipei de proiect și desfășurării activităților acestora;
- baza logistică: mobilier (birouri, scaune, dulapuri pentru arhivarea fizică a documentelor proiectului) și echipamente IT, precum o multifuncțională și laptopuri pentru fiecare membru al echipei de proiect;
- mijloace de comunicație (telefonie și conexiune internet);
- site-ul solicitantului, pentru o comunicare și promovare eficientă și completă a rezultatelor proiectului.

5. MENTENANȚĂ ȘI SUSTENABILITATE

5.1. Mentenanță

Se va asigura suport și garanție pe o perioadă de 3 ani de la punerea în funcțiune pentru sistemul informatic dezvoltat.

Toate produsele hardware și software, precum și toate soluțiile achiziționate vor dispune de garanție pentru o perioadă de 3 ani de la punerea în funcțiune și își vor menține același nivel de performanță, ca la livrare, pe toată perioada de garanție.

Beneficiarul va asigura toate resursele umane, materiale și financiare în perioada post-implementare pentru a susține funcționalitățile implementate în cadrul proiectului.

Soluția tehnică a fost dimensionată pentru a asigura scalabilitatea software și hardware a aplicației. Vor exista proceduri clare de administrare (backup/restaurare/reconfigurare) a sistemului și manuale de utilizare.

În cadrul perioadei de garanție se vor asigura:

- rezolvarea bug-urilor care nu au fost identificate în timpul implementării și care apar în faza de producție;
- întreținerea și buna funcționare a sistemului furnizat în parametrii agreați (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- instalarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- instalarea de noi versiuni oferite de producător ale produselor COTS, în condițiile în care arhitectura sistemului și constrângerile o permit;
- actualizarea manualelor de utilizare și altor documente în urma efectuării corecțiilor;
- reparații/înlocuiri ale componentelor defecte la locația de instalare a beneficiarului;
- consiliere și suport telefonic 8 ore pe zi, de luni până vineri în cadrul programului normal de lucru al beneficiarului, prin serviciul Help-desk atât pentru produsele hardware, cât și software;
- toate incidentele vor fi gestionate prin intermediul unei aplicații software de gestionare a tichetelor;
- remediere software de la distanță cu acordul beneficiarului;
- actualizări software la locația de instalare a beneficiarului sau de la distanță;
- reconfigurări hardware și software la nivelul inițial solicitat în cazul în care erorile apărute nu sunt datorate beneficiarului;
- mentenanță preventivă periodică;
- consiliere și suport tehnic pentru posibilități de extindere a soluției existente;
- managementul vulnerabilității, precum și teste de penetrare anuale.

Mentenanța sistemului informatic integrat pentru gestionarea activității SPFL propus prin proiect este esențială pentru asigurarea funcționării optime, securității și actualizării continue. Aceasta implică un set de activități tehnice și administrative menite să prevină problemele, să remedieze erorile și să îmbunătățească sistemul pe termen lung.

Tipuri de mentenanță:

1. Mentenanța corectivă: implică identificarea și remedierea erorilor și disfuncționalităților apărute în sistem;
2. Mentenanța preventivă: se efectuează periodic pentru a preveni apariția problemelor;
3. Mentenanța evolutivă: implică adaptarea și îmbunătățirea continuă a sistemului pentru a răspunde nevoilor în schimbare;

Activitățile de mentenanță constau în:

1. Monitorizare și diagnosticare prin utilizarea unor instrumente automate pentru monitorizarea performanței și detectarea timpurie a erorilor, analiza alertelor de securitate;

2. Actualizări și pach-uri prin instalarea regulată a actualizărilor de securitate pentru a preveni vulnerabilitățile și implementarea noilor versiuni software pentru a îmbunătăți performanța și funcționalitățile;
3. Securitate cibernetică prin detectarea și prevenirea atacurilor cibernetice prin firewall-uri, sisteme de detectare a intruziunilor și criptare, respectiv prin managementul accesului utilizatorilor și aplicarea unor politici stricte de autentificare;
4. Backup și recuperare prin realizarea backup-urilor periodice pentru protecția datelor împotriva pierderii sau coruperii și prin stabilirea unor proceduri clare de recuperare în caz de defecțiuni majore;
5. Suport tehnic și asistență pentru utilizatori prin oferirea de suport tehnic prin call center sau email pentru rezolvarea problemelor utilizatorilor și prin crearea unor ghiduri pentru utilizatori.

Mentenanța va fi asigurată din fondurile proprii ale Beneficiarului în perioada de durabilitate și va avea rolul de a asigura că sistemul funcționează fără întreruperi majore, oferind servicii constante cetățenilor. Protejează datele sensibile împotriva atacurilor și accesului neautorizat și prevenirea problemelor costisitoare prin mentenanță preventivă.

Mentenanța sistemului informatic integrat propus prin proiect este un proces continuu, esențial pentru asigurarea eficienței, securității și accesibilității serviciilor digitale. O strategie de mentenanță bine definită contribuie la creșterea satisfacției utilizatorilor și la funcționarea stabilă a sistemului pe termen lung.

5.2. Sustenabilitate

Sustenabilitatea proiectului propus la finanțare vizând dezvoltarea unui sistem informatic integrat pentru gestionarea activității SPFL Ploiești depinde de o serie de factori, printre care menționăm planificarea resurselor financiare, tehnologiile utilizate în dezvoltarea sistemului informatic integrat, acceptarea sistemului de către utilizatori și impactul asupra mediului.

Sustenabilitatea financiară a proiectului este dată de faptul că beneficiarul deține resurse financiare suficiente și o stabilitate instituțională pe termen lung pentru susținerea activităților proiectului în etapa post-implementare. Instituția solicitantă promovează o politică bugetară eficientă care îi permite continuarea activităților din proiectul propus la finanțare, la aceasta adăugându-se și oportunitățile viitoare de atragere a fondurilor nerambursabile care să susțină creșterea acțiunilor de digitalizare a activităților instituției pentru oferirea unor servicii publice performante către cetățeni/mediul de afaceri.

Automatizarea proceselor și digitalizarea fluxurilor de lucru ale SPFL Ploiești pentru furnizarea unor servicii digitale îmbunătățite către cetățeni și mediul de afaceri pot contribui la reducerea costurilor administrative și la obținerea unor economii semnificative pe termen lung. În plus, funcționarii publici se pot concentra pe activitățile esențiale, în locul celor repetitive.

Dimensiunea tehnologică a sustenabilității este dată de scalabilitatea și flexibilitatea sistemului informatic integrat pentru gestionarea activității SPFL Ploiești care trebuie să fie capabil să se adapteze la creșterea numărului de utilizatori și la evoluția tehnologică. Sistemul informatic propus este proiectat astfel încât să permită adăugarea de noi funcționalități și să fie interoperabil prin integrarea cu alte sisteme

(guvernamentale/private) pentru o utilizare eficientă, pe termen lung. Tehnologia implementată va fi flexibilă pentru a putea răspunde evoluțiilor legislative, sociale sau tehnologice.

Pentru atragerea utilizatorilor și menținerea încrederii acestora, este crucială protejarea datelor cetățenilor prin măsuri avansate de securitate cibernetică. De asemenea, planificarea mentenanței prin stabilirea unui cadru clar pentru întreținerea și actualizarea sistemului informatic reprezintă o premisă pentru o utilizare eficientă, pe termen lung, a acestuia.

Dimensiunea socială a sustenabilității vizează accesibilitatea și incluziunea digitală, în sensul că sistemul trebuie să fie ușor de utilizat pentru toate categoriile sociale, inclusiv pentru persoanele cu dizabilități sau cele mai puțin familiarizate cu tehnologia. Acest lucru înseamnă că proiectul propus la finanțare contribuie la reducerea decalajului digital prin facilitarea accesului la tehnologie pentru toate categoriile sociale. Pentru ca sistemul informatic integrat dezvoltat prin proiect să poată fi folosit de angajații SPFL Ploiești, furnizorul sistemului va asigura tutoriale, manuale de utilizare și cursuri de pregătire a utilizatorilor în vederea dezvoltării abilităților și cunoștințelor necesare pentru creșterea gradului de adopție a aplicației software implementate în cadrul proiectului. În plus, cetățenii Municipiului Ploiești care vor utiliza sistemul informatic propus prin proiect vor fi implicați în dezvoltarea și îmbunătățirea sistemului prin solicitarea unui feedback constant.

Resursele umane incluse în Unitatea de Implementare a Proiectului vor fi menținute și pe perioada de durabilitate a proiectului pentru transferabilitatea cunoștințelor dobândite pe parcursul implementării proiectului în generarea unor noi proiecte care să crească valoarea adăugată a serviciilor publice furnizate de SPFL Ploiești.

Dimensiunea ecologică a sustenabilității este dată de faptul că sistemul informatic propus prin proiect va fi găzduit în Cloud-ul Guvernamental, ceea ce va contribui la reducerea amprentei de carbon. Regimul de exploatare a echipamentelor de cloud guvernamental poate fi optimizat pentru procesare masivă în afara orelor de maximă sarcină, când se va lucra cu energie mai ieftină sau din surse alternative. Controlul configurațiilor și al sarcinii de calcul se face folosind soluțiile de virtualizare, ceea ce îmbunătățește factorul de utilizare al energiei - reducând timpii morți, când sistemele așteaptă sarcini noi, fără să execute comenzi utile. Optimizarea multifactorială a utilizării energiei electrice și termice reduce direct emisiile de dioxid de carbon (CO_2) din centralele și generatoarele de energie folosind combustibili fosili (gaz, păcură sau cărbune).

Serviciile publice electronice elimină sau minimalizează nevoia de a imprima sau fotocopia documente și, prin urmare, reduc cererea pentru hârtie cu efect pozitiv asupra mediului înconjurător prin reducerea defrișărilor și a poluării. În acest mod, se reduc și spațiile de arhivare a dosarelor solicitărilor legate de serviciile publice care ar fi necesitat un consum ridicat de diverse utilități (în special electricitate), ceea ce are iar un impact pozitiv asupra mediului înconjurător.

Transformarea proceselor fizice în procese digitale permite contribuabililor să acceseze serviciile online, diminuând emisiile de carbon asociate transportului până la ghișeele instituției publice prin reducerea deplasărilor fizice.

Impactul pozitiv asupra mediului este dat și de utilizarea în proiect a unor echipamente IT conforme cu standardele de eficiență energetică.

Dimensiunea instituțională și legislativă a sustenabilității este dată de conformitatea sistemului informatic integrat propus prin proiect cu legislația națională și europeană privind protecția datelor și securitatea cibernetică și de susținerea proiectului pe termen

lung de către factorii de decizie din cadrul instituției solicitante pentru a genera valoare adăugată atât la nivelul administrației publice, cât și pentru cetățeni și mediul de afaceri.

Sistemul informatic integrat pentru gestionarea activității SPFL Ploiești este unul sustenabil daca este eficient economic, scalabil tehnologic, acceptabil social, ecologic și conform cu reglementările legale în vigoare.

Caracterul durabil al proiectului propus la finanțare depinde de modul în care acesta răspunde nevoilor pe termen lung ale cetățenilor, asigură eficiența administrativă și protejează mediul. Prin implementarea de soluții scalabile, incluzive și ecologice, astfel de proiecte devin piloni ai modernizării și sustenabilității în sectorul public.

Data: 25.02.2025

Întocmit: S.C. BASIC RESAL S.R.L.,

VASILESCU CRISTINA SIMONA,

Administrator

[redacted]