Ministerul Agriculturii și Dezvoltării Rurale
Agenția de Plăți și Intervenție pentru Agricultură
Bd. Carol I nr. 17, sector 2, București
fax 021.3054.900 www.apia.org.ro

Nr. 2167/28.10.2025

Mihaela Stanescu
Digitally signed by Mihaela Stanescu
Date: 2025.12.23 14:36:47 +02'00'

Se aprobă,
DIRECTOR GENERAL,
Gabriela Nicoleta ANDREI

PROPUN SPRE APROBARE
DIRECTOR GENERAL ADJUNCT,
Constantin MIHAI

CAIET DE SARCINI

pentru achiziția publică având ca obiect:
Servicii de dezvoltare a Sistemului Informatic Integrat pentru
”Portalul unic al fermierilor solicitanți ai sprijinului în agricultură gestionat de Agenția de Plăți și Intervenție pentru Agricultură”

Cod CPV principal:
72212900-8 Diverse servicii de dezvoltare de software şi sisteme informatice
Coduri CPV secundare: 32420000-3 Echipament de rețea, 32424000-1 Infrastructură de rețea, 80511000-9 - Servicii de formare a angajatilor, 48820000 2 servere, 30000000-9 – Echipamente IT, 30233000-1 - Dispozitive de stocare și citire, 30232000-4 – Echipament periferic

2025

Cuprins

1. INTRODUCERE 6
2. CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII 7
2.1. INFORMAȚII DESPRE AUTORITATEA CONTRACTANTĂ 7
2.2. INFORMAȚII DESPRE CONTEXTUL CARE A DETERMINAT ACHIZIȚIA 7
2.3. INFORMAȚII DESPRE BENEFICIILE ANTICIPATE DE CĂTRE AUTORITATEA CONTRACTANTĂ 8
2.4. FACTORII INTERESAȚI ȘI ROLUL ACESTORA 9
3. DESCRIREA SERVICIILOR SOLICITATE 10
3.1. OBIECTUL CONTRACTULUI 10
3.2. DESCRIEREA SITUAȚIEI ACTUALE LA NIVELUL BENEFICIARULUI 10
3.2.1. Cadrul legislativ 10
3.2.2. Structura organizatorică 12
3.2.3. Sistemul informatic existent 17
3.2.4. Prezentarea serviciilor publice oferite 25
3.3. OBIECTIVELE GENERALE ȘI SPECIFICE LA CARE CONTRIBUIE FURNIZAREA PRODUSELOR ȘI PRESTAREA SERVICIILOR 25
4. CERINȚE GENERALE PRIVIND SOLUȚIA TEHNICĂ 27
4.1. CERINȚE GENERALE 27
4.2. PREVEDERI DE SECURITATE 28
5. CERINȚELE FUNCȚIONALE ALE SISTEMULUI 31
5.1. CERINȚE FUNCȚIONALE 31
5.1.1. Portal public în vederea asigurării accesului cetățenilor la informații și servicii publice digitale 31
Funcționalități suplimentare ce ar trebui asigurate prin Portalul Public: 31
5.1.2. Sistem de management / gestiune a documentelor 32
Beneficii 44
Conformitate legală 45
5.2. ARHITECTURA FUNCȚIONALĂ A SISTEMULUI 45
5.3. MANAGEMENTUL UTILIZATORILOR ȘI ACCESUL LA SISTEM 48
5.4. SECURITATEA SISTEMULUI 49
5.5. CONFIDENȚIALITATEA DATELOR 51
5.6. ARHITECTURA TEHNICĂ 52
5.6.1. Dimensionarea componentelor funcționale și a celor de suport ale mediului de producție 53
5.7. COMPONENTA DE INFRASTRUCTURĂ HARDWARE 53
5.7.1. Componentele hardware și de comunicații 53

5.7.2. Platformă de virtualizare hiperconvergentă 68
5.7.3. Scannere de mare viteză 71
5.8. COMPONENTELE SOFTWARE 72
5.8.1. Componenta de portal 72
5.8.2. Componenta pentru managementul documentelor 79
Funcționalitate de recunoaștere a întrebărilor/documentelor similare 85
Funcționalitate de alertă și blocare a răspunsurilor către beneficiari cu dosare/procese în curs 85
Cerințe funcționale: 85
Avantaje: 86
5.8.3. Componenta de business process management (BPM) 90
5.8.4. Componenta integrată de gestiune și analiză a datelor 91
5.8.5. Componenta de analiză și raportare avansată a datelor 98
5.8.6. Componenta de integrare și pregătire a datelor (ETL) 100
5.8.7. Componenta de interoperabilitate 101
5.8.8. Componenta pentru administrarea identității utilizatorilor 108
5.8.9. Componenta de securizare a accesului privilegiat 114
5.8.10. Componenta de monitorizare a performanței aplicațiilor 116
5.8.11. Componenta inteligentă de optimizare automată a resurselor 117
5.8.12. Componenta de mascare a datelor 119
5.8.13. Componenta de service desk 122
5.8.14. Componenta de protecție a datelor (salvare / restaurare) 125
5.8.15. Componenta de monitorizare infrastructură 129
5.8.16. Componenta de instruire în vederea conștientizării securității pentru utilizatori și administratori 136
5.8.17. Componenta de monitorizare evenimente de securitate (SIEM) 138
5.9. SERVICII 144
5.9.1. Serviciile de livrare, instalare echipamente hardware 144
5.9.2. Serviciile de livrare, instalare și dezvoltare software 146
5.9.3. Testarea și asigurarea calității sistemului 153
6. INSTRUIRE UTILIZATORI - INCLUSIV CONȘTIENTIZARE SECURITATE INFORMATICĂ 157
7. GARANȚIA 159
8. ATRIBUȚII ȘI RESPONSABILITĂȚI ALE PĂRȚILOR 164
8.1. OBLIGAȚIILE AUTORITĂȚII CONTRACTANTE: 165
8.2. OBLIGAȚIILE OFERTANTULUI DEVENIT CONTRACTANT 165
8.2.1. Obligațiile generale ale Ofertantului devenit Contractant 165
8.2.2. Obligațiile specifice ale Ofertantului devenit Contractant 166
9. IPOTEZE ȘI RISCURI 169

9.1. IPOTEZE 169
9.2. RISCURI 169
10. ABORDAREA, METODOLOGIA ȘI PLANUL DE LUCRU ÎN CADRUL CONTRACTULUI 172
10.1. METODOLOGIA PENTRU REALIZAREA SERVICIILOR 173
10.2. PLANUL DE LUCRU 174
10.3. GRAFIC DE PRESTARE 175
11. LOCUL ȘI DURATA DESFĂȘURĂRII ACTIVITĂȚILOR 177
11.1. LOCUL DESFĂȘURĂRII ACTIVITĂȚILOR 177
11.2. DURATA CONTRACTULUI 177
12. RESURSE NECESARE / EXPERTIZA NECESARĂ 178
12.1. NUMĂRUL DE EXPERȚI PE CATEGORIE DE EXPERTIZĂ 179
12.2. EXPERȚII PRINCIPALI (EXPERȚII CHEIE) 180
12.3. PROFILUL EXPERȚILOR CHEIE 183
12.3.1. Expert cheie nr. 1: Manager de proiect 183
12.3.2. Expert cheie nr. 2: Expert Analist business 184
12.3.3. Expert cheie nr. 3: Expert Arhitect de sistem 184
12.3.4. Expert cheie nr. 5: Expert coordonator testare 185
12.3.5. Expert cheie nr. 5: Expert implementare Portal 186
12.3.6. Expert cheie nr. 6: Expert implementare soluție management documente 187
12.3.7. Expert cheie nr. 7: Expert implementare soluție de gestiune a utilizatorilor 188
12.3.8. Expert cheie nr. 8: Expert software monitorizare date, sisteme și aplicații 188
12.3.9. Expert cheie nr. 9: Expert implementare soluție de Asistență Tehnică / Service Desk 189
12.3.10. Expert cheie nr. 10: Expert implementare soluție de virtualizare 190
12.3.11. Expert cheie nr. 11: Expert hardware și rețele 190
12.3.12. Expert cheie nr. 12: Expert securitate informatică 191
12.4. ALTE CONDIȚII REFERITOARE LA CALIFICAREA EXPERȚILOR 191
12.5. EXPERȚI SECUNDARI (EXPERȚI NON-CHEIE) 192
12.6. PERSONALUL ADMINISTRATIV ȘI PERSONALUL SUPORT / BACKSTOPPING PENTRU ACTIVITATEA EXPERȚILOR PRINCIPALI ÎN CADRUL CONTRACTULUI 193
12.7. RESURSELE CONTRACTANTULUI, NECESARE PENTRU DESFĂȘURAREA ACTIVITĂȚILOR CONTRACTULUI 194
12.8. INFRASTRUCTURA CONTRACTANTULUI NECESARĂ PENTRU DESFĂȘURAREA ACTIVITĂȚILOR CONTRACTULUI 194
12.9. INFRASTRUCTURA ȘI RESURSELE DISPONIBILE LA NIVEL DE AUTORITATE CONTRACTANTĂ PENTRU ÎNDEPLINIREA CONTRACTULUI 195

13. MANAGEMENTUL/GESTIONAREA CONTRACTULUI ȘI ACTIVITĂȚI DE RAPORTARE.....196
13.1. GESTIONAREA RELAȚIEI DINTRE CONTRACTANT ȘI AUTORITATEA CONTRACTANTĂ 196
13.1.1. Ședințe / întâlniri.....197
13.1.2. Modalitatea de abordare a eventualelor cereri de schimbare / modificări nesubstanțiale 198
13.1.3. Opțiuni de suplimentare fără a se depăși valoarea maximă aprobată a proiectului.....198
13.2. RAPORTAREA ÎN CADRUL CONTRACTULUI 198
13.3. EVALUAREA PERFORMANȚEI FURNIZORULUI 200
13.3.1. Termenele de prestare.....200
13.3.2. Nivelul de calitate a livrabilelor.....201
14. RECEPȚIA PRODUSELOR ȘI SERVICIILOR 203
14.1. RECEPȚIA PRODUSELOR.....204
14.2. RECEPȚIA SERVICIILOR.....206
14.3. LIVRABILE PENTRU PRODUSELE FURNIZATE ȘI SERVICIILE PRESTATE.....206
14.4. FINALIZAREA SERVICIILOR ÎN CADRUL CONTRACTULUI 208
14.5. MONITORIZAREA REALIZĂRII ACTIVITĂȚILOR ȘI A REZULTATELOR PE PERIOADA DERULĂRII CONTRACTULUI.....208
14.6. ASIGURAREA CALITĂȚII 208
15. MODALITĂȚI ȘI CONDIȚII DE PLATĂ.....210
16. CERINȚE GENERALE PREDARE CODURI SURSĂ 212
17. MODUL DE PREZENTARE A OFERTELOR TEHNICE.....214
18. CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT 217
18.1. LEGISLAȚIE EUROPEANĂ 218
18.2. LEGISLAȚIE NAȚIONALĂ 218
18.3. CONFLICT DE INTERESE 219
18.4. CONFIDENȚIALITATE.....219
18.5. DREPTURI DE PROPRIETATE INTELECTUALĂ 220
19. INFORMAȚII SUPLIMENTARE / ADMINISTRATIVE.....222

1. INTRODUCERE

Această secțiune a Documentației de Atribuire include ansamblul cerințelor pe baza cărora fiecare Ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru implementarea sistemului informatic integrat care face obiectul Contractului ce rezultă din această procedură.

În cadrul acestei proceduri, **Agenția de Plăți și Intervenție pentru Agricultură** (denumită în continuare **APIA**) îndeplinește rolul de Autoritate Contractantă, respectiv Achizitor în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

Acolo unde sunt menționate produse de o anumită origine, sursa, producție, un procedeu special, o marca de fabrica sau de comerț, un brevet de invenție, o licență de fabricație, se va citi "sau echivalent". Aceste specificații tehnice care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație sunt menționate doar pentru identificarea cu ușurință a tipului de produs și NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse din cadrul procedurii.

Ofertanții trebuie să răspundă integral cerințelor minime incluse în Caietul de sarcini și într-o formă care nu limitează aria sau serviciile solicitate.

În acest sens, orice ofertă prezentată care se abate de la prevederile Caietului de sarcini, va fi luată în considerare numai în măsura în care Propunerea Tehnică presupune asigurarea unui nivel calitativ superior cerințelor minime obligatorii din Caietul de sarcini.

Nu se admit oferte parțiale din punct de vedere cantitativ și calitativ, ci numai oferte integrale, care corespund tuturor cerințelor minime stabilite prin prezentul Caiet de sarcini.

2. CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII

2.1. INFORMAȚII DESPRE AUTORITATEA CONTRACTANTĂ

Agenția de Plăți și Intervenție pentru Agricultură (**APIA**) este instituția de specialitate a administrației publice centrale, înființată în anul 2004 în subordinea Ministerului Agriculturii și Dezvoltării Rurale, cu personalitate juridică, finanțată integral de la bugetul de stat, responsabilă cu gestionarea unor forme de sprijin destinate susținerii agriculturii românești, finanțate din Fondul European de Garantare Agricolă (FEGA), Fondul European Agricol pentru Dezvoltare Rurală (FEADR) și din bugetul național (BN).

Conducerea APIA este asigurată de un director general numit, în condițiile legii, prin ordin al ministrului agriculturii și dezvoltării rurale, care are calitatea de ordonator secundar de credite și care, în exercitarea atribuțiilor sale, emite decizii.

Directorul general este sprijinit în activitatea sa de trei directori generali adjuncți numiți prin decizie a directorului general APIA.

La nivelul APIA funcționează ca organism consultativ Comitetul director – organism colectiv de analiză și evaluare, cu rol consultativ, care ia hotărâri în problemele privind activitatea APIA, cu excepția celor care, potrivit legii, sunt în competența altor organisme. Componența Comitetului este stabilită prin decizie a directorului general.
APIA este organizată pe nivel central și nivel județean. In cadrul centrelor și județene se regăsesc și centrele locale. Structura organizatorică se regăsește pe site-ul APIA.

2.2. INFORMAȚII DESPRE CONTEXTUL CARE A DETERMINAT ACHIZIȚIA

Conform Raportului de activitate pentru anul 2023, de la aderarea României la Uniunea Europeană, APIA a derulat fonduri europene și naționale destinate susținerii agriculturii românești și fermierilor români de peste 40 de miliarde euro, având o rată medie anuală a absorbției fondurilor de peste 96%.
Dacă în anul 2007 APIA derula mai puțin de 10 forme de sprijin destinate fermierilor români, în noua perioadă de programare 2023-2027, din cele 89 intervenții incluse în noul Plan Strategic PAC al României, 63 vor fi implementate de APIA, iar din cele 15 miliarde de euro alocate României, mai mult de 12 miliarde vor fi gestionate de APIA. În ultimii ani, APIA a început procesul de digitalizare al proceselor de primire cereri, de gestionare a acestora în cadrul aplicațiilor informatice, dar datorită constrângerilor bugetare nu s-a reușit integrarea unui sistem de management al documentelor pe relația cu cetățenii, beneficiari ai fondurilor europene sau potențiali beneficiari.

În acest context, la nivelul APIA s-a identificat necesitatea și oportunitatea dezvoltării unui sistem informatic integrat de tip platformă, cloud ready, modern, modular, colaborativ și interoperabil cu alte sisteme informatice, sistem care va facilita accesul cetățenilor, mediului privat și instituțiilor și autorităților publice la serviciile publice oferite de către APIA. În cadrul sistemului se vor implementa atât servicii publice integral electronice, cu grad mare de sofisticare (transmitere integral electronică a dosarelor aferente solicitărilor, precum și primirea electronică a răspunsurilor sau a documentelor solicitate), cât și servicii publice parțial electronice, cu grad mai scăzut de sofisticare (transmitere electronică a solicitării și ulterior ridicare a documentelor emise de la ghișee sau doar accesul la formulare tipizate sau simpla informare cu privire la procedurile necesare în vederea obținerii unui anumit serviciu).

Proiectul este finanțat prin Programul Creștere Inteligentă, Digitalizare și Instrumente Financiare 2021-2027 (PCIDIF), Măsura 1: Servicii publice destinate cetățenilor și/sau firmelor, Acțiunea 2.2.1: E-guvernare și digitalizare în beneficiul cetățenilor.

Achiziția sistemului informatic integrat este esențială pentru realizarea obiectivelor proiectului în termenul stabilit.

2.3. INFORMAȚII DESPRE BENEFICIILE ANTICIPATE DE CĂTRE AUTORITATEA CONTRACTANTĂ

Beneficiile implementării proiectului se regăsesc, în primul rând, în calitatea serviciilor oferite către cetățeni (G2C), dar și la nivel instituțional.

Implementarea sistemului informatic integrat va transforma fundamental modul în care **APIA** interacționează cu cetățenii, entitățile reglementate și autoritățile partenere, generând beneficii semnificative. Prin digitalizarea proceselor, sistemul va reduce timpul și costurile asociate gestionării cererilor de licențe, avize și petiții, permițând o procesare mai rapidă și mai precisă.

Beneficiile create de proiect sunt multiple, atât pentru cetățeni/mediul de afaceri/instituțiile administrației publice, cât și pentru **APIA**.

Principalele beneficii identificabile și directe ale realizării proiectului propus sunt prezentate în continuare:

- Pentru cetățeni:
    - Facilitarea modului de interacțiune: metodă structurată de a trimite solicitări, întrebări sau reclamații, cu posibilitatea de a urmări progresul acestora;
    - Facilitatea de a programa online întâlniri sau consultări, eliminând necesitatea deplasărilor inutile sau a așteptării la coadă;
    - Primirea de notificări personalizate privind statusul solicitărilor, scadențele importante, sau alerte de interes public;
    - Descărcarea și/sau completarea online a formularelor necesare pentru atingerea obiectivelor APIA, acela de a pune la dispoziția celor interesați unelte și fluxuri pentru depunerea de cereri și documente justificative în vederea obținerii fondurilor europene destinate agriculturii, instrucțiuni pas cu pas pentru diverse proceduri administrative.
    - Urmărirea în timp real a stadiului de autorizare și plată a dosarului depus, oferind transparență și predictibilitate privind procesul de evaluare și decontare a fondurilor
- Pentru personalul angajat în cadrul APIA:
    - Organizarea documentelor într-un format electronic centralizat;
    - Posibilitatea unei planificări mai eficiente a zilei de lucru și reducerea aglomerației din spațiile de primire a publicului;
    - Organizarea eficientă a solicitărilor, prioritizarea în funcție de urgență și gestionarea eficientă a timpului;
    - Comunicarea eficientă cu un număr mare de cetățeni, fără a fi nevoie de eforturi manuale repetitive;
    - Reducerea timpului petrecut cu distribuirea și explicarea formularelor către cetățeni, și centralizarea informațiilor;
    - Asigurarea securității datelor.

Rezultatele așteptate în urma proiectului sunt următoarele:

- Rezultat 1: **Procese optimizate la nivelul APIA** pentru digitalizarea serviciilor publice pe relația cu cetățeni și mediul de afaceri;
- Rezultat 2: Un **sistem informatic integrat de tip platformă**, cloud ready, modern, modular, colaborativ și interoperabil cu alte sisteme informatice, pentru furnizarea către cetățeni a informațiilor necesare pe fluxurile de lucru specifice APIA;
- Rezultat 3: **Servicii publice digitalizate dezvoltate/optimizate**;
- Rezultat 4: **Asigurarea infrastructurii hard** pentru funcționarea acestuia până la migrarea în cloud;
- Rezultat 5: **Personal instruit** pentru administrarea și utilizarea sistemului informatic integrat dezvoltat în vederea facilitării accesului cetățenilor și mediului de afaceri la servicii publice digitalizate – se va stabili un număr de persoane (angajați ai APIA) instruite pentru administrarea și utilizarea sistemului informatic dezvoltat.

2.4. FACTORII INTERESAȚI ȘI ROLUL ACESTORA

Proiectul implică mai multe categorii de părți interesate, fiecare cu roluri distincte:

- Cetățenii persoane fizice și persoanele juridice de drept privat beneficiari direcți ai diferitelor scheme de plată operate și aflate în responsabilitatea APIA
- autoritățile și instituțiile publice implicate care trebuie să furnizeze date sau input pentru furnizarea serviciilor publice aflate în responsabilitatea APIA
- autoritățile și instituțiile publice care beneficiază de date și informații furnizate de APIA pentru serviciile publice aflate în responsabilitatea lor
- angajații APIA care vor utiliza sistemul informatic în vederea furnizării serviciilor publice.

3. DESCRIREA SERVICIILOR SOLICITATE

3.1. OBIECTUL CONTRACTULUI

Scopul principal al contractului este implementarea „la cheie" a Sistemului Informatic Integrat pentru *"Portalul unic al fermierilor solicitanți ai sprijinului în agricultură gestionat de Agenția de Plăți și Intervenție pentru Agricultură"*, în conformitate cu cerințele din prezentul caiet de sarcini.

Obiectul principal al contractului este reprezentat de prestarea de servicii IT pentru implementarea Sistemului Informatic Integrat pentru *"Portalul unic al fermierilor solicitanți ai sprijinului în agricultură gestionat de Agenția de Plăți și Intervenție pentru Agricultură"*, în conformitate cu cerințele din prezentul caiet de sarcini.
În subsidiar, pentru realizarea obiectului principal, se vor avea în vedere:

- **furnizarea de licențe software**, în conformitate cu cerințele din prezentul caiet de sarcini;
- **prestarea de servicii IT**, constând în totalitatea serviciilor pentru implementarea sistemului, în conformitate cu cerințele din prezentul caiet de sarcini;
- **furnizarea de echipamente**, în conformitate cu cerințele din prezentul caiet de sarcini;
- **servicii instruire utilizatori.**

3.2. DESCRIEREA SITUAȚIEI ACTUALE LA NIVELUL BENEFICIARULUI

3.2.1. Cadrul legislativ

Agenția de Plăți și Intervenție pentru Agricultură (APIA) funcționează în subordinea Ministerului Agriculturii și Dezvoltării Rurale în baza **Legii nr. 1/2004** cu modificările și completările ulterioare. Conform legii, APIA este organ de specialitate al administrației publice centrale, în subordinea Ministerului Agriculturii și Dezvoltării Rurale, cu personalitate juridică, finanțat integral de la bugetul de stat.

Cadrul normativ care reglementează și încadrează activitatea APIA este, pe lângă legea 1/2004, în principal, cadrul normativ european care reglementează diferitele fonduri și scheme dedicate agriculturii: Fondul European de Garantare Agricolă - FEGA (plăți directe, măsuri de piață) și Fondul European Agricol pentru Dezvoltare Rurală - FEADR (prin intermediul măsurilor delegate din cadrul PNDR). Un cadru legislativ particular este cel care instituie și reglementează ajutoarele naționale tranzitorii și ajutoarele de stat în domeniul agricol, furnizate din bugetul național al României.

Cu privire la cadrul normativ, principalele regulamente europene cu incidență directă asupra procedurilor de plată și de furnizare a serviciilor publice de către APIA sunt:

- REGULAMENTUL (UE) NR. 1308/2013 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 17 decembrie 2013 de instituire a unei organizări comune a piețelor produselor agricole și de abrogare a Regulamentelor (CEE) nr. 922/72, (CEE) nr. 234/79, (CE) nr. 1037/2001 și (CE) nr. 1234/2007 ale Consiliului;
- REGULAMENTUL (UE) 2021/2115 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 2 decembrie 2021 de stabilire a normelor privind sprijinul pentru planurile strategice care urmează a fi elaborate de statele membre în cadrul politicii agricole comune (planurile strategice PAC) și finanțate de Fondul european de garantare agricolă (FEGA) și de Fondul european agricol pentru dezvoltare rurală

(FEADR) și de abrogare a Regulamentelor (UE) nr. 1305/2013 și (UE) nr. 1307/2013;

- REGULAMENTUL (UE) 2021/2116 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 2 decembrie 2021 privind finanțarea, gestionarea și monitorizarea politicii agricole comune și de abrogare a Regulamentului (UE) nr. 1306/2013.
- Planul strategic PAC 2023-2027 al României, aprobat prin Decizia de punere în aplicare a Comisiei Europene C (2022) 8.783 din 7 decembrie 2022, cu modificările și completările ulterioare;
- Regulamentul delegat (UE) 2022/126 al Comisiei din 7 decembrie 2021 de completare a Regulamentului (UE) 2021/2.115 al Parlamentului European și al Consiliului cu cerințe suplimentare referitoare la anumite tipuri de intervenții specificate de statele membre în planurile lor strategice PAC pentru perioada 2023-2027 în temeiul regulamentului respectiv, precum și cu norme privind raportul pentru standardul GAEC 1 (bune condiții agricole și de mediu);
- Regulamentul delegat (UE) 2022/127 al Comisiei din 7 decembrie 2021 de completare a Regulamentului (UE) 2021/2.116 al Parlamentului European și al Consiliului cu norme privind agențiile de plăți și alte organisme, gestiunea financiară, verificarea conturilor, garanțiile și utilizarea monedei euro;
- Regulamentul de punere în aplicare (UE) 2021/2.289 al Comisiei din 21 decembrie 2021 de stabilire a normelor de aplicare a Regulamentului (UE) 2021/2.115 al Parlamentului European și al Consiliului în ceea ce privește prezentarea conținutului planurilor strategice PAC și sistemul electronic pentru schimbul securizat de informații;
- Regulamentul de punere în aplicare (UE) 2021/2.290 al Comisiei din 21 decembrie 2021 de stabilire a normelor referitoare la metodele de calculare a indicatorilor de realizare și de rezultat comuni stabiliți în anexa I la Regulamentul (UE) 2021/2.115 al Parlamentului European și al Consiliului de stabilire a normelor privind sprijinul pentru planurile strategice care urmează a fi elaborate de statele membre în cadrul politicii agricole comune (planurile strategice PAC) și finanțate de Fondul european de garantare agricolă (FEGA) și de Fondul european agricol pentru dezvoltare rurală (FEADR) și de abrogare a Regulamentelor (UE) nr. 1.305/2013 și (UE) nr. 1.307/2013;
- Regulamentul delegat (UE) 2022/1.408 al Comisiei din 16 iunie 2022 de modificare a Regulamentului (UE) 2021/2.116 al Parlamentului European și al Consiliului în ceea ce privește plata avansurilor pentru anumite intervenții și măsuri de sprijin prevăzute în Regulamentele (UE) 2021/2.115 și (UE) nr. 1.308/2013 ale Parlamentului European și ale Consiliului;
- Regulamentul de punere în aplicare (UE) 2022/1.173 al Comisiei din 31 mai 2022 de stabilire a normelor de aplicare a Regulamentului (UE) 2021/2.116 al Parlamentului European și al Consiliului în ceea ce privește sistemul integrat de administrare și control din cadrul politicii agricole comune;
- Regulamentul de punere în aplicare (UE) 2024/587 al Comisiei din 12 februarie 2024 de stabilire a unei derogări de la Regulamentul (UE) 2021/2.115 al Parlamentului European și al Consiliului în ceea ce privește aplicarea standardului privind bunele condiții agricole și de mediu ale terenurilor (standardul GAEC) 8, datele de eligibilitate a cheltuielilor pentru contribuția din FEGA și normele privind modificările planurilor strategice PAC pentru modificările anumitor ecoscheme pentru anul de cerere 2024
- Regulamentul (UE) nr. 1.305/2013 al Parlamentului European și al Consiliului din 17 decembrie 2013 privind sprijinul pentru dezvoltare rurală acordat din Fondul european agricol pentru dezvoltare rurală (FEADR) și de abrogare a Regulamentului (CE) nr. 1.698/2005 al Consiliului, cu modificările și completările ulterioare;

- Regulamentul (UE) nr. 1.306/2013 privind finanțarea, gestionarea și monitorizarea politicii agricole comune și de abrogare a Regulamentelor (CEE) nr. 352/78, (CE) nr. 165/94, (CE) nr. 2.799/98, (CE) nr. 814/2000, (CE) nr. 1.290/2005 și (CE) nr. 485/2008 ale Consiliului, cu modificările și completările ulterioare;
- Regulamentul de punere în aplicare (UE) nr. 809/2014 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 1.306/2013 al Parlamentului European și al Consiliului în ceea ce privește sistemul integrat de administrare și control, măsurile de dezvoltare rurală și ecocondiționalitatea, cu modificările și completările ulterioare;
- Regulamentul (UE) 2021/2117 al Parlamentului European și al Consiliului din 2 decembrie 2021 de modificare a Regulamentului (UE) nr. 1308/2013 de instituire a unei organizări comune a piețelor produselor agricole, a Regulamentului (UE) nr. 1151/2012 privind sistemele din domeniul calității produselor agricole și alimentare, a Regulamentului (UE) nr. 251/2014 privind definirea, descrierea, prezentarea, etichetarea și protejarea indicațiilor geografice ale produselor vitivinicole aromatizate și a Regulamentului (UE) nr. 228/2013 privind măsurile specifice din domeniul agriculturii în favoarea regiunilor ultraperiferice ale Uniunii.

În vederea implementării proiectului, cadrul normativ relevant este reprezentat și de:
- Ordonanță de Urgență nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, cu modificările și completările ulterioare;
- Hotărârea Guvernului nr. 112/2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental;
- Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate;
- Legea nr. 135/2007 privind arhivarea documentelor în formă electronică, cu modificările și completările ulterioare;
- Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea;

Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2).

- Cerințele tehnice ale platformei naționale **ROeID** privind autentificarea și autorizarea utilizatorilor.

3.2.2. Structura organizatorică

Structura centrală a APIA include direcții și servicii, fiecare cu responsabilități specifice:

1. Direcția audit intern
Este organizată și funcționează conform prevederilor Legii nr. 672/2002 privind auditul public intern, republicată, cu modificările și completările ulterioare, în subordinea directă și nemijlocită a directorului general al APIA. Are ca obiectiv principal îmbunătățirea managementului APIA prin desfășurarea activităților de asigurare - care

reprezintă examinări obiective ale elementelor probante, efectuate în scopul de a furniza conducerii APIA o evaluare independentă a proceselor de management al riscurilor, de control și de guvernanță în gestionarea FEGA, FEADR și BN – și a activităților de consiliere menite să adauge valoare și să îmbunătățească procesele guvernanței în gestionarea FEGA, FEADR și BN, fără ca auditorul intern să își asume responsabilități manageriale.

2. Direcția metodologie, monitorizare, rapoarte și relații instituționale
Are ca obiectiv principal stabilirea unui model unitar la nivelul APIA pentru elaborarea, modificarea, aprobarea și difuzarea manualelor de proceduri și păstrarea evidenței diferitelor versiuni ale acestora, precum și activitatea de monitorizare și raportare către Comisia Europeană, către managementul APIA și către instituțiile externe interesate. De asemenea, coordonează, organizează, îndrumă și răspunde de activitatea privind relațiile instituționale.

3. Direcția management resurse umane
Răspunde de reconfirmarea acreditării APIA referitoare la Mediul intern în conformitate cu cerințele CE potrivit Regulamentului delegat nr. 127/2022, stabilește strategia generală privind activitățile de resurse umane și de formare profesională continuă a personalului propriu pentru întreaga Agenție.
În scopul consolidării capacității de absorbție a fondurilor FEGA și FEADR la nivelul întregii instituții și pentru asigurarea managementului și a implementării Planului strategic PAC 2023-2027, planifică și urmărește neîntrerupt consolidarea structurii de resurse umane.

4. Direcția juridică
Asigură apărarea drepturilor și intereselor legitime ale APIA; colaborează cu Direcția management resurse umane pentru reconfirmarea acreditării și pentru armonizarea legislației naționale cu cea europeană, urmărind conformitatea cu cerințele europene, pe segmentul de resurse umane.

5. Direcția antifraudă, control intern
Exercită atribuții de control și prevenție în toate domeniile de activitate ale APIA, în vederea asigurării protecției intereselor financiare ale UE și ale României.

6. Serviciul securitate internă și arhivă
Organizează, coordonează și răspunde de activitatea de protecție a informației/documentelor clasificate și are atribuții privind evidența, inventarierea, selecționarea, păstrarea și folosirea documentelor la nivelul APIA.

7. Serviciul relații cu publicul și comunicare
Organizează activitatea de comunicare și relații cu publicul, precum și crearea și menținerea unui circuit optim al documentelor.
Activitățile desfășurate de acest serviciu reprezintă servicii publice foarte importante pentru fermieri și ceilalți potențiali beneficiari de finanțări. În acest sens, dintre atribuțiile serviciului amintim promovarea măsurilor/schemelor de plată / intervențiilor/programelor/proiectelor derulate din fonduri europene și de la bugetul național, informarea și consilierea potențialilor beneficiari, cât și a beneficiarilor existenți, la sediul instituției, dar și prin e-mail sau telefon, privind activitatea APIA și măsurile/schemele de plată/intervențiile/programele/proiectele gestionate, acordarea de consultanță fermierilor în soluționarea unor probleme specifice privind accesarea fondurilor europene și de la bugetul de stat.

8. Compartimentul securitate și sănătate în muncă, PSI
Asigură evaluarea riscurilor de accidentare și îmbolnăvire profesională la locurile de muncă, precum și reevaluarea riscurilor ori de câte ori sunt modificate condițiile de muncă și propune măsuri de prevenire corespunzătoare.

9. Direcția intervenții IACS – sectorul vegetal și condiționalitate
Activitatea direcției are un impact direct asupra beneficiarilor APIA, având responsabilități precum elaborarea manualelor de proceduri privind primirea și administrarea cererilor de plată pentru schemele de plăți directe finanțate din FEGA și a ajutoarelor naționale tranzitorii, pentru implementarea intervențiilor aferente sectorului vegetal gestionate prin sistemul integrat de administrare și control (IACS) din cadrul planului strategic PAC 2023-2027; coordonarea activităților de elaborare /actualizare /implementare a procedurilor pentru măsurile delegate din PNDR 2014-2020 (măsura 10, măsura 11, măsura 15).
De asemenea, direcția elaborează/actualizează procedurile privind primirea și administrarea cererilor de plată pentru măsurile de dezvoltare rurală din sectorul vegetal, finanțate de FEADR (proceduri de lucru detaliate privind primirea, înregistrarea, verificarea cererilor aferente măsurilor de dezvoltare rurală) și participă la elaborarea procedurilor privind actualizarea și întreținerea Sistemului de Identificare a Parcelelor Agricole (LPIS) și la elaborarea procedurilor privind întreținerea Registrului Unic de Identificare (RUI).
Serviciul condiționalitate din cadrul direcției asigură elaborarea manualului de procedură privind condiționalitatea, a Ghidului fermierilor privind condiționalitatea și a Ghidului fermierului privind condiționalitatea socială.

10. Direcția plăți directe – sector zootehnic
Coordonează tehnic și metodologic departamentele tehnice din cadrul centrelor județene/locale cu privire la intervențiile aferente sectorului zootehnic din PAC 2023-2027 (sprijinul cuplat pentru venit, eco-scheme, ANT-uri), intervențiile delegate din cadrul PS 2023-2026 (DR 06 și DR 03), măsuri de dezvoltare rurală delegate (M14, M1 – P8), ajutoare de stat (motorină, ameliorare), schemă de ajutor de stat „Microgranturi în domeniul agroalimentar”, alte ajutoare excepționale, ajutoare de stat cu caracter temporar acordate sectorului zootehnic cu surse de finanțare FEGA/FEADR/BN.
Coordonează activitatea de elaborare/actualizare/implementare a ghidurilor solicitantului și a procedurilor operaționale care asigură derularea și gestionarea în bune condiții a intervențiilor aferente sectorului zootehnic și a celor delegate din cadrul PAC 2023-2027, măsurilor de dezvoltare rurală finanțate prin FEADR, a ajutoarelor de stat, a ajutoarelor excepționale, a ajutoarelor de stat cu caracter temporar acordate sectorului zootehnic.

11. Direcția control pe teren
Participă la stabilirea cadrului normativ de gestionare a intervențiilor specifice dezvoltării rurale cuprinse în Planul strategic PAC 2023 – 2027 și a intervențiilor aferente sectorului vegetal din cadrul Planului strategic PAC 2023 – 2027 finanțate din FEGA și bugetul național, elaborează și actualizează periodic procedurile care asigură derularea și gestionarea în bune condiții a controlului clasic pe teren și a controlului prin monitorizare.
Asigură îndeplinirea atribuțiilor privind măsurile delegate în ceea ce privește implementarea măsurilor și intervențiilor de dezvoltare rurală din Planul strategic PAC 2023-2027 finanțate din alocarea FEADR și implementarea la nivel județean a procedurilor de control teren.

12. Direcția IT-LPIS

Stabilește strategia IT a APIA, în funcție de necesitățile identificate pentru asigurarea infrastructurii și securității IT; participă la stabilirea politicilor, standardelor și procedurilor conform cărora se desfășoară activitățile IT din APIA.
Participă la stabilirea politicilor, standardelor și procedurilor conform cărora se desfășoară activitățile IT din Agenție, de stabilire a standardelor și procedurile pentru dezvoltarea și programarea sistemelor IT, documentația sistemelor, operarea sistemelor, securitatea informațiilor și gestionarea datelor;
Asigură în conformitate cu politica de securitate a sistemelor IT, clasificarea informației conform nivelului cerut de securitate, pentru confidențialitate, integritate și disponibilitate.
Realizează actualizarea și întreținerea LPIS și definește criteriile de risc care trebuie utilizate pentru analiza de risc, evaluează și actualizează anual eficacitatea analizei de risc, respectiv stabilește eșantioanele de control și supracontrol pentru intervențiile aferente sectoarelor vegetal și zootehnic, dezvoltare rurală și condiționalitate din cadrul Planului strategic PAC 2023-2027, administrate prin sistemul informatic IACS.

13. Direcția control administrativ și autorizare plăți
Elaborează procedura operațională privind controlul administrativ – sector vegetal și autorizarea plăților pentru intervențiile/ măsurile solicitate în cererea de plată, din PAC 2023-2027; actualizează și monitorizează sistemul IACS, modulele captură date, control administrativ , calcul și autorizare plăți, elaborează și transmite în teritoriu instrucțiuni privind funcționalitățile dezvoltate în sistemul IACS privind sectorul vegetal și urmărește modul de aplicare a acestora; efectuează calculul, transferul, calculul manual, supracontrolul și monitorizarea aprobării listelor de plată pentru măsurile delegate din PNDR 2014-2020 și PAC 2023-2027.

14. Serviciul inspecții / supracontrol
Coordonează tehnic, metodologic și monitorizează activitatea desfășurată de inspectorii din cadrul B/CI/S-CJ, conform planului anual de inspecții aprobat, pe domenii de activitate specifice, pentru fiecare măsură, schemă de sprijin financiar verificată; efectuează acțiuni de inspecție/supracontrol pentru scheme de plată/măsuri de sprijin și ajutor financiar derulate prin DMPCE și DPD-SZ, în vederea verificării respectării legislației europene și naționale aplicabile.

15. Direcția măsuri de piață, comerț exterior
Prin intermediul serviciilor și compartimentelor organizate în cadrul direcției, se asigură realizarea verificărilor administrative/validărilor cererilor de plată și ale documentelor justificative pentru fiecare măsură de piață și pentru intervențiile stabilite prin PAC 2023-2027, precum și autorizarea cererilor de plată și transmiterea solicitărilor de alimentare a conturilor cu sumele autorizate către Direcția economică.
De asemenea, se asigură elaborarea și actualizarea procedurilor și metodologiilor pentru toate segmentele de activitate, respectiv măsurile de piață și intervențiile stabilite prin PAC 2023-2027, implementarea, compatibilitatea și suficiența controlului.

16. Direcția economică
Îndeplinește două dintre cele trei funcții ale APIA, respectiv plata și contabilizarea fondurilor nerambursabile destinate finanțării PAC 2023-2027 – FEGA, măsuri delegate din FEADR, precum și a fondurilor de cofinanțare și prefinanțare alocate de la bugetul de stat sau din alte surse.
Totodată este responsabilă cu înregistrare, recuperare a creanțelor bugetare aprobate de directorul general și de coordonarea activitatea de înregistrare, recuperare a creanțelor bugetare aprobate de directorii executivi a Centrelor Județene, aferente

fondurilor europene şi fonduri publice naţionale, din Registrul Debitorilor Europene respectiv Registrul Debitorilor Națională.
Pentru a indeplini funcția de plata, o alta atribuție importanta a Direcţiei Economice este asigurarea finanțării Agenției, atât pentru efectuarea plăților către beneficiarii formelor de sprijin financiar pentru agricultură, cât și pentru asigurarea cheltuielilor administrative aferente APIA central și CJ APIA: cheltuieli de personal, bunuri și servicii, active nefinanciare.
În vederea elaborării Situației financiare consolidate, se realizează verificarea situațiilor financiare aferente perioadei de raportare (trimestriale și anuale) întocmite de ordonatorii terțiari de credite. Aceste documente oficiale reflectă în mod fidel și real poziția și performanța financiară a Agenției, oferind totodată informații relevante privind activitatea desfășurată și cheltuielile efectuate.

17. Direcția patrimoniu, achiziții publice și administrativ
Desfășoară activitățile de achiziții publice, de gestionare a patrimoniului și pe cele cu caracter administrativ.
APIA are în subordine 42 de centre județene, cu personalitate juridică, conduse de directori executivi, numiți prin decizie a directorului general. Directorii executivi au calitatea de ordonatori terțiari de credite pentru fondurile de la bugetul de stat, cu excepția cheltuielilor prefinanțate și cofinanțate prin schemele de plată FEGA și schemele de plată FEADR.

Structura organizațională la nivel judetean
APIA are o structură de 42 centre județene inclusiv centrele locale arondate pe aria de competență a fiecăruia conform regulamentului intern de funcționare, după cum urmează:

a. Serviciul autorizare plati

Asigură activitățile specifice pentru informarea fermierilor, inregistrarea in registrul fermierilor, primirea cererilor de plată, gestionarea acestora, autorizarea la plată a fermeirilor din sectorul vegetal si zootehnic pentru fermele de dețin cel puțin 50 ha teren.

b. Compartiment IT – LPIS

Asigură activitățile specifice pentru buna functionare a infrastructurii IT la nivel judetean si local, respectarea politicii de securitate IT.

c. Serviciul masuri specifice

Asigură activitățile specifice pentru intervențiile, ajutoarele și măsurile specifice acordate în sectorul zootehnic, cele legate de renta viageră și măsurile de piață ți intervențiilor în sectorul apicol, sectorul vitivinicol, si legume fructe.

d. Serviciul control pe teren

Asigură activitățile specifice pentru controlul pe teren al fermeirilor și înregistrarea rezultatelor în sistemele informatice.

e. Serviciul economic, recuperare debite si resurse umane

Asigură activitățile specifice pentru fluxurile specifice operațiunilor economice necesare pentru buna desfășurare a activității centrului județean respectiv asigurarea fluxurilor specifice pentru achiziții și gestionare parc auto la nivel județean. De asemenea asigură fluxurile specifice pentru înregistrarea si gestionarea debitelor stabilite la nivelul centrului județean și activitățile specifice pe fluxul de resurse umane la nivel județean.

f. Comp. inspectii/supracontrol

Obiectivul activității de inspecții/supracontrol este de a asigura funcționarea eficientă a sistemului de inspecție si control a centrului județean, în conformitate cu prevederile europene privind asigurarea asistenței financiare prin FEGA și FEADR.

g. Comp. juridic si relatii cu publicul

Asigură suport juridic și consultanță juridică, avize de legalitate și alte activități ce țin de asistența juridică la nivelul centrului județean și local. Pentru relații cu publicul atribuțiile sunt legate de asigurarea circuitului documentelor și furnizarea de informații de interes public.

h. Centre locale

Asigură activitățile specifice pentru informarea fermierilor, inregistrarea in registrul fermierilor, primirea cererilor de plată, gestionarea acestora, autorizarea la plată a fermeirilor din sectorul vegetal si zootehnic pentru fermele cu mai puțin de 50 ha teren

Structura organizatorică și regulamentele de funcționare și organizare pot fi consultate pe site-ul APIA, pentru o mai bună descriere a organizării.

3.2.3. Sistemul informatic existent

SI-APIA implementează fluxuri, proceduri și procese interne de lucru, în vederea gestionării, monitorizării, raportării și efectuării plăților către solicitanții de fonduri europene și fonduri naționale.

SI-APIA este organizat în jurul unei baze de date cuprinzând informații asupra beneficiarilor de subvenții și este realizat astfel încât să permită APIA să proceseze plățile pe suprafața și pentru zootehnie făcute către fermieri. De asemenea, sistemul implementat asigură derularea măsurilor de reglementare a pieței, prin subsistemul Scheme privind Reglementarea Pieței și a plăților aferente măsurilor de dezvoltare rurală delegate din PNDR, prin subsistemul de Dezvoltare Rurală.

Baza de date SI-APIA se bazează pe unicitatea fermierului/solicitantului și este esențială pentru ca SI-APIA să opereze eficient. Aceasta baza de date a fost instalata și este pe deplin operațională**. La momentul actual, aproximativ 2.000.000 de fermieri sunt înregistrați în baza de date a registrului unic de identificare a fermierilor, dintre care aproximativ 800.000 au și solicitări de sprijin pentru măsurile și intervențiile gestionate de APIA.**

Tehnologiile folosite pentru realizarea sistemului informatic sunt:

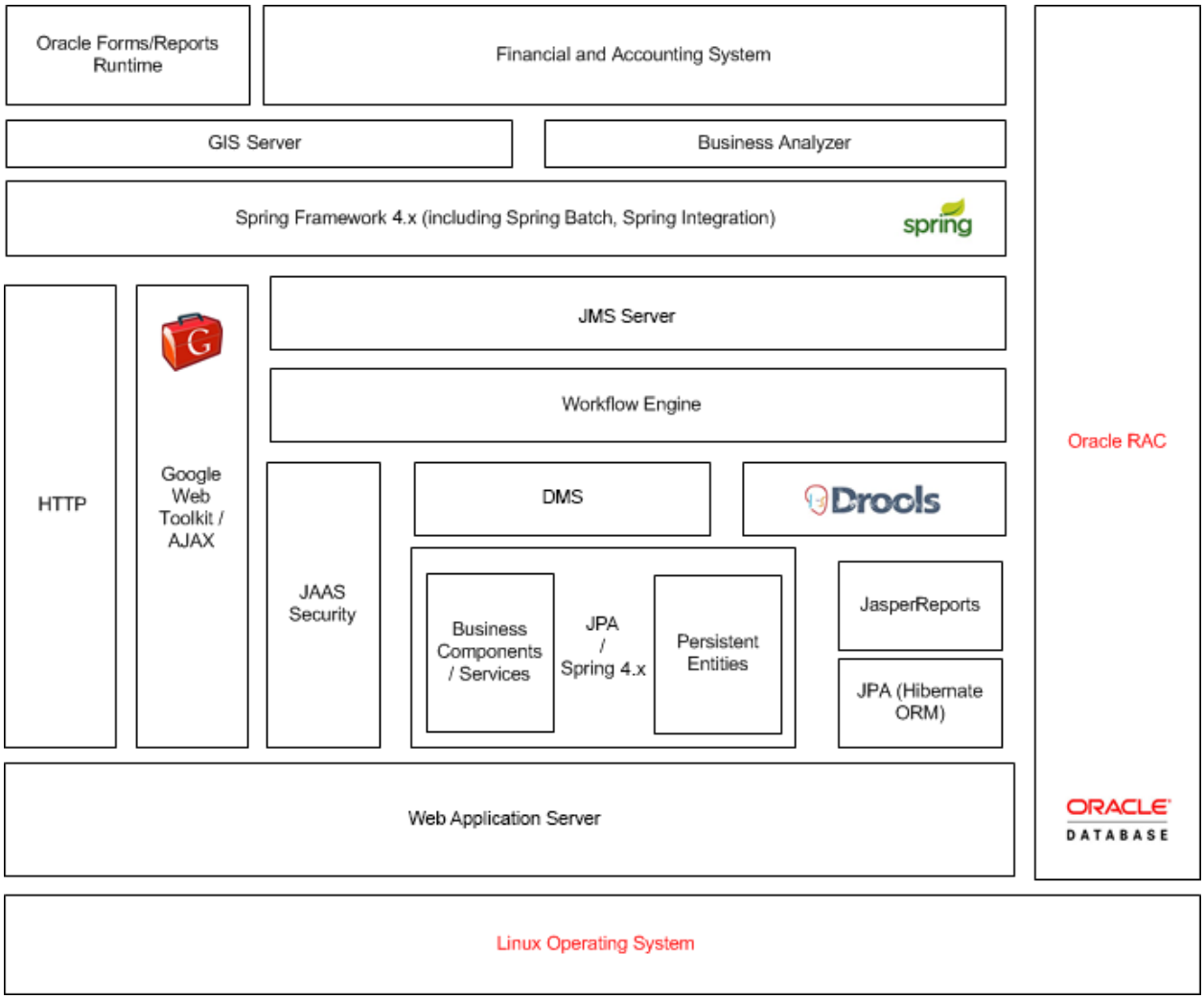
- Sisteme de operare:
  - Linux pentru serverele de aplicații;
  - ORACLE Linux pentru serverele de baze de date;
- Baze de date: Oracle; Postgres;
- Tehnologie GIS: Geoserver.

Sistemul Integrat de Administrare și Control (IACS) este un sistem campanizat, care are funcționalități specifice pentru fiecare campanie de depunere cereri, specifice anului pentru care se solicită sprijin, în funcție de legislația specifică campaniei de depunere cereri de plată.

Aplicația actuală este dezvoltată folosind biblioteci open-source atat în zona de server-side cat și în zona de client-side.

Se folosesc următoarele biblioteci pentru a acoperi tot fluxul de date:

- În zona de client side se folosește framework-ul Google Web Toolkit (GWT 2.5.1) pentru a avea o decuplare între logica de prezentare și logica de date;
- În partea de server side se folosește stack-ul de la Spring pentru a facilita lucrul cu componentele din aceasta zonă:
    - Spring IOC – container de componente reutilizabile;
    - Spring AOP – necesar pentru a acoperi necesarul de cross cutting (tranzacționalitate, logging, monitorizare acțiuni utilizatori);
    - Spring Batch – necesar pentru procesarea loturilor mari de activități în masă;
    - Spring Plugin – necesar în cadrul proceselor de lucru pentru decuplarea și modularizarea funcționalităților;
    - Hiberate JPA – pentru persistarea datelor în serverul de baze de date;
    - Jasper Reports – pentru design și generare rapoarte.



Totodată, este asigurată interfațarea între multiple subsisteme / sisteme, atât interne, cât externe, prin următoarele modalități:

Sistem/Subsistem consumator	Sistem/Subsistem furnizor	Modalitate interfatare
IACS	ANSVSA	REST
AFIR	IACS	WSDL
IACS	LPIS	acces direct baza de date
LPIS	IACS	acces direct baza de date
Interfață Financiar Contabilitate	Market Regulation	acces direct baza de date
IACS	IPA(Aplicația Geospațială)	acces direct baza de date
IPA(Aplicația Geospațială)	IACS	acces direct baza de date
Sistem IQ Management	Interfață Financiar Contabilitate	fișiere
IACS (Campanii anterioare)	IACS (Campania curenta)	WSDL
IACS (Campanii viitoare)	IACS (Campania curenta)	WSDL
Interfață Financiar Contabilitate	SIVECO Applications	acces direct baza de date
SIVECO Applications	Interfață Financiar Contabilitate	acces direct baza de date

Infrastructura sistemului informatic al APIA

Structura sistemului

Sistemul este proiectat într-o arhitectură web based. Fiecare instanță a clientului poate trimite solicitări către serviciile back-end APIA, prin infrastructura rețelei client-server. Elementele server procesează solicitările și returnează rezultatele către front-end. Clienții pot cere prin Interfață Grafică Utilizator culegerea parametrilor solicitărilor și afișarea rezultatelor. Mediile de execuție back-end sunt conectate prin intermediul infrastructurii rețelei interne.

Sistemul informatic a fost proiectat astfel încât să rezulte o descompunere în subsisteme cu roluri și caracteristici bine definite fără a avea o suprapunere de funcționalități între două subsisteme. Arhitectura sistemului informatic este una de tip n-tier, după cum urmează:

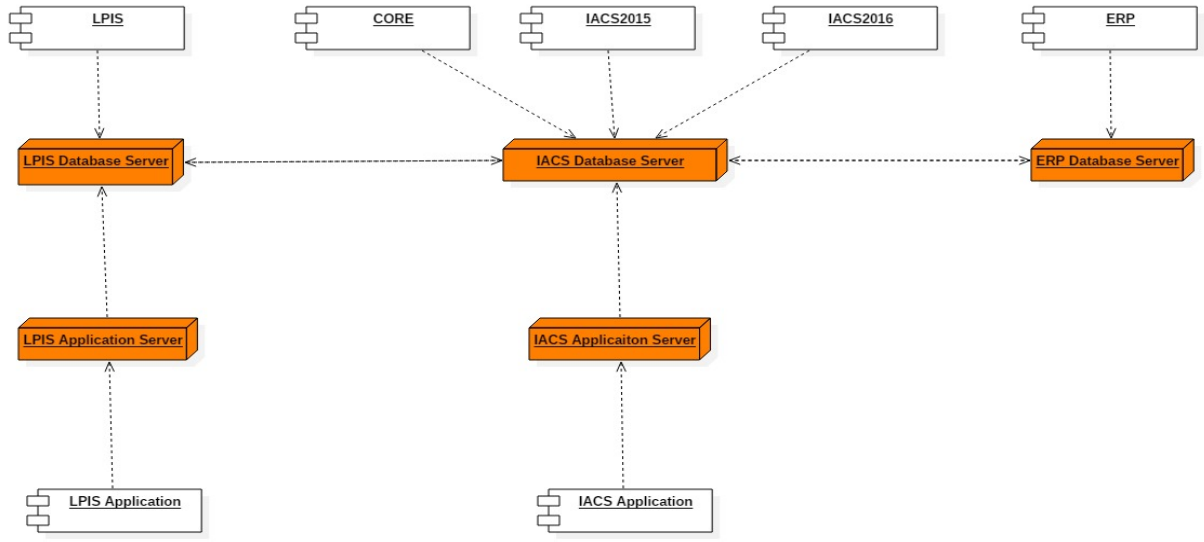
- *Componenta prezentare* – cel mai de sus nivel al aplicației și reprezintă interfață cu utilizatorul. Funcția principala a acestei componente este de a interpreta instrucțiunile primite de la utilizator și de a furniza rezultatele;
- *Componenta aplicație* – este nivelul care coordonează aplicația, interpretează comenzi primite de la utilizator, ia decizii pe baza unor evaluări logice și realizează calculele cerute de fluxul de business;
- *Componenta persistenta* – reprezintă nivelul responsabil cu persistarea datelor în vederea accesării ulterioare.

Arhitectura software este bazată pe paternul arhitectural MVC care structurează aplicația în trei niveluri ce realizează separarea modului în care informația este reprezentată intern de modul în care aceasta este prezentată sau utilizată de utilizatorul aplicației:

- *Controller* – parte din MVC și primul layer al aplicatiei responsabil să intercepteze part-requesturile/requesturile de tip AJAX venite de la componenta de client-side;

- *Service* – parte a bussines layer-ului aplicației, este responsabil cu implementarea logicii de business a aplicației. Acest layer este layer-ul tranzacțional astfel încât toate operațiile de scriere la baza de date să se execute în cadrul undei singure tranzacții, iar operațiile de citire (marcate cu @Transactional(readOnly=true) vor folosi o singură conexiune la bază de date fără a face savePoint-uri intermediare, optimizând astfel atât pool-ul de conexiuni la baza de date, cât și memoria internă a serverului de aplicație;
- *Model* (Repository) – layer responsabil cu citirea și stocarea informațiilor din/în baza de date.

Arhitectura back-end



Pentru a segmenta baza de date, datele sunt divizate în mai multe scheme, printre care o schemă comună tuturor campaniilor și scheme diferite pentru fiecare an de campanizare, începând cu anul 2007.

LPIS back-end este instalat într-un mediu de execuție separat față de celelalte subsisteme IACS și are următoarele caracteristici:

- Baza de date LPIS este instalată pe serverul comun al bazei de date și este interfațată cu Registrul Fermierilor și IACS;
- Serverul de aplicație LPIS este instalat pe serverul sau de aplicație și deține rețea expusă pentru clienți;
- LPIS Gateway are rolul de interfațare a comunicării între sistemul IACS și LPIS.

Sistemul LPIS este integrat cu celelalte subsisteme, pe baza unei interfețe informatice, realizate la nivelul bazei de date. O interfață specială este cea realizată cu sistemul IPA Online/Aplicația Geospațială care gestionează completarea declarațiilor de suprafață de către fermieri în procesul de depunere cereri de sprijin.

Tehnologiile utilizate sunt: PostGIS / PostgreSQL, Geoserver, Apache Tomcat, OpenLayers3, Geotools.

Structura Back-end pentru subsistemul de gestiune Financiar Contabil (ERP)

Subsistemul de gestiune Financiar-Contabil are trei niveluri principale, descrise în continuare:

- Baza de date pentru subsistemul de gestiune Financiar-Contabil este instalată pe serverul bazei de date comune;
- Aplicația server-ului subsistemului de gestiune Financiar-Contabil este aplicația server secundara instalata pe platforma sa de execuție;
- Aplicația client a subsistemului de gestiune Financiar-Contabil este aplicația client secundară instalată pe fiecare computer client și care interacționează direct cu baza de date.

Arhitectura Front-end
Părțile front-end sunt proiectate să utilizeze o platformă web browser.

Integrarea subsistemelor
Modulele din cadrul subsistemului IACS comunica intre ele prin intermediul Separated Interface pattern. Subsistemele folosesc modelul Interfetei Locale în stratul de transport. Interfata Locala inseamnă ca obiectele nu sunt distribuite intre părțile sistemului. Aceasta abordare introduce un nivel minim în apelarea serviciilor din sisteme externe.

Niveluri ale arhitecturii

a. Concepte Generale

Fiecare modul al subsistemului IACS este structurat pe trei niveluri: nivelul client de prezentare, nivelul logicii de proces (nivel de mijloc) și nivelul de date (acces și management).
Nivelul client este responsabil pentru afișarea interfeței utilizator și pentru gestionarea interacțiunii cu utilizatorii și include browser-e web Internet standard.
Funcționalitatea (logică) de bază a modulelor sistemului este realizată la nivelul de mijloc, cu ajutorul serverului de aplicație. Serverul de aplicație este o platformă de programare pentru dezvoltarea și rularea aplicațiilor cu arhitectura pe mai multe niveluri. Nivelul de mijloc este el însuși un nivel multi-stratificat (întreaga arhitectură este de tip “n-tier”).
Nivelul de date (de persistență) este responsabil pentru stocarea și recuperarea datelor aplicației și include serverul bazei de date.

b. Nivelul client

Nivelul client realizează interfața cu utilizatorii și permite accesul utilizatorului la funcțiile specializate de business. Nivelul client include *browser-ul web* standard, care afișează pagina web primită de la nivelul de mijloc. Validări simple ale datelor sunt realizate și la acest nivel, deși validarea principală este realizată la nivelul de mijloc.

c. Nivelul de mijloc

Nivelul de mijloc realizează logica business-ului. Acest nivel este găzduit de serverul de aplicație. Serverul de aplicație furnizează servicii comune, cum ar fi autorizarea și autentificarea, conectarea la baza de date etc. Logica problemei reprezintă un aspect complex și, din acest motiv, nivelul de mijloc este divizat în mai multe straturi:

- Stratul de prezentare;
- Stratul logic al aplicației;
- Stratul sursei de date.

d. Nivelul de prezentare

Nivelul de prezentare este implementat utilizând un model de arhitectură care reprezintă o variație a model-view-controller pattern. Principala caracteristică a acestui model arhitectural este că un controlor gestionează comunicarea client și apelarea logică a business-ului. Prezentarea se găsește în principal în stratul de prezentare.

Conținutul aplicației este strict dinamic – paginile sunt prezentate numai în aceste părți ale sistemului, care este accesibil utilizatorului conectat. Datele sunt stocate și prezentate în limba română. Toate caracterele sunt codificate în format UTF-8.

e. Stratul nivelului logic

Nivelul logic este divizat în două părți:

- Logica business-ului;
- Logica aplicației.

Logica business-ului este realizată prin aplicarea domain model pattern. Domain model pattern presupune crearea modelului obiectului domeniului. Acest model încorporează atât comportamentul, cât și datele. O asemenea abordare permite implementarea și reutilizarea regulilor complexe de business. Există un minim de cuplare din domain model la alte straturi.
Stratul de prezentare comunică numai cu stratul de serviciu și nu este cuplat cu domain model, exceptând accesul read-only. Alte subsisteme ale sistemului invocă operațiunile de business apelând stratul de serviciu.

f. Stratul sursei de date

Stratul sursei de date este responsabil pentru regăsirea datelor și furnizează date pentru stratul logic al domeniului. Datele din baza de date sunt mapate în clasele din domeniul logic și aceste clase sunt utilizate ca date intermediare. Toate datele scrise sunt executate în cadrul tranzacției de la nivelul bazei de date.

g. Nivelul de persistență

Nivelul de persistență este responsabil pentru stocarea datelor procesate în sistem. Datele sunt stocate în baza de date. Modulul accesează datele bazei de date prin stratul sursei de date localizat în nivelul de mijloc. Baza de date furnizează managementul centralizat al bazei de date, accesul la date și modificarea datelor. Integritatea datelor este garantată datorită constrângerilor definite în baza de date a aplicației.

h. Comunicarea între niveluri

Nivelurile comunică prin apelări la straturi “inferioare”, ceea ce înseamnă că nivelul client apelează stratul de mijloc și acesta apelează stratul de persistență. Apelarea înapoi la un strat superior nu este permisă. Datele straturilor sunt regăsite de la stratul inferior la stratul superior utilizând schema cerere-răspuns.

i. Comunicare internă în cadrul nivelului de mijloc

Stratul de prezentare comunică numai cu stratul de serviciu. Acesta nu este cuplat cu domain model. Schimbările la domain model sunt efectuate utilizând stratul de serviciu. Alte Subsisteme ale sistemului pot invoca operațiunile de business prin apelarea stratului de serviciu.
Straturile comunică (schimbă date) prin utilizarea în principal a modelului DTO.

j. Interogarea directă a bazei de date

Câteodată, procesele de business implică procesarea unui volum mare de date (de exemplu generarea rapoartelor). În această situație stratul de serviciu poate accesa direct baza de date.
Este posibil să se apeleze direct procedurile stocate în baza de date sau să se regăsească un volum mare de date direct din baza de date. Apelările directe sunt realizate din stratul de serviciu, ceea ce înseamnă că stratul de prezentare trebuie să apeleze mai întâi serviciul. Este foarte important ca fiecare modificare a datelor prin apelare directă să fie în concordanță cu comportamentul stratului sursei de date, iar apelarea directă a modificărilor datelor trebuie să fie realizată în modul „optimistic offline lock pattern”.

Facilități cheie ale infrastructurii
Scopul acestei secțiuni este acela de a furniza descrierea facilităților cheie ale infrastructurii. Facilitățile au fost divizate în mai multe categorii de interes, după cum sunt prezentate în continuare.

a. Securitatea aplicației
Autentificarea și autorizarea utilizatorului sunt realizate de către serverul de aplicație. Accesul la funcțiile sistemului este permis numai utilizatorilor care au drepturile necesare. Drepturile sunt alocate rolurilor și nu direct utilizatorilor. Modelul rolurilor este proiectat să fie ierarhic. Rolurile pot moșteni drepturi. Fiecărui utilizator i se pot asocia oricâte roluri.
Utilizatorii sunt autentificați o singura dată într-o sesiune. Autentificarea bazată pe parolă este realizată de către componentele nucleu ale sistemului și următoarea sesiune este creată. Apelările următoare ale aceluiași client sunt conectate cu acea sesiune. Serverul de aplicație asociază automat drepturi corespunzătoare acelor apeluri. Sesiunile expiră prin operațiunea de deconectare explicită sau prin timeout configurabil. Nucleul sistemului furnizează funcționalitatea de a defini complexitatea minimă a parolelor utilizatorilor și de a impune schimbarea parolelor la intervale definite de timp.

b. Tranzacții
Tranzacțiile business sunt administrate prin sistemul „offline optimistic lock pattern" pus la dispoziție prin intermediul bibliotecilor Hibernate/JPA. Serverul bazei de date folosește nivelul de separare *Read Commited*.

Tehnologii folosite în cadrul sistemului IACS

a. Java Enterprise 6
Java Enterprise Edition 6 este o platformă de programare software pentru crearea și rularea aplicațiilor business distribuite pe mai multe niveluri de arhitectuă. Java EE include specificațiile mai multor interfețe de serviciu care simplifică semnificativ dezvoltarea sistemului. Aceasta permite dezvoltatorului să creeze aplicații care sunt portabile între implementările platformei și scalabilă, în timpul integrării cu tehnologiile moștenite.

b. **Serverele bazelor de date**
Oracle și PostgreSQL RDBMS sprijină accesul SQL la datele alfanumerice și binare. Extensia PostGIS a PostgreSQL oferă suport pentru lucru cu date spațiale. Aceasta suportă o serie largă de operatori spațiali, instrumente de administrare, funcții, partiționarea spațială și indexarea.
Baza de date ORACLE este instalată pe un echipament Oracle Exadata Half Rack.

c. **Spring Framework**
Spring este framework-ul care oferă suport la nivel de infrastructură de aplicație care pune la dispoziție un model complex și complet de dezvoltare și configurare a aplicațiilor moderne realizate în tehnologie Java.

d. **Hibernate**
Hibernate este o bibliotecă ORM (Object-Relational Mapping) pentru limbajul Java, utilă pentru maparea modelului orientat pe obiecte peste bazele de date relaționale. Principalul atu al acestei biblioteci este faptul că oferă o soluție rapidă, de înaltă

performanță, independentă de tipul bazei de date folosite pentru modelarea obiectelor unei baze relaționale.
Principala caracteristică a Hibernate este maparea între clasele Java și tabelele bazelor de date precum și între tipurile de date Java și SQL. Hibernate pune la dispoziție posibilitatea redactării de query-uri și data-retrieval.

e. **Jasper Reports**

JasperReports este o componentă open-source de generare a rapoartelor, care poate scrie într-o varietate de dispozitive de ieșire: ecran, imprimantă, sau poate exporta datele de ieșire în fișiere în format PDF, HTML, Microsoft Excel, RTF, ODT, CSV sau XML. Poate fi folosit în aplicații Java, inclusiv Java EE sau aplicații web , pentru a genera conținut dinamic.
Rapoartele JasperReports sunt definite într-un format de fișier XML, denumit JRXML, care pot fi codate manual, generate, sau proiectate, folosind instrumente specifice. Principala diferență între utilizarea XML și un fisier a .jasper este faptul că fișierul XML ar trebui să fie compilat în timpul rulării.

f. **Google Web Toolkit**

Google Web Toolkit (GWT) este un set de instrumente de dezvoltare pentru construirea și optimizarea aplicațiilor web complexe.
SDK-ul GWT oferă un set de bază de API-uri și widget-uri Java. Acestea permit scrierea aplicațiilor AJAX în limbaj Java și apoi din compilarea surselor rezultând cod client-side JavaScript optimizat, compatibil cu toate browserele web.

g. **Drools**

Drools este un sistem de management de gestiune al regulilor de business (BRMS) cu un motor de inferențe bazat pe înlănțuire, cunoscut și ca motor de reguli de producție, folosind o implementare îmbunătățită a algoritmului Rete. Drools suportă standardele JSR-94

Sistemul IACS permite interfațări diverse în funcție de cerințele beneficiarului. De asemenea, poate fi adaptat în cadrul contractelor existente pentru a prelua servicii web, documente electronice, etc din alte sisteme care ar putea furniza aceste informații, punctual pentru aria de interes.

La momentul actual, documentele se depun fizic la sediile APIA centrale/locale/județene, după caz, iar informațiile din aceste documente se introduc manual pe fluxurile create în cadrul aplicației IACS, necesitând un volum mare de muncă și cu risc de introducere eronată a datelor.

Sistemul IACS poate furniza informații din baza de date care să fie preluate de alte aplicații pentru a crea documente precompletate în funcție de necesitățile identificate pe fluxurile de lucru. Conectarea se face prin servicii web, prin care pe baza identificatorului unic stabilit se furnizează informațiile necesare după caz.
Aplicația GEOSPATIALA (GIS) este o altă aplicație de sine stătătoare, care gestionează și partea vectorială cu parcelele fermierilor. *În noua aplicație se va integra doar link de accesare pentru a facilita accesul fermierilor la toate aplicațiile existente*.
Aplicațiile existente care furnizează servicii ce sunt accesate de beneficiarii APIA se vor adapta pentru a utiliza zona de conectare ca punct unic ce va fi furnizat de aplicația nou-dezvoltată pentru interfața cu cetățenii.

Aplicația GEOSPATIALA (GIS) oferă, ca și IACS, informații din baza de date care pot fi preluate de alte aplicații pentru a crea documente precompletate în funcție de necesitățile identificate pe fluxurile de lucru. Conectarea se face prin servicii web, prin care pe baza identificatorului unic stabilit se furnizează informațiile necesare după caz. De asemenea, se va interfața cu aplicația nouă pentru preluarea automată a unor formulare specifice depuse de cetățeni, după caz.Cele de mai sus reprezinta o descriere a sistemului existent ce nu face obiectul acestui caiet de sarcini. Prin acest caiet de sarcini se vor furniza doar servicii de interfațare si conectare cu sistemul informatic existent, pe lângă celelalte cerințe specifice solicitate prin caietul de sarcini.

3.2.4. Prezentarea serviciilor publice oferite

APIA este responsabilă cu gestionarea unor forme de sprijin destinate susținerii agriculturii românești, finanțate din Fondul European de Garantare Agricolă (FEGA), Fondul European Agricol pentru Dezvoltare Rurală (FEADR) și din bugetul național (BN). Legat de acestea, APIA este responsabilă cu oferirea următoarelor servicii publice către cetățeni și companii, care se regăsesc în Catalogul Național al Serviciilor Publice gestionat de ADR:

- Primirea și gestionarea cererilor de sprijin gestionate de APIA din fondurile FEGA și FEADR și buget național pentru suprafață și animale sau alte scheme și fonduri aflate în sarcina APIA conform cerințelor specifice de la momentul implementării proiectului
- Administrarea și plata rentei viagere;
- Administrarea și plata unor scheme de sprijin pentru fermieri: motorină, sprijin pentru ameliorarea raselor, scheme pe zootehnie, bunăstarea animalelor, sprijin în sectorul viti-vinicol, în sectorul fructe-legume, în sectorul apicol;
- Primirea raportărilor obligatorii prin regulamente europene pentru sectoare ca cel de lapte;
- Emitere licențe de export-import.

3.3. OBIECTIVELE GENERALE ȘI SPECIFICE LA CARE CONTRIBUIE FURNIZAREA PRODUSELOR ȘI PRESTAREA SERVICIILOR

Obiectivul general al proiectului constă în **digitalizarea și îmbunătățirea semnificativă**, după caz, **a serviciilor publice furnizate de instituție către beneficiarii direcți ai diferitelor scheme de plată operate de și aflate în responsabilitatea APIA**.

Astfel, serviciile publice înscrise în Catalogul Național al Serviciilor Publice, care se adresează cetățenilor și mediului de afaceri vor fi digitalizate extensiv, îmbunătățind semnificativ calitatea și eficiența acestora și, în același timp optimizând procesele de lucru interne care susțin furnizarea serviciilor, precum și procesul de partajare de informații relevante cu alte entități publice.

Proiectul propus vizează următorul grup țintă:

- cetățenii persoane fizice și persoanele juridice de drept privat beneficiari direcți ai diferitelor scheme de plată operate și aflate în responsabilitatea APIA;
- autoritățile și instituțiile publice implicate care trebuie să furnizeze date sau input pentru furnizarea serviciilor publice aflate în responsabilitatea APIA;
- autoritățile și instituțiile publice care beneficiază de date și informații furnizate de APIA pentru serviciile publice aflate în responsabilitatea lor;

- angajații APIA care vor utiliza sistemul informatic în vederea furnizării serviciilor publice.

Obiectivele specifice ale proiectului sunt:

- OS 1: **Digitalizarea integrală a serviciilor** de plăți către cetățeni și mediul de afaceri prin implementarea la nivelul APIA a unui sistem informatic integrat:
  - Furnizarea de servicii publice integral online către cetățeni și companii, prin intermediul unui portal on-line de tip **spațiu privat virtual**;
  - Colectarea, prelucrarea și agregarea rapidă și eficientă a informațiilor primite/transmise prin **sistemul informatic integrat**;
  - Structurarea și informatizarea **procedurilor de comunicare**, atât intra-instituționale, cât și interinstituționale;
- OS 2: **Eficientizarea proceselor interne** ale APIA:
  - Automatizarea și monitorizarea proceselor de lucru și acces operativ la toate informațiile necesare desfășurării activității;
- OS 3: **Creșterea nivelului de pregătire**, cunoștințe și abilități ale personalului din cadrul APIA pentru administrarea și pentru utilizarea sistemului informatic dezvoltat prin proiect.

4. CERINȚE GENERALE PRIVIND SOLUȚIA TEHNICĂ

4.1. CERINȚE GENERALE

Niveluri necesare pentru implementarea proiectului:

- La **nivel legal**: se vor avea în vedere secțiunile „Cadrul legislativ" și „Structura organizatorică" a APIA, atât la nivel central cât și la nivel județean.

Schimburile de date trebuie să respecte: cadrul juridic de care depind părțile interesate (dreptul național și internațional, proprietatea intelectuală, confidențialitatea etc.) sau acordurile contractuale între părțile interesate (modalități de schimb, niveluri de servicii etc.). În ceea ce privește autoritățile și instituțiile publice, nivelul juridic vizează asigurarea faptului că diversele cadre juridice în temeiul cărora funcționează diferite organizații nu împiedică furnizarea de servicii publice neîntrerupte.

Primul pas spre abordarea interoperabilității juridice este de a efectua „verificări ale interoperabilității" prin examinarea legislației existente în vederea identificării barierelor în calea interoperabilității: restricții sectoriale sau geografice privind utilizarea și stocarea datelor, modele de licențe de date diferite și vagi, obligații prea stricte de a utiliza tehnologii digitale sau moduri de livrare specifice pentru furnizarea serviciilor publice, cerințe contradictorii pentru procese operaționale identice sau similare sau nevoi de securitate și protecție a datelor depășite, etc.

Cetățenii români, ca și cetățenii europeni, au așteptări în ceea ce privește accesarea unor servicii publice ușor mai ales prin intermediul canalelor digitale. În acest context, tehnologiile TIC și interoperabilitatea sistemelor ce urmează a fi dezvoltate cu cele deja existente trebuie luate în considerare cât mai devreme posibil în procesul de elaborare a legilor.

- La **nivel organizațional**: alinierea proceselor operaționale presupune documentarea acestora într-un mod stabilit de comun acord și cu ajutorul unor tehnici de modelare general acceptate, inclusiv a informațiilor schimbate, astfel încât toate administrațiile publice participante la furnizarea serviciilor publice naționale și europene să poată înțelege ansamblul procesului operațional („end-to-end"), precum și rolul care le revine în cadrul acestuia. Documentarea proceselor operaționale în cadrul proiectului se va realiza folosind tehnici de modelare general acceptate și presupune realizarea unor acorduri cu furnizorii de servicii din administrația publică asupra modului în care procesele vor trebui să fie aliniate pentru furnizarea unui serviciu public electronic către cetățeni și mediul de afaceri.

- La **nivel semantic**: se va utiliza, pentru setul minim de date, vocabularul ISA, de exemplu Core Natural Person și Core Legal Persons și orice alt vocabular identificat în faza de analiză, necesar pentru schimbul de date transfrontalier.

- La **nivel tehnic**:
    - Platforma tehnică trebuie să suporte standarde deschise, fiind necesar a fi compatibilă cu serverele care respectă specificațiile non-proprietare și cu standardele existente;

- Sistemul informatic trebuie proiectat, instalat, testat și pus în funcțiune ca un sistem complet integrat, scalabil, deschis, extensibil, flexibil, cu atribute înalte de securitate și disponibilitate, interoperabil cu alte sisteme informaționale, prin interfețe care vor fi descrise mai jos;
- Utilizarea unei arhitecturi modulare care să permită o cuplare redusă între componente și în care responsabilitățile fiecărei componente sunt specializate;
- Structura modulară permite adăugarea de noi module fără modificări în modulele software finalizate;
- Pentru schimbul de date cu alte sisteme se solicită utilizarea de standarde deschise (de exemplu bazate pe XML/JSON);
- Sistemul va expune o interfață bazată pe servicii WEB, prin care aplicațiile instituțiilor pot transmite informație folosind un canal de comunicare sistem la sistem;
- Sistemul propus va permite exportul informațiilor stocate în diverse formate (de exemplu bazate pe XML/JSON);
- Furnizorul va avea în vedere că toate cerințele și caracteristicile sunt minime și obligatorii;
- Furnizorii au obligativitatea de a include în propunerea tehnică și comercială toate componentele software, hardware și de servicii pe care le consideră necesare, chiar dacă acestea nu sunt individualizate sau solicitate în mod explicit.

Atingerea interoperabilității necesită coordonare între sectoare atunci când se dezvoltă soluții digitale. În cadrul elaborării documentației de implementare sunt recomandate următoarele:

- Terminologie comună pentru proiectarea, evaluarea și comunicarea despre soluțiile de eGovernment: administrațiile publice pot beneficia în mare măsură de terminologia comună pentru a comunica eficient și fără ambiguități – peste barierele lingvistice și jargonul specific domeniului – atunci când proiectează, evaluează, documentează și descoperă blocuri de construcție a soluțiilor (cadre), instrumente, servicii utilizate pentru a furniza servicii publice digitale interoperabile;
- Interfețe stabile și standardizate pentru serviciile publice digitale: arhitecții și dezvoltatorii IT au sarcina de a defini interfețe stabile între serviciile publice digitale, conform standardelor deschise și specificațiilor de interoperabilitate (prin, de exemplu, Biblioteca Europeană de Specificații de Interoperabilitate, ELIS), astfel încât partenerii se pot baza pe ei pentru a construi servicii publice digitale noi, agregate și pentru a evita blocarea furnizorilor;
- privire de ansamblu asupra blocurilor de construcție a soluțiilor (SBB) deja existente, cum este, de exemplu, nodul EIDAS.

4.2. PREVEDERI DE SECURITATE

Pentru securitatea și confidențialitatea schimbului de date se vor asigura mecanisme de securitate, în conformitate cu cerințele de securitate aplicabile categoriei respective de date.

Transferul datelor prin intermediul sistemului se va realiza în formă criptată.

Transferul datelor trebuie organizat într-o manieră în care identitatea destinatarului este cunoscută în mod cert înainte de a permite destinatarului să prelucreze datele primite.

Furnizorul sistemului informatic trebuie:

- să asigure implementarea cerințelor minime de securitate cibernetică prevăzute de legislația națională și europeană și de standardele și specificațiile naționale, europene și internaționale aplicabile în domeniul securității cibernetice, în special cele prevăzute de Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare;
- să implementeze, să asigure procese și proceduri specifice pentru asigurarea securității operaționale a serviciului;
- să se asigure că datele stocate sau aflate în tranzit sunt protejate în mod adecvat împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri de protecție a rețelei informatice și de criptare a datelor;
- să nu permită accesul fără drept la datele din sistem aflate sub autoritatea lor și să se asigure că accesul la toate interfețele de servicii este limitat la persoanele autentificate și autorizate pe baza necesității de a cunoaște;
- să nu afecteze, prin acțiunile proprii, securitatea altor rețele și sisteme informatice;
- să se asigure că personalul este instruit corespunzător pentru utilizarea Sistemului Informatic și controlat periodic pentru a preîntâmpina erori umane sau încălcări de securitate.
- să se asigure că protecția datelor este garantată prin implementarea, la nivelul fiecărui sistem informatic implicat în schimbul de date, a:
    - principiilor „confidențialității prin concepție” și „securității prin concepție”, pentru a asigura securitatea modulelor și a infrastructurii lor;
    - planurilor 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;
    - planurilor de continuitate a activității și planurilor de rezervă și de redresare pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucere a tuturor funcțiilor la situația normală cât mai curând posibil;
    - unui 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 monitorizate și trebuie luate măsuri corespunzătoare pentru a preveni orice repetare a încălcărilor.

Ținând cont că sistemul informatic va gestiona date cu caracter personal, vor trebui respectate următoarele 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** - sistemul trebuie să asigure un proces de disponibilitate prin garantarea redundanței tuturor componentelor sistemului, pentru asigurarea păstrării coerentei și necoruperii datelor.

În cadrul proiectului, se va implementa o serie întreagă de soluții și instrumente de securitate, printre care:

- Asigurarea posibilităților de autentificare multifactor folosind două modalități de tipul carduri electronice cu certificate digitale, OTP, etc., prin interconectarea cu sisteme de furnizare de identitate notificate conform regulamentului EIDAS (ROeID) și reutilizare nod eIDAS, conform documentației publice privind implementarea once-only principle;
- Posibilitatea de criptare a datelor în trafic și în modul de stocare în baza de date;
- Auditarea activităților realizate în sistem și a solicitărilor de acces la serviciile expuse prin intermediul platformei.

Ofertantul si subcontractanții acestuia trebuie să fie certificați pentru standardele ISO/IEC 27001 și 27002 pentru securitatea informațiilor

5. CERINȚELE FUNCȚIONALE ALE SISTEMULUI

5.1. CERINȚE FUNCȚIONALE

În cadrul sistemului informatic integrat se vor dezvolta următoarele cerințe:

5.1.1. Portal public în vederea asigurării accesului cetățenilor la informații și servicii publice digitale

Soluția va dispune de o **interfață de tip portal web**, prin care vor fi puse la dispoziția cetățenilor informații și servicii structurate în așa fel încât să permită utilizatorului să se ghideze singur către problematica dorită și să consulte informațiile dorite.

Se vor implementa astfel atât servicii electronice complete, cu grad mare de sofisticare (transmitere integral electronică a dosarelor aferente solicitărilor, precum și primirea electronică a răspunsurilor sau a documentelor solicitate), cât și servicii electronice parțiale, cu grad mai scăzut de sofisticare (transmitere electronică a solicitării și ulterior ridicare a documentelor emise de la ghișee sau doar accesul la formulare tipizate sau simpla informare cu privire la procedurile necesare în vederea obținerii unui anumit serviciu).

Portalul Public:

Va asigura accesul online la serviciile gestionate exclusiv de către APIA și va fi compus dintr-o platformă (portal WEB) de furnizare a serviciilor electronice pentru cetățeni și mediul de afaceri, de tip spațiu privat virtual, prevăzută cu:

- Facilități de transmitere integral electronică a cererilor/formularelor aferente solicitărilor;
- Primirea electronică a răspunsurilor sau a documentelor solicitate, cu semnătură electronică și/sau scanate, după caz;
- Informare/asistență online cu privire la serviciile publice, prin intermediul unei facilități de tip chat bot bazat pe inteligență artificială integrat în spațiul privat virtual;
- Transmitere de notificări cu privire la statusul cererilor depuse;
- Petiții prin portal și prin aplicațiile mobile;
- Integrare în portal a petițiilor depuse fizic la registratura APIA;
- Aplicații Mobile pentru IOS și Android.

Funcționalități suplimentare ce ar trebui asigurate prin Portalul Public:

- **Urmărirea în timp real a stadiului cererilor, autorizărilor și plăților**, cu afișarea detaliată a etapelor parcurse și termenelor estimate de soluționare, stadiul recuperării creanțelor;
- **Spațiu personalizat pentru fiecare utilizator**, care să permită vizualizarea istoricului solicitărilor, documentelor depuse, răspunsurilor primite și notificărilor primite de la APIA;
- **Sistem de autentificare securizat**, utilizând mijloace de identificare electronică (ex. eIDAS, SPV, CNP și parolă, semnătură electronică calificată etc.);
- **Integrare cu alte platforme guvernamentale** (ex. Ghiseul.ro, hub-ul de interoperabilitate, sistemul național de plăți), pentru simplificarea fluxurilor administrative și evitarea depunerii multiple de documente;

- **Calendar electronic de programări și consultări**, pentru programarea online a întâlnirilor cu funcționarii APIA;
- **Mecanism de feedback și evaluare a satisfacției utilizatorilor**, pentru îmbunătățirea continuă a serviciilor publice;
- **Acces la materiale informative și tutoriale video**, privind modul de completare a cererilor, procedurile administrative și criteriile de eligibilitate;
- **Arhivă electronică securizată**, care să permită stocarea și accesarea documentelor depuse pe o perioadă determinată;
- **Sistem de raportare și statistici personalizate**, care să ofere utilizatorilor o imagine de ansamblu asupra cererilor proprii sau asupra fondurilor disponibile/consumate;
- **Mecanism de alertare automată**, pentru termene-limită, documente lipsă sau modificări legislative relevante.

Ca flux de interacțiune cu utilizatorul, spațiul privat virtual va pune la dispoziție formulare online pre-completate. Datele pentru pre-completare vor fi preluate, în funcție de metadatele stabilite pentru fiecare formular (v. mai jos și în anexe), via serviciu web, din Sistemul Integrat de Administrare și Control (IACS). Interfața online va permite atât completarea online a formularului completat, cât și descărcarea unui fișier PDF inteligent, pentru completare off-line. La finalul completării formularului online, va fi generat fișierul PDF în vederea semnării electronice. PDF semnat electronic va fi apoi integrat în pachetul de documente electronice configurat a fi necesar pentru fiecare tip de interacțiune cu utilizatorul.

Spațiul privat virtual va permite utilizatorului, de asemenea, accesarea lpis.apia.org.ro sau a link-ului specific aplicației geospațiale după caz, fără a mai fi necesară autentificarea suplimentară.

Portalul public va permite, de asemenea, un tip de utilizator reprezentând altă autoritate publică. Acesta va avea la dispoziție o interfață prin care va putea încărca documente (e.g., adeverințe) cu privire la un anumit solicitant (identificat în interfață prin CNP/cui după caz).

Pentru cetățenii interesați care nu sunt înrolați în registrul unic de identificare, sistemul va pune la dispoziție și o interfață prin care aceștia se vor putea înrola și solicita identificator unic, după caz.

5.1.2. Sistem de management / gestiune a documentelor

Portalul va fi integrat cu un sistem de gestionare a documentelor (DMS) care permite configurarea fluxurilor interne de lucru conform modului de organizare și funcționare al instituției. DMS-ul va permite centralizarea facilă, controlul, securizarea și trasabilitatea documentelor și a sarcinilor de lucru, pe baza unui mecanism de gestionare a rolului utilizatorilor configurabil pornind de la atribuțiile de serviciu ale angajaților instituției.

În mod curent, APIA gestionează un volum mare de date și informații, iar buna lor gestionare presupune colectarea, clasificarea, indexarea și stocarea fizică a nenumărate dosare pe suport de hârtie. Și aceste documente, pe lângă cele provenite prin intermediul portalului online, vor trebui să fie digitizate și integrate în fluxurile de lucru administrate unitar via DMS.

Din documentele aflate pe fluxurile de lucru în DMS, la diferite etape ale procesării, vor fi necesare atât validări cu date existente în IACS, cât și actualizări ale unor date din IACS cu date extrase din documente. Pentru interacțiunea dintre DMS și IACS vor fi configurate servicii web care să permită completarea automată a diferitelor interfețe de lucru ale IACS cu date extrase din documente. În sens invers, validările realizate cu succes în IACS/aplicatia geospațială vor trebui să poată funcționa drept condiții pentru a permite fluxurilor din DMS trecerea la pasul următor.

Prin intermediul sistemului de management, documente pot fi identificate cu ușurință, sunt protejate de ștergeri accidentale ori intenționate și se poate verifica stadiul de lucru în care se află un anumit document.
Beneficiile unei soluții pentru managementul documentelor sunt imediate și presupun:

- reducerea costurilor de administrare și depozitare a documentelor;
- protejarea eficientă a datelor sensibile;
- acces controlat la documente;
- creșterea productivității;
- conformarea cu legislația în vigoare;
- existența unei baze de date unitare;
- integrarea facilă cu alte sisteme;
- identificarea facilă a informațiilor în funcție de context.
- Instrumente de raportare și monitorizare, care să permită vizualizarea volumului de documente gestionate, a duratei de procesare și a gradului de utilizare a fluxurilor;
- Interfață web și mobilă, care să asigure accesul securizat la documente și sarcini de oriunde, inclusiv prin aplicațiile mobile ale portalului;
- Notificări automate și alerte, pentru termene-limită, documente în așteptare sau aprobări întârziate;
- Modul de colaborare (comentarii, atașamente, note interne), pentru lucrul în echipă pe același document, fără duplicare;
- Suport pentru clasificarea documentelor conform tipologiilor APIA (cereri, rapoarte, decizii, note interne, dosare de plată etc.), cu posibilitatea de creare de modele (template-uri) standardizate.

Funcționalități minime ale sistemului integrat:

Registratura electronică

DMS-ul va conține inclusiv o soluție de registratură electronică. Aceasta va permite preluarea documentelor din următoarele surse:

- Documente electronice depuse de utilizatori prin intermediul diferitelor funcționalități ale portalului sau furnizate pe e-mail pe adresa de corespondență APIA.
- Documente digitizate rezultate din scanarea și OCR-izarea dosarelor depuse în format fizic sau cele furnizate pe e-mail ce nu sunt în format care să permită citirea automată a informațiilor. Pentru acestea, soluția trebuie să pună la dispoziție o interfață care să permită încărcarea de către angajații registraturilor a documentelor OCR-izate. Interfața va permite generarea de noi sarcini de lucru, la nivelul DMS, aferente dosarului respectiv. De asemenea, interfața va permite asocierea acelui dosar cu un cont de utilizator din portal sau generarea unui nou cont de utilizator în portal. Print intermediul acelui cont de utilizator, fermierul își va putea accesa spațiul privat virtual, în care va putea regăsi toate

documentele digitizate și toate informațiile despre stadiul procedurii (în mod similar cu situația în care ar fi depus acele documente electronic). Pentru realizarea digitizării documentelor, vor fi puse la dispoziție echipamente de tip scanner, în fiecare punct de lucru APIA.
- Documente interne APIA necesare pentru asigurarea fluxurilor de lucru și gestionare a documentelor

- **Înregistrare automată a documentelor sosite prin multiple canale** (portal online, e-mail oficial, API, poștă electronică guvernamentală, ghișeu fizic), cu posibilitatea de clasificare automată pe baza conținutului sau metadatelor;
- **Generare automată a numerelor de înregistrare** conform regulilor instituției (inclusiv prefixe, sufixe, an, tip document, cod direcție etc.);
- **Marcarea documentelor cu niveluri de clasificare/confidențialitate** (public, intern, restricționat, secret etc.);
- **Căutare și filtrare avansată** după criterii multiple (număr de înregistrare, emitent, beneficiar, termen, tip document, cuvinte-cheie din conținut);
- **Validarea automată a câmpurilor obligatorii** la înregistrare (ex. tip document, emitent, dată, compartiment responsabil), reducând erorile de introducere;
- **Funcționalitate de redirecționare / repartizare automată** a documentelor către compartimente sau persoane responsabile, în funcție de tipul sau sursa acestora;
- **Corelare automată cu dosarele existente** — dacă un document aparține unui dosar deja înregistrat, acesta este atașat automat acolo.
- **Fluxuri de lucru configurabile pentru procesarea documentelor**, inclusiv stadii predefinite (înregistrat – repartizat – în lucru – rezolvat – arhivat);
- **Alocare automată a termenelor de răspuns** conform legislației (ex. 30 de zile pentru petiții, 10 zile pentru răspunsuri interinstituționale etc.);
- **Notificări automate** către utilizatori privind documente noi, termene-limită, sau solicitări repartizate.
- **Alerte automate pentru documente care depășesc termenul de răspuns**;
- **Rapoarte și statistici dinamice** privind volumul documentelor înregistrate, timpul mediu de soluționare, distribuția pe departamente etc.;
- **Export automat de rapoarte** pentru conducere, auditori sau alte instituții de control.
- **Integrare cu modul OCR** (recunoaștere optică a textului) pentru scanarea și indexarea documentelor fizice;
- **Scanare directă în aplicație** și salvarea automată în format PDF/A;
- **Acces mobil securizat,** pentru ca documentele să poată fi vizualizate sau aprobate de pe dispozitive mobile;

Descriere componentă registratură electronică

Registratura electronică este soluția eficientă de înregistrare a documentelor și de păstrare a evidenței acestora.

Modulul de registratură înregistrează rapid intrările și ieșirile de documente, reduce apariția erorii umane, urmărește în timp real intrările și ieșirile și oferă flexibilitatea de a atașa ulterior documente la înregistrarea inițială.

Aplicația permite înregistrarea tuturor documentelor vehiculate într-o instituție și gestionarea eficientă a acestora, oferind o evidență în timp real a documentelor din sistem. Modulul de registratură electronică are o interfață intuitivă și pune accentul pe eficiență și implicit pe mai puțin timp petrecut cu procesarea documentelor.

Registratura este modulul din aplicație care se ocupă cu introducerea rapidă a documentelor în sistem și generarea de numere de înregistrare pentru acestea sau pentru dosarele în care sunt conținute. Documentele și dosarele care sunt create vor fi stocate în Depozitul de documente, în locația stabilită de utilizator la generarea lor sau locația stabilită implicit de către administratorul aplicației. La nivelul aplicației pot fi definite mai multe depozite de documente.

Registratura este compusă din registre, la care un utilizator poate avea acces în funcție de drepturile pe care le deține. Registrele conțin documentele sau dosarele înregistrate și li se pot aloca intervale de numerotare precum și atribuirea unui format specific de numerotare.

În cadrul sistemul de management al documentelor vor fi definite oricâte registre (nu există o limitare a numărului de registre permise), configurate în funcție de necesitățile identificate în faza de analiză sau pe parcursul proiectului. O intrare în registratura conține atât metadate, cât și fișiere asociate.

Automatizarea și optimizarea fluxurilor de lucru

În cadrul sistemului se va asigura **automatizarea și optimizarea fluxurilor de lucru:**

Software-ul de automatizare a fluxurilor de lucru eficientizează activitățile care sunt în mod tradițional manuale, pentru a ajuta instituțiile să economisească timp, să reducă riscul erorii umane și să sporească productivitatea la locul de muncă.

Prin automatizarea proceselor, permite echipelor să se concentreze pe proiectele cu impact mai mare, în locul activităților repetitive, și oferă vizibilitate asupra fluxurilor de lucru pentru a ajuta la identificarea zonelor de oportunitate.

Un flux de lucru este o secvență organizată de sarcini, activități sau procese. Aceste fluxuri de lucru sunt, de asemenea, o modalitate de a vedea cum funcționează activitățile.
Permit gestiunea proceselor, asigurând circulația documentelor pe trasee ierarhice sau pre-configurate, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea și circulația informațiilor și a documentelor în cadrul organizației, precum și a celor generate în relația cu terți.

Designerul de fluxuri permite utilizatorilor să proiecteze și să simuleze procesele într-un mediu bazat pe web. Modelatorul de date permite utilizatorilor non-tehnici să vizualizeze, să modifice și să creeze modele de date.

Flux de înregistrare a solicitărilor

Un fermier sau oricare cetățean ar putea utiliza platforma ce va fi implementată pentru a depune o gamă largă de solicitări și documentații legate de gestionarea și accesarea fondurilor aflate în atribuțiile APIA. Platforma facilitează procesul de comunicare cu autoritățile competente, oferind un mijloc eficient și organizat pentru trimiterea și primirea de informații.

Prin utilizarea registraturii electronice, procesul de gestionare a fondurilor europene devine mai transparent, mai rapid și mai eficient, reducând birocrația și timpul de așteptare pentru procesarea documentelor.

Beneficiarii pot avea acces mai ușor la informațiile de care au nevoie și pot gestiona mai eficient aspectele administrative ale proiectelor finanțate de UE.

Acest flux are în vedere necesitate unor operațiunii cât mai simple pentru utilizator, ținând cont de publicul țintă principal (fermieri - oameni care lucrează în câmp, în ferme și care își doresc o interfață facilă, rapidă).

Înregistrarea Solicitării: Punctul inițial/start - utilizatorii înregistrează o cerere în portal (se va aloca număr de înregistrare automat).

Utilizatorul va selecta din meniurile predefinite tipul de solicitare, de exemplu:

- contestație,
- reclamație/petiție,
- înștiințare,
- completare documente,
- completare cerere, modificare cerere, retragere cerere,
- solicitare de informații (va selecta ce tip de informații dorește- Legea 544/2001, informații suplimentare legate de oportunitățile de finanțare disponibile, condiții de eligibilitate sau termene limită, altele),
- alt tip.

În funcție de selecția inițială, meniul va afișa doar variantele specifice, spre ex:

- utilizatorul alege la „Tip cerere" - contestație;
- sistemul va afișa un meniu „Tip contestație":
    - Contestație la raportul de control,
    - Contestație la decizia de plată,
    - Contestație la procesul-verbal de stabilire a creanțelor bugetare,
    - Alt tip de contestație.

De asemenea, pentru uniformizarea solicitărilor, meniul va conține un câmp denumit "Tipul subiectului/ Informații despre subiectul cererii", în care vor fi completate informații, de exemplu:

- Statusul cererii depuse (se va completa numărul cererii),
- Decizia de plată pentru cererea …. (se va introduce nr de înregistrare al acesteia),
- Eliberare adeverință tip…. (selector de tipuri, se va selecta tipul),
- Transmitere documente din dosarul cererii de plată (implementarea unei verificări CNP solicitant/ CNP pentru care se solicită, dacă nu sunt identice se va genera un răspuns precompletat având la bază prevederile legislative legate de furnizarea de informații despre alte persoane/ date cu caracter personal, răspuns care va fi validat de un funcționar APIA). Ar trebui să existe o excepție cu privire la solicitarea de documente de către administratorul unei societăți, verificarea trebuind să fie făcută la nivel de CNP administrator.
- rezultatele controalelor de orice tip efectuate pentru cererea/cererile sale, dacă acestea au fost finalizate;

Verificarea Validității (Schimbare status "verificare completitudine"): se verifică dacă cererea îndeplinește anumite criterii (de exemplu, completitudinea informațiilor, date de contact valide, verificare corespondenta CNP/CUI cu ID fermier pentru utilizatorii înregistrați etc).

În această etapă, ar trebui să existe două posibilități:

1. Solicitarea este incompletă, se transmite către utilizator pentru completare, se schimbă statusul în „incomplet”;
2. Solicitarea este validă, continuă fluxul spre repartizare, se schimbă statusul în „complet”.

Repartizarea cererii: pentru solicitările al căror obiect este clar, care fac parte din categoriile prestabilite, ar trebui să existe posibilitatea repartizării automate atât către Secretariatul general/județean, dar și către Direcția de specialitate/ serviciu/birou după caz (pe baza unui algoritm de corespondență subiect ales de utilizator - atribuții direcții).

Spre exemplu, un utilizator dorește să afle care este valoarea debitului datorat. Dacă va alege din câmpul de tematică propusă „Debite/obligații financiare”, solicitarea poate fi direcționată și către directorul Direcției Economice/Șeful Serviciul recuperare debite. Propunerea este să fie direcționată către un funcționar de conducere, având în vedere obligația acestuia de a repartiza cererea către un consilier din cadrul compartimentului pe care îl coordonează, dar și pentru respectarea confidențialității, prevenirea oricăror situații de incompatibilitate sau de acces neautorizat.

În aceasta etapă, statusul devine „repartizat spre rezolvare”.

Procesarea solicitării de informații: Etapele de procesare a solicitării, care pot include revizuire, aprobare, etc. În principiu se reia fluxul, dar în sens invers.

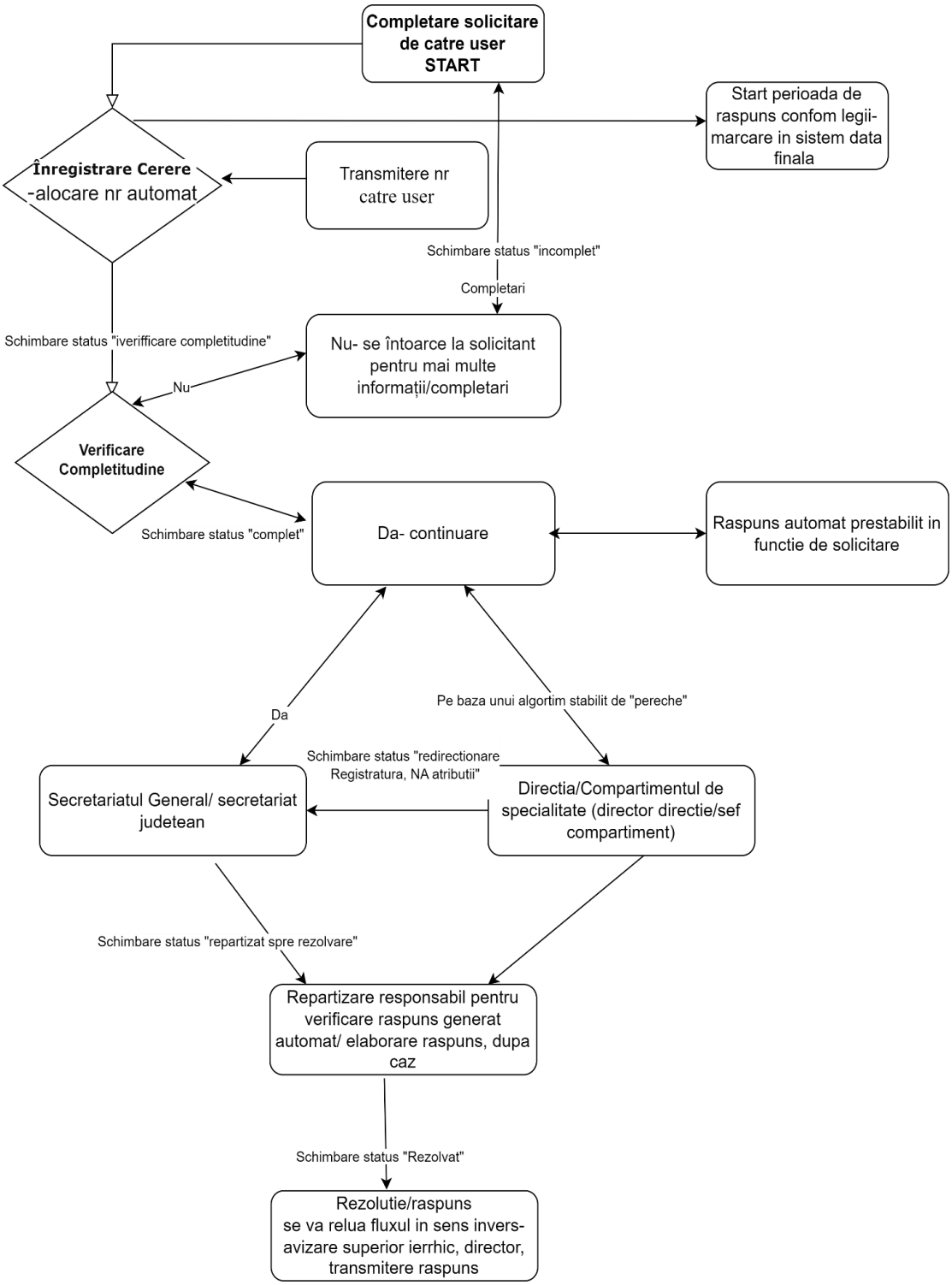
Comunicarea cu Solicitantul: Interacțiunea cu persoana care a făcut cererea, cum ar fi notificările despre statusul cererii- în contul de utilizator, acesta poate urmări statusul cererii. Pentru persoanele care nu au cont de utilizator, va exista posibilitatea verificării statusului prin completarea datelor personale și a numărului de înregistrare primit la depunere inițială (sau chiar și în lipsa acestuia, câmpul să nu fie unul blocant dacă nu este completat).

Rezolvarea: Etapa finală, se transmite răspuns solicitantului, solicitarea trece în status „închis”.

Atenție: orice solicitare înregistrată prin portal trebuie dusă în status închis, chiar dacă răspunsul nu este unul favorabil solicitantului.

În cazul în care solicitarea nu intră în atribuțiile APIA, aceasta trebuie redirecționată instituțiilor abilitate, conform legii. Și în acest caz i se transmite răspuns solicitantului, urmând pașii de mai sus, iar cererea trece în status „închis”.

Ghiduri și Asistență: în Portal vor fi accesibile ghiduri pas cu pas pentru completarea documentelor


Completare solicitare de catre user START
Start perioada de raspuns confom legii- marcare in sistem data finala
Înregistrare Cerere -alocare nr automat
Transmitere nr catre user
Schimbare status "incomplet"
Completari
Schimbare status "iverifficare completitudine"
Nu- se întoarce la solicitant pentru mai multe informații/completari
Nu
Verificare Completitudine
Schimbare status "complet"
Da- continuare
Raspuns automat prestabilit in functie de solicitare
Da
Pe baza unui algortim stabilit de "pereche"
Schimbare status "redirectionare Registratura, NA atributii"
Secretariatul General/ secretariat judetean
Directia/Compartimentul de specialitate (director directie/sef compartiment)
Schimbare status "repartizat spre rezolvare"
Repartizare responsabil pentru verificare raspuns generat automat/ elaborare raspuns, dupa caz
Schimbare status "Rezolvat"
Rezolutie/raspuns se va relua fluxul in sens invers- avizare superior ierrhic, director, transmitere raspuns

Utilizator înregistrat

Portalul va permite înregistrarea fiecărui beneficiar/fermier care dorește acest lucru. Pe baza datelor transmise - nume, CNP, adresă e-mail, număr de telefon pentru înregistrarea în 2 pași ca element suplimentar de Securitate - se vor crea date de acces sub forma utilizator și parolă, precum și contul aferent.

Pentru fermierii care au cereri depuse la APIA, utilizatorul poate fi id-ul de fermier/ acesta trebuie să fie obligatoriu de completat la accesarea anumitor meniu/ solicitări (eroare blocantă).

Totuși, pentru facilitarea accesului la ID-ul de fermier, portalul va conține un meniu în cadrul căruia, pe baza CNP/CUI, se va face verificarea cu Registrul fermierilor și se va afișa id-ul de fermier sau mesaj că nu există ID pentru acel CNP/CUI.
Pentru utilizatorii APIA se vor defini useri si roluri specifice în funcție de atribuțiile specifice pe care le au pe fluxul de lucru.

Depunerea de documente justificative pentru cererile de plată

Pe fluxurile specifice au fost identificate mai multe tipuri de documente care sunt necesar a fi depuse de cetățenii care solicită plata în domeniul agricol pentru măsurile/intervențiile gestionate de APIA.

Documente ce se pot depune electronic (completate sau scanate) pe fluxurile de lucru printr-un sistem electronic sunt de exemplu fără a ne limita la acestea:

5.1.2.1 Documente specifice depunerii/modificării cererii de plată pentru diverse intervenții:

- Documente Contabile Interne,
- Declarație de multiplicare,
- Carnet de comercializare,
- Copie autorizare ca procesator – cânepă,
- Copie autorizație de cultivare/procesare – cânepă,
- Copie Contract încheiat intre fermier și Procesator/Cumpărător,
- Documentul oficial de calitate a seminței utilizate,
- Acte doveditoare privind livrarea,
- Declarație privind varietăți de cânepă cultivate și cantități de semințe utilizate pentru cânepă,
- Copie de pe certificatul de înregistrare/sau certificatul constatator eliberat de Oficiul Național al Registrului Comerțului din care să rezulte activitatea de procesare a unității către care a livrat producția,
- Copie Factură cumpărare semințe certificate,
- Document privind utilizare producție pentru furajare,
- Adeverință conformă cu Registrul Agricol (poate fi realizată interfața cu registrul agricol sau document tipizat care să fie completat de responsabili din cadrul primăriilor),
- Dovada încheierii activității ca administrator/acționar,
- Adeverință de rol agricol (poate fi realizată interfața cu registrul agricol sau document tipizat care să fie completat de responsabili din cadrul primăriilor),
- Certificatul de înregistrare ONRC (poate fi realizată interfața cu registrul ONRC sau document tipizat care să fie completat de responsabili din ONRC).

- Registrul acționariatului societății,
- Statutul,
- Actul de înființare/actul constitutiv/actul normativ de înființare/regulamentul de organizare și funcționare,
- Documente de forță majoră / circumstanțe excepționale (FM/CE) și circumstanțe naturale (CN),
- Extras de cont bancar,
- Certificatul constatator eliberat de ONRC (poate fi realizată interfața cu registrul ONRC sau document tipizat care să fie completat de responsabili din ONRC),
- Actul de înființare/actul constitutiv/actul normativ de înființare,
- Fișa postului,
- Contract închiriere/concesiune/comodat cu unitățile administrativ-teritoriale,
- Contract concesiune cu ADS (poate fi realizată interfața cu ADS sau document tipizat care să fie completat de responsabili din ADS),
- Adeverința eliberată de Agenția Națională de Administrare Fiscala,
- Adeverința privind veniturile realizate,
- Procura notarială/împuternicire,
- Documente care dovedesc utilizarea terenului,
- Autorizații pentru producerea seminței,
- Proces verbal de calamitate,
- Alte documente care vor fi identificate la momentul analizei pentru implementare.

5.1.2.2 Documente specifice pentru controalele pe teren:

- Înștiințări pentru încorporarea culturii de toamnă/ acoperirea solului / banda M10-P7,
- Registrul exploatației,
- Magazie PPP,
- Platformă gunoi,
- Registrul de evidență a PPP,
- Caietele de agromediu,
- Plan de fertilizare,
- Dovadă justificare arderi,
- Notificarea – GAEC 7,
- Copie raport de control,
- Situații privind parcelele neconforme (codificate cu roșu) pentru care sunt necesare clarificări și/sau fotografii cu geolocație,
- Depunerea contestațiilor la raportul final de control prin monitorizare,
- Alte documente care vor fi identificate la momentul analizei pentru implementare.

5.1.2.3 Documente specifice pentru rentieri:

- Declarația pentru obținerea vizei anuale (Anexa 1),
- Cererea de reanalizare a dosarului (Anexa 2),
- Cererea moștenitorului (Anexa 3),
- Cererea de eliberare duplicat carnet de rentier agricol (Anexa 4),
- Cererea de modificare date (Anexa 5),
- Cererea de modificare date moștenitor (Anexa 5.1),
- Răspuns la Notificarea de completare documente pentru acordarea rentei viagere agricole,

- Alte documente care vor fi identificate la momentul analizei pentru implementare.

5.1.2.4 Interfața pentru petiții și sesizări

- Cererea de eliberare date și informații pe Legea 544/2001,
- Alte cereri de clarificare referitoare la cererile de sprijin depuse de solicitanții sprijin.

5.1.2.5 Depunerea de documente de modificare a cererilor existente

Se va asigura funcționalitate pentru efectuarea solicitărilor de modificări ale cererilor în derulare, conform termenelor și în funcție și de statusul cererii.

Au fost identificate următoarele tipuri de documente care pot fi completate electronic de către cetățean pe fluxurile de lucru specific cererilor de plată prin interfața nou creată:

- Declarație privind completarea și asumarea, precum și închiderea cererii de plata (an campanie),
- Formular M1- Schimbarea declarației de suprafață (an campanie),
- Formular M1.2 - Schimbarea declarației privind apa pentru irigații (an campanie),
- Formular M2 – Completarea cererii de plată (an campanie),
- Formular M3 – Retragerea parțială a declarației de suprafață (an campanie),
- Solicitare de retragere a sprijinului aferent unor intervenții/ măsuri de sprijin din cererea de plată (an campanie),
- Declarație pe propria răspundere privind varietățile de cânepă pentru fibră cultivate și cantitatea de semințe utilizate/ha pentru înființarea culturii de cânepă,
- Declarația de retragere totală a suprafeței din cererea de plată (an campanie),
- Formularul M4 – Schimbarea adresei/coordonatelor bancare/numelui societății,
- Cerere pentru transfer de exploatație/schimbarea formei de organizare,
- Înștiințarea cu privire la forța majoră/ circumstanța excepțională,
- Alte cereri de clarificare referitoare la cererile de sprijin depuse de solicitanți.

5.1.2.6 Notificări și Comunicări

- Notificări privind schimbări legislative sau regulamente nou-aplicabile.
- Comunicări legate de controalele pe teren sau audituri programate pentru cererile depuse, dacă legislația nu stabilește interdicții în acest sens.
- Notificări legate de obligațiile sale aferente cererilor depuse, de tipul „este necesar să transmiteți până la data de xx/xx/xxxx”, „este necesar să vă prezentați la data de xx/xx/xxxx”.
- Setări personalizate pentru tipurile de alerte dorite.

5.1.2.7 Actualizări de Date Personale sau ale societății, asociației etc.

- Actualizarea informațiilor de contact sau a datelor bancare, însoțite de încărcarea documentelor doveditoare în portal.
- Schimbări ale structurii organizatorice sau ale reprezentanților legali, însoțite de încărcarea documentelor doveditoare în portal.

5.1.2.8 Soluționarea de Probleme și Întrebări

- Vor fi rezolvate unele dintre solicitările de clarificări sau de asistență prin implementarea unei soluții de tip chat bot care să conțină răspunsuri la anumite întrebări prestabilite și să se actualizeze dacă utilizatorii repetă o anumită problemă/întrebare care nu este prestabilită (ML/AI).

5.1.2.9 Depunerea de Contestații sau Reclamații

- Contestarea deciziilor luate de autorități în ceea ce privește administrarea, autorizarea cererilor sau rezultatele controalelor.
- Reclamații legate de întârzieri în procesarea plăților sau alte disfuncționalități.

5.1.2.10 Solicitarea de Informații

- Cereri de informații suplimentare legate de oportunitățile de finanțare disponibile, condiții de eligibilitate, sau termene limită.
- Răspunsuri predefinite automat în funcție de solicitarea utilizatorului. Spre exemplu, dacă acesta dorește să afle ce scheme/măsuri poate accesa pentru o anumită suprafață/cultură/tip de animale/sector viticol/apicol etc, sistemul să genereze automat un răspuns care să necesite doar validarea din back-office de către funcționarii APIA.
- Răspunsuri predefinite pentru solicitarea de informații legate de termenele de depunere. În meniu, vor fi implementate șabloane cu scheme/măsurile derulate astfel încât utilizatorul să selecteze schema/măsura dorită, iar sistemul să genereze automat un răspuns predefinit cu aceste informații.
- Solicitarea de informații de interes public conform Legii 544/2011 - utilizatorul va putea selecta din contul său ce tip de informații de interes public dorește (meniu prestabilit), iar dacă informațiile sunt generale (organigrama, situația veniturilor salariale brute pe funcții în cadrul APIA, acte normative specifice APIA, rapoarte, planul de achiziții etc), sistemul să genereze automat un răspuns (și să atașeze documentele, după caz), care să necesite doar validarea din back-office de către funcționarii APIA.

5.1.2.11 Posibilitatea solicitării diferitelor tipuri de adeverințe sau documente oficiale care pot confirma diverse informații financiare-contabile sau legate de cererile depuse.

- Pot fi documente ca: adeverințele pentru solicitarea de credit, adeverință cu suma plătită, situația plăților, situația creanțelor, sancțiunilor multianuale, suprafața depusă, scheme accesate.

Din contul de utilizator va exista meniul „Solicită adeverință”, iar utilizatorul va selecta tipul acesteia:
- adeverință tip pentru solicitare credit bancar,
- adeverință tip pentru dovada sumelor plătite de către APIA (va exista posibilitatea selectării perioadei pentru care se dorește),
- adeverință tip necesară depunerii proiectelor la AFIR,
- extras din Registrul fermierilor (format tip prin care se atestă că utilizatorul este înscris în RUI, cu ID fermier),
- adeverință din care să rezulte numărul de animale per exploatație (integrare cu bazele de date ANSVA, ANZ/cu baza de date IACS- raportul UVM din sistem),
- adeverințe emise de responsabili management resurse umane.

Sistemul va completa automat datele prin integrare cu sistemele existente la nivel APIA (IACS, SVAP, APLICATIA GEOSPATIALA, etc).

5.1.2.12 Interfațare cu Ipa Online/Aplicația geospațială pentru ca utilizatorul să poată identifica suprafețe pe baza coordonatelor cadastrale/ numărului cadastral.

Se va integra în cadrul interfeței o funcționalitate prin care se poată accesa aplicația geospațială, fără a mai fi necesară autentificarea suplimentară în aceasta. Nu se va realiza dezvoltare GIS suplimentară.

5.1.2.13 Meniu de simulare

Meniul de simulare ar trebui să ofere utilizatorilor informații despre sumele de bani ce pot fi obținute pe suprafață, pe animale, motorină și orice alt tip de măsuri/scheme/intervenții derulate prin APIA. Acest lucru va include subvenții pe suprafață, plăți directe, subvenții pentru tinerii fermieri, orice alte intervenții ce se desfășoară la nivelul APIA.

Utilizatorul va completa câmpuri prestabilite, precum: tipul de cultură, suprafața, numărul și tipul de animale, practicile agricole sustenabile, vârsta, tipul sprijinului, etc, după caz.

La nivelul APIA sunt gestionate peste 80 de intervenții și pachete pentru care se acordă sprijin, ca urmare simularea trebuie realizată pentru cel puțin 80 de intervenții în funcție de modificările legislative disponibile la momentul implementării sistemului. Simulatorul trebuie, așadar, să fie configurabil de către personalul responsabil din cadrul instituției pentru a implementa variabilitatea în timp a prevederilor legale.

5.1.2.14 Programări online pentru audiențe

Se va realiza o interfață în care solicitanții de audiență să poată solicita o audiență. Confirmarea audienței se va face prin portal și se va transmite și pe e-mail/ sms către solicitant pentru o mai bună comunicare în relația cu cetățenii.

La nivel de utilizator APIA ar trebui să fie implementat cel puțin:

Managementul solicitărilor primite prin Portal

- Vizualizare și gestionare solicitări și a documente depuse,
- Actualizarea stării solicitării (se va implementa notificarea cu privire la termenul scadent de răspuns),
- Comunicare directă cu cetățenii pentru clarificări sau solicitări suplimentare.

Programări și Calendar

- Vizualizarea și gestionarea programărilor, audiențelor,
- Notificări și reamintiri pentru întâlnirile programate.

Rapoarte și Analize

- Generarea de rapoarte privind tipurile de solicitări înregistrate (nr de cereri înregistrate prin Portal, nr de cereri închise, stadiul, tipul de solicitare, subiectele cele mai utilizate, timpul de răspuns etc),
- Extragere/ vizualizare Registrul de intrări-ieșiri.

Comunicare și Feedback

- Instrumente de comunicare directă cu cetățenii (mesagerie internă, email),
- Modul de Sondaje pentru primirea unor informații relevante de la utilizatorii portalului. Colectarea și analiza feedback-ului pentru îmbunătățirea serviciilor.
- Implementarea unei funcționalități de transmitere de notificări/invitații utilizatorilor înregistrați cu privire la evenimente de interes pentru aceștia (conferințe, întâlniri, informări) organizate pentru beneficiari/fermieri.

Utilizator neînregistrat

Se va defini un flux similar celui de utilizator înregistrat, însă cu stabilirea unor limitări – a unor informații la care să nu aibă acces automat.

Arhivare electronică

Arhiva electronică asigură localizarea facilă a solicitărilor primite prin portal, optimizează spațiul de stocare și oferă siguranță în procesarea și stocarea datelor.
Arhiva electronică este o soluție la îndemână ce optimizează timpul și spațiul instituțiilor și oferă disponibilitate la copia electronică a documentelor ce poate fi accesată de mai mulți utilizatori în același timp. În cazul unei catastrofe sau situații de urgență, recuperarea imediată a datelor este vitală, iar deținerea unei arhive electronice este un sistem de back-up foarte bine pus la punct.
Instituțiile sunt obligate să păstreze în arhive, conform legii, anumite documente.
Cerințe funcționale:

- **Înregistrare și indexare:** Documentele trebuie să fie clasificate și indexate automat, pe baza tipului, datelor, emitentului și altor metadate relevante;
- **Căutare și regăsire rapidă:** Sistemul trebuie să permită căutare full-text, filtrare după metadate și identificarea documentelor în funcție de context;
- **Gestionarea ciclului de viață:** Sistemul trebuie să suporte fluxul complet al documentelor: înregistrare – procesare – arhivare – distrugere conform termenelor legale;
- **Acces controlat:** Accesul la documente trebuie să fie securizat, bazat pe roluri și niveluri de confidențialitate (public, intern, secret);
- **Audit și trasabilitate:** Toate operațiunile asupra documentelor trebuie înregistrate în jurnal de audit, inclusiv modificări, vizualizări și ștergeri;
- **Integrare:** Arhiva electronică trebuie să fie integrată cu sistemul de management al documentelor (DMS) și cu registratura electronică, pentru un flux de lucru unitar;
- **Automatizare backup:** Sistemul trebuie să asigure replicarea și backup-ul automat al datelor, cu posibilitatea restaurării rapide în caz de incident;
- **Format și compatibilitate:** Documentele trebuie stocate în formate standardizate (PDF/A, XML etc.), compatibile cu arhivarea pe termen lung;
- **Acces simultan:** Mai mulți utilizatori pot accesa în același timp copii electronice ale documentelor, fără conflicte de acces;
- **Interoperabilitate:** Sistemul trebuie să permită schimbul de documente și date cu alte arhive electronice sau platforme guvernamentale, respectând standardele naționale și europene.

Beneficii

- Reducerea costurilor cu spațiul fizic și administrarea documentelor pe hârtie;
- Disponibilitate rapidă și continuă a documentelor arhivate, inclusiv în situații de urgență;
- Suport pentru audit și raportare detaliată;
- Scalabilitate pentru gestionarea volumelor mari de documente pe termen lung;

- Creșterea securității și protecției datelor sensibile.

Conformitate legală

Soluția de arhivare electronică trebuie să respecte:

- Legea Arhivelor Naționale;
- Normele privind arhivarea documentelor electronice APIA;
- Reglementările privind protecția datelor cu caracter personal (GDPR);
- Standardele de interoperabilitate și arhivare electronică (ISO 15489, eIDAS, MoReq).

5.2. ARHITECTURA FUNCȚIONALĂ A SISTEMULUI

Arhitectura sistemului informatic și principii generale

Prin arhitectura sistemului informatic înțelegem structurile, mecanismele și interfețele utilizate, precum și comunicarea între părțile componente. Arhitectura de sistem descrie viziunea fizică și logică a sistemului propus, relevă modul în care sistemul va fi construit, definește modul în care vor fi utilizate diferite concepte, dar și aspecte vizând posibilitatea dezvoltării viitoare a sistemului.

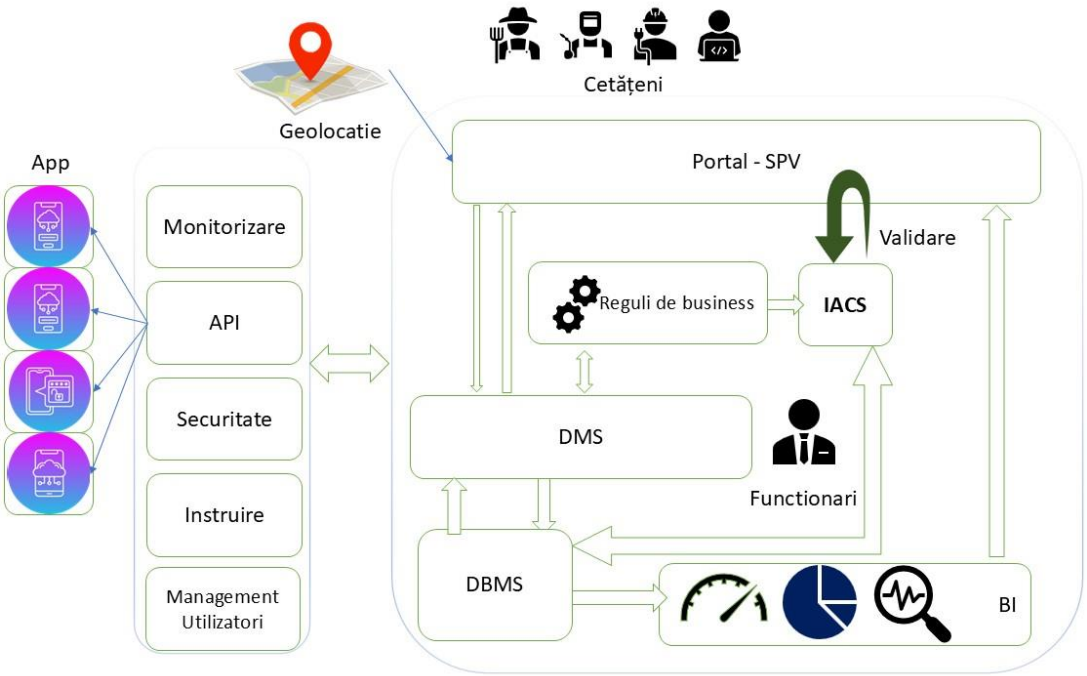
La proiectarea, realizarea și implementarea sistemului trebuie să se țină cont de următoarele principii generale:

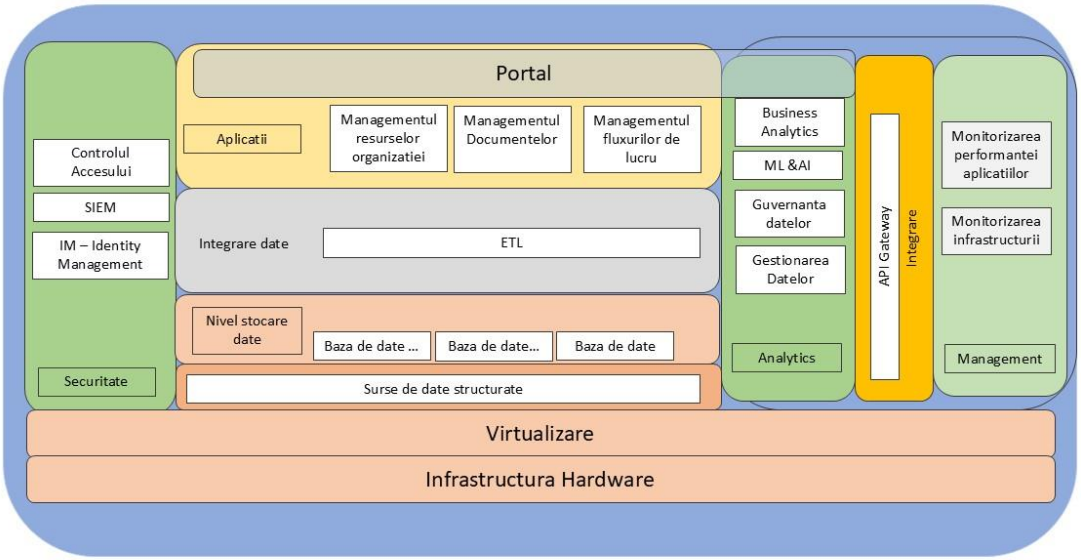
- **Principiul legalității:** care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- **Principiul divizării arhitecturii pe nivele:** constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
- **Principiul arhitecturii bazate pe servicii (SOA):** constă în distribuirea funcționalității aplicațiilor 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 canalele 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 de acces neautorizat.
- **Principiul transparenței:** presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicatii;
- **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 al 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;
- **Principiul integrării cu aplicațiile existente** în vederea utilizării în comun a informațiilor, schimbului de informații în timp real, accesului datelor dintr-o componentă în alta.

În particular, pentru arhitectura sistemului informatic se insistă asupra respectării următoarelor principii primordiale:
- implementarea unei soluții centralizate client-server, WEB based, cu acces autorizat la interfață și date, utilizând componente software mature, de tip COTS (Comercial off the shelf - existente de pe raft);
- produsele software incluse în soluție sau sub formă de subscripție valabilă pentru toate funcționalitățile pe perioada de implementare a contractului și pentru întreaga perioadă de garanție;
- asigurarea unei securități adecvate a sistemului informatic pentru a proteja informația și subsistemele componente împotriva utilizării lor neautorizate sau a divulgării informației cu caracter personal sau a celei cu accesibilitate limitată;
- dezvoltarea și implementarea sistemului informatic cu posibilitatea reutilizării datelor pentru alte procese sau în perspectiva asigurării posibilității de dezvoltare de noi funcționalități;
- asigurarea capacității de restabilire în urma dezastrelor (asigurarea securității fizice și logice) ca parte componentă a planului de implementare.
- sistemul informatic ofertat trebuie să răspundă la următoarele cerințe tehnice minimale:
    - soluție în tehnologia WEB, centralizată, în care accesul la interfață și la date sa fie un acces autorizat,
    - componentele software ofertate să fie componente bazate pe tehnologii open-source,
    - să fie asigurate măsuri de securitate a sistemului informatic, astfel încât să se protejeze informația și subsistemele componente, împotriva utilizării neautorizate sau a divulgării informațiilor cu caracter personal sau a informațiilor cu accesibilitate limitată,
    - arhitectura să fie o arhitectură modernă din punct de vedere tehnologic, de exemplu de tip multi-tier (prezentare, logica aplicației, baza de date),
    - soluția implementată să fie scalabilă și portabilă pe diverse platforme hardware,
    - să poată fi accesat folosind browsere web cele mai uzuale: Mozilla Firefox, Google Chrome, Edge,
    - să permită salvarea și recuperarea datelor înregistrate în sistem și să asigure integritatea și consistența acestora,
    - să permită restabilirea rapidă a serviciilor în cazul unei avarii accidentale,
    - separarea pe componente pentru gestiunea identității, colectarea datelor și a analiza datelor,
    - utilizarea de componente scalabile, compatibile cu arhitecturi de calcul distribuit de tip „cloud ready”,
    - utilizarea de mecanisme de raportare bazate pe standarde deschise, clare și ușor de gestionat,
    - utilizarea tehnologiilor de tip inteligență artificială și învățare mașină pentru extragerea de statistici și indicatori compoziți relevați din seturi mari de date,

- reducerea necesarului de intervenție umană în colectarea și procesarea datelor,
- platformă cu funcționalități de tip Spațiu Privat Virtual.





Pentru asigurarea obiectivelor proiectului (cap „Obiectivele proiectului”), în cadrul sistemului vor fi incluse mai multe componente și submodule împărțite pe următoarele categorii:

- *Nivel de prezentare* – portalul pentru accesul la serviciile administrative expuse;
- *Nivel de aplicații* – componentele necesare funcționării sistemului;
- *Nivelul de date* – componentele de stocare a datelor gestionate în cadrul platformei și a datelor de auditare a activităților realizate în cadrul sistemului;
- *Nivel de suport* – componentele de administrare, monitorizare, backup și replicare;
- *Securitate* – componentele de securizare a datelor la nivelul sistemului și la nivelul bazelor de date.

Principalele componente funcționale, de securitate și de suport ale platformei sunt:

- Componenta de **portal** prin intermediul căreia se expun procesele administrative necesare;
- Componenta de **management documente** ce va gestiona colaborarea inter-instituțională și internă;
- Componenta de **BPM** ce va gestiona realizarea de fluxuri de date în procesele interne și inter-instituționale;
- Sistem de **gestiune și analiză a datelor**;
- O componentă de **analiză și raportare**;
- Componenta de **interoperabilitate** ce va permite schimbul de informații între diferite sisteme existente dar și viitoare la nivelul instituțiilor publice;
- O soluție de **administrare a identității utilizatorilor** care va asigura următoarele procese:
    - Conectarea cu platforma identităților electronice RoeID și EIDAS pentru cetățenii europeni;
    - Crearea și mentenanța identităților digitale și a rolurilor în platformă, pentru identitățile care nu fac obiectul ROeID (exemplu: reprezentanți ai administrației);
    - Auditarea și raportarea informațiilor corespunzătoare proceselor executate în cadrul soluției.
- O soluție de **securizare a accesului privilegiat** care are rolul de a proteja, gestiona și monitoriza accesul privilegiat la resursele critice ale sistemului.
- O soluție de **monitorizare aplicații** ce va permite detectarea și remedierea imediată, pe cât posibil automată, problemelor de funcționare care afectează utilizarea în bune condiții a sistemului informatic și îndeplinirea sarcinilor de serviciu;
- Componenta **SIEM,** ce oferă posibilitatea colectării și monitorizării log-uri din cadrul sistemului.

5.3. MANAGEMENTUL UTILIZATORILOR ȘI ACCESUL LA SISTEM

Autentificarea participanților la schimbul de date se va putea realiza prin soluția RoeID în conformitate cu cerințele naționale privind identificarea electronică și autentificarea utilizatorilor în mediul online.

Soluția tehnică propusă trebuie să asigure un **nivel ridicat de securitate, trasabilitate și conformitate** în procesul de autentificare, autorizare și audit al activităților desfășurate în cadrul aplicațiilor instituției.

Este necesar ca soluția tehnică să implementeze cel puțin următoarele funcționalități:

- posibilitatea restricționării accesului utilizatorilor privilegiați la datele manipulate de aplicațiile de business, prin segregarea responsabilității;
- autentificarea furnizorilor de servicii și a altor persoane autorizate , cu control individual al drepturilor de acces;
- posibilitatea de autentificare multi-factor (MFA), bazată pe metode recunoscute (parolă + certificat digital / OTP / dispozitiv mobil);
- dezactivarea automată a conturilor neutilizate sau compromise.

Această componentă trebuie să răspundă următoarelor cerințe generale:

- Definirea și documentarea procedurilor și proceselor necesare pentru operarea soluției.

- Minimum următoarele cerințe vor fi acoperite de aceste proceduri și definiții de procese:
    - Operarea și administrarea soluției în mod proactiv și eficient,
    - Monitorizarea permanentă a funcționării sistemului cu alertarea anomaliilor – erori sau avertizări legate de funcționalitate,
    - Readucerea sistemului în parametrii normali de operare,
    - Persoane cu nivel mediu de cunoștințe IT și despre produsele soluției să poată aplica procedurile definite.
- Toate componentele soluției vor înregistra principalele evenimente de succes sau de eroare în jurnale specializate care îndeplinesc următoarele cerințe:
    - pot fi securizate pentru a limita accesul la aceste informații,
    - permit consultarea lor directă de către un operator uman,
    - permit interpretarea prin metode programatice – sunt organizate într-un mod consistent și structura este documentată.

Sistemul informatic propus trebuie să pună la dispoziția administratorilor o componentă care va îndeplini atât funcțiile de audit informatic cât și funcțiile de control al accesului la informații.

Soluția de audit și control va îndeplini următoarele cerințe generale:
- Va păstra un istoric de tip log al activității utilizatorilor aplicației.
- Va permite includerea informațiilor despre momentul în care au fost modificate anumite seturi de date de către utilizatori.

5.4. SECURITATEA SISTEMULUI

Cerințe minime:
- Datele transportate prin intermediul platformei să fie transportate în formă criptată.
- Transferul datelor sa fie organizat într-o manieră în care identitatea destinatarului este cunoscută în mod cert înainte de a permite destinatarului să prelucreze datele primite.
- Prelucrarea datelor cu caracter personal de către instituțiile și autoritățile publice, de persoane fizice și de către entitățile de drept privat în procesul de utilizare și furnizare a serviciilor publice să se realizeze cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.

Sistemul va fi proiectat astfel încât să respecte Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE precum și legislația națională în domeniul prelucrării datelor cu caracter personal precum și Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

Sistemul informatic trebuie să fie protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le gestionează.

Designul soluției de securitate trebuie să fie astfel conceput încât să asigure securitatea și confidențialitatea atât a datelor personale ale utilizatorilor, dar și a conținutului și a anumitor funcționalități ale aplicației, astfel încât utilizatorii să acceseze doar acele

secțiuni și conținut care le este permis prin apartenența la un profil sau machete de securitate.

Soluția de securitate va fi astfel configurată încât:
- Să nu permită persoanelor neautorizate modificarea sau alterarea semantică a informațiilor din sistem;
- Să asigure consistența datelor și să permită identificarea sursei datelor inițiale și a persoanelor care au accesat sau au înregistrat aceste date în sistem;
- Să asigure securizarea/protecția datelor vehiculate în sistem pe mai multe niveluri – la nivel de acces în rețea, la nivel de aplicație și la nivel de bază de date.

Prevederile de securitate vor fi implementate la următoarele niveluri ale soluției informatice propuse:

Controlul Accesului Logic
- Nu se permite acces neautentificat la date și informații (mai puțin secțiunea publică). Orice acces în aplicație, atât la nivelul utilizatorilor cât și la nivelul altor module de aplicație, este precedat de identificarea, autentificarea și autorizarea accesului;
- Parolele de acces între modulele aplicației (de ex: la baza de date) sunt stocate criptat în fișierele de configurare;
- Credențialele de acces nu se transmit în clar prin rețea între componentele sistemului;
- Sesiunile de lucru inactive trebuie să expire după o perioadă de timp configurabilă (implicit 10 minute);
- Serviciile și porturile de comunicație folosite vor fi documentate într-o listă a serviciilor utilizate. Serviciile și porturile neutilizate vor fi dezactivate;
- Sistemul informatic și componentele acestuia se vor instala și configura numai pe sisteme care au aplicate ultimele patch-uri de securitate.

Jurnalizare, monitorizare, auditare
Jurnalizarea evenimentelor semnificative legate de controlul accesului
- Înregistrarea în jurnal a autentificărilor cu succes (dată, oră, adresa IP),
- Înregistrarea în jurnal a autentificărilor fără succes (dată, oră, adresa IP),
- Aceste jurnale vor fi disponibile în aplicație pentru vizualizare de către administratorii sistemului.

Testare de securitate
Cu ocazia desfășurării auditului de securitate cibernetică periodic, se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate, în vederea identificării disfuncționalităților și vulnerabilităților și recomandării măsurilor de remediere a acestora.

Aplicația va fi supusă unor verificări riguroase de securitate (auditare de securitate și test de penetrare) pentru a se identifica și elimina orice vulnerabilități înainte de a se utiliza în producție, precum și regulat, la intervale definite de timp. Testele vor respecta cel puțin metodologiile OSSTM (Open Source Security Testing Methodology) sau OWASP (Open Web Applications Security Project). Raportul final de testare de securitate va cuprinde vulnerabilitățile existente în cadrul sistemului și componentelor acestuia și va fi structurat astfel:
- Sumar Executiv;
- Obiectivele și scopul evaluării;

- Prezentare succintă a metodologiei utilizate;
- Descrierea contextului în care s-a desfășurat evaluarea;
- Lista testelor de securitate efectuate.

Prezentarea individuală a vulnerabilităților descoperite după cum urmează:
- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnică;
- Analiza severității și probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere;
- Alte detalii și recomandări.

Scanarea de vulnerabilități informatice se va realiza prin utilizarea de aplicații dedicate și actualizate la momentul realizării scanărilor. În acest sens se vor utiliza aplicații care să conțină baze de date de vulnerabilități la nivel de rețea, sisteme de operare, aplicații/servicii, care, pe de-o parte, trebuie să permită auditarea activităților realizate astfel încât să poată fi demonstrată efectuarea acestor activități și, pe de altă parte, să conțină baze de date actualizate cu exploit-uri (coduri care demonstrează că o vulnerabilitate poate fi exploatată însă fără ca sistemul să fie propriu-zis compromis).

5.5. CONFIDENȚIALITATEA DATELOR

Asigurarea confidențialității este o activitate de bază pentru furnizarea serviciilor publice.
În cadrul proiectului se vor respecta următoarele principii:
- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- 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, trebuie să asigure respectarea de către operatori a 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.

5.6. ARHITECTURA TEHNICĂ

Arhitectura sistemului va fi constituită din soluții redundante, cu asigurarea disponibilității și balansarea încărcării (cluster HA) pentru componentele funcționale critice ale sistemului conform tabelului de mai jos.

Pentru asigurarea funcționării în bune condiții a performanței sistemului vor fi asigurate următoarele medii:

a) **Mediul de producție** - asigură funcționarea în producție a sistemului și reprezintă mediul care va fi utilizat în mod direct de către beneficiar pentru schimbul de informații electronice și furnizarea serviciilor electronice expuse către cetățeni;
b) **Mediul de dezvoltare** și **testare** – asigură mediul pe care vor fi dezvoltate și apoi testate - într-un mod integrat, înainte ca acestea să fie trecute în producție - toate componentele sistemului.
c) **Mediul de disaster-recovery** - va fi folosit pentru restabilirea funcționării sistemului în urma unui dezastru; va fi plasat în cadrul componentei de Cloud Dedicat a Cloud-ului Privat Guvernamental și va avea rolul de a minimiza impactul nefuncționării centrului de date de producție și de a asigura continuitatea operațiunilor.

Mediul de producție și mediul de testare și dezvoltare vor avea, din punct de vedere al numărului de noduri, respectiv al modalității de asigurare a disponibilității și scalabilității sistemului, aceeași arhitectură tehnică, diferențe existând doar la nivelul dimensionării acestor medii.
Mediul de producție va fi dimensionat fără limitarea din punct de vedere al licențierii pe infrastructura hardware minimă solicitată; în cazul soluțiilor cu altă metrică sau modalitate de licențiere, infrastructura software va trebui sa asigure **un minim de 2 milioane de utilizatori distincți.**

Mediul de dezvoltare și testare va fi dimensionat pentru asigurarea unui număr minim de 50 de utilizatori.

Mediul de disaster-recovery va fi dimensionat pentru a permite restaurarea rapidă a funcționării sistemului și pentru funcționarea acestuia pentru o perioadă scurtă de timp, până la repunerea în funcțiune a mediului de producție.

Ținând cont atât de sensibilitatea datelor și de nivelul de securitate solicitat în cadrul proiectului, cât și de asigurarea de către producători a suportului tehnic pentru toate componentele funcționale, de securitate și suport ale platformei, furnizorul este solicitat să ofere versiunea comercială (COTS) pentru tot software-ul standard.
Solutiile COTS vor fi licentiate în mod “Perpetual” sau de tip subscripție valabilă pe toata perioadă de garanție și să funcționeze pe arhitectură de tip “on-premise”.

Pentru a reduce complexitatea arhitecturii, precum și costurile administrative și operaționale, platforma de aplicații propusă trebuie să fie pe deplin integrată la nivelul componentelor de management a fluxurilor și proceselor de emitere, aplicații software personalizate pentru acest sistem.

Sistemul informatic va fi proiectat astfel încât să funcționeze în regim de înaltă performanță și disponibilitate și va fi structurat pe trei niveluri, conform celor mai bune practici în domeniu: stocarea datelor, prelucrare și prezentare.

5.6.1. Dimensionarea componentelor funcționale și a celor de suport ale mediului de producție

Dimensionarea componentelor funcționale și a celor de suport ale mediului de producție va trebui să asigure minimul de resurse de procesare după cum urmează:

Nr. crt.	Componenta	Număr minim de noduri Mediu de producție	Disponibilitate minimă	Număr core-uri minime /nod
1.	Componenta portal	2	HA	16
2.	Componenta de management documente	2	HA	32
3.	Componenta de gestiune și analiza a datelor	2	HA	64
4.	Componenta de tip BPM	2	HA	32
5.	Componenta de interoperabilitate	2	HA	16
6.	Componenta de raportare avansata	1		32
7.	Componenta pentru administrarea identității utilizatorilor	2	HA	64
8.	Componenta de securizare a accesului privilegiat	2	HA	8
9.	Componentă de monitorizare a performanței aplicațiilor	1		24
10.	Componenta de optimizare a resurselor	1		16
11.	Componenta de tip SIEM	1		16
12.	Componenta de integrare și pregătire a datelor tip ETL	2	HA	8
13.	Componenta de mascare a datelor	1		8
14.	Service desk	1		16
15.	Backup	1		16
16.	Monitorizare infrastructură	1		16
17.	Componenta de instruire securitate	1		8

5.7. COMPONENTA DE INFRASTRUCTURĂ HARDWARE

5.7.1. Componentele hardware și de comunicații

Cerințele minime pentru echipamentele hardware și de comunicații sunt:

Nr.	Descriere	Cantitate/bucăți
1)	Platforma de interconectare – Switch Data Center	2
2)	Sistem de calcul modular	1

Nr.	Descriere	Cantitate/bucăți
3)	Platforma unificată de securitate	2
4)	Platforma de balansare a traficului de aplicație	2
5)	Rack echipat (inclusiv UPS rack-abil)	3
6)	Scannere de mare viteză	330

Platforma de interconectare – Switch Data Center

Se vor livra 2 echipamente de tip Switch Data Center cu rol de interconectare a tuturor componentelor ofertate (sisteme si platforme) din cadrul proiectului în reteaua din centrul de date de producție. Fiecare switch va trebui să respecte următoarele specificații:

Cerințe tehnice generale	- Echipamentul va avea caracteristicile unui switch destinat mediului de centru de date, care să asigure simultan următoarele funcționalități:
	  - Switch Ethernet Layer 2;
	  - Switch Ethernet Layer 3;
	- Interfețe fizice disponibile:
	  - Minim 6 40G/100G Ethernet (cu conector QSFP28)
	  - Minim 48 10G/25G Ethernet (cu conector SFP+) care să suporte următoarele tipuri de transceivere:
	  ▪ 10GBASE-SR
	  ▪ 10GBASE-LR
	  ▪ 10GBASE-ER
	  ▪ 25GBASE-SR
	  ▪ 1000Base-T
	- Șasiu instalabil în rack de 19” cu kit de rack-are inclus;
	- Înălțime maximă 1RU, per switch

Conectică instalată (per switch)	- Douăsprezece (12) porturi de tip 100G Ethernet echipate cu cabluri pasive de tip QSFP-QSFP pentru interconectarea echipamentelor livrate; - Minim 1 interfață 100Base-TX/1000Base-T pentru management „out of band”; - Minim 1 port consolă serială; - Minim 1 port USB;
Performanțe (per switch)	- Comutarea la nivel 2: minim 3.5 Tbps și minim 1.2 Bpps; - Minim 3900 de ID-uri pentru VLAN-uri per switch; - Procesor de control multi-core.
Funcționalități minimale de nivel 2 instalate	- Încapsulare IEEE 802.1Q; - Rapid Per-VLAN Spanning Tree Plus sau echivalent; - Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instanțe; - Spanning Tree PortFast, Root Guard și Bridge Assurance sau echivalent; - MC-LAG/Virtual Port Channel sau o tehnologie echivalentă care să permită crearea unui “link-aggregation group” între

	două switch-uri pe de o parte și un alt echipament de tip client (server, switch, router, etc) de partea cealaltă; - Link Aggregation Control Protocol (LACP): IEEE 802.3ad; - Posibilitatea balansării legăturilor din Port Channel utilizând informații de nivel 2, 3 și 4; - Mecanisme de control al inundării rețelei cu trafic unicast, multicast și broadcast; - Private VLAN, inclusiv pe porturile de tip trunk 802.1Q; - LLDP (IEEE 802.3ab) - protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1Q-în-Q, IEEE 802.3an; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames
Funcționalități minimale de nivel 3 instalate	- Suport pentru următoarele protocoale Layer 3: - Open Shortest Path First (OSPF) versiunile 2 și 3; - Border Gateway Protocol (BGP); - RIP v2 - Multicast PIM SM, SSM și MSDP - Posibilitatea de a filtra accesul pe interfețe după informații despre adresa IP sursă sau destinație și în același timp și portul TCP/UDP sursă sau destinație
Funcționalități minimale de QoS	- Layer 2 IEEE 802.1p (CoS); - Configurare QoS per port; - Minim 8 cozi hardware de servire per port; - Clasificarea traficului bazată pe liste de control al accesului
Funcționalități de înaltă disponibilitate	- Surse de alimentare, ventilatoare și module de expansiune de tip “hot-swappable”; - Surse de alimentare redundante tip “1:1”; - Ventilatoare redundante tip “N:1”
Funcționalități de management	- Suport pentru SPAN și Encapsulated Routed SPAN - Suport pentru netflow/sflow sau echivalent - Suport pentru revenirea la o configurație anterioară - Suport pentru standardul AAA, Tacacs+ și Radius - Suport pentru interfață XML (Netconf) - Suport pentru monitorizarea utilizării bufferelor interne - Suport pentru protocolul SSHv2 și SCP
Parametri de alimentare (per switch)	- 2 (două) surse AC integrate, configurabile în mod redundant ce pot fi înlocuite în timpul funcționării echipamentului, cu certificare 80 Plus Platinum sal echivalent - Frecvența de funcționare: 50-60 Hz

Sistem de calcul modular

Sistem hiperconvergent - Infrastructura Hiperconvergentă reprezintă un sistem de tip hiperconvergent, care reunește funcționalitățile de stocare și procesare sub umbrela unui sistem de virtualizare. Astfel, se pot identifica cel puțin următoarele componente ale unui sistem de tip hiperconvergent:

- Noduri de stocare/procesare ce includ resurse ca: Procesoare, Memorie și Drive-uri pentru stocare (Noduri Hiperconvergente)
- Sistem de fișiere distribuit ce are ca rol prezentarea spațiului de stocare din cadrul tuturor nodurilor de stocare/procesare ca un tot unitar către sistemul de virtualizare

- Sistem de virtualizare (hypervizor) cu rol de virtualizare a resurselor hardware în vederea creării de mașini virtuale
- Echipamente de interconectare, atât intre nodurile sistemului, cât și cu celelalte elemente din infrastructura Beneficiarului.

Arhitectura sistemului de tip Hiperconvergent necesar a se implementa în cadrul acestui proiect va include noduri de stocare/procesare de tip Noduri Hiperconvergente, împreună cu celelalte componente necesare pentru operaționalizarea sistemelor în arhitectura hiperconvergentă și va respecta următoarele cerințe generale:

- să asigure un grad ridicat de performanță, fiabilitate și flexibilitate,
- să fie proiectată pentru rularea de aplicații critice de tip "enterprise level",
- să asigure scalabilitatea facilă a sistemului în cazul unor nevoi ulterioare de creștere a resurselor de calcul, interconectare precum și a resurselor de stocare.

Produsele hardware și software trebuie să constituie o soluție integrată, producătorul soluției urmând să asigure un punct de contact unic pentru suportul tehnic pe întreaga durată a contractului. Produsul se va livra împreună cu toate licențele necesare funcționării sistemului Hiperconvergent. Toate serverele trebuie să fie de tip hiperconvergent, iar discurile locale (interne) ale tuturor serverelor trebuie să constituie un cluster prezentat ca un grup unitar și distribuit de resurse disponibile pentru toate nodurile controlate de hipervizor.

Soluția ofertată se va compune dintr-un sistem de înaltă performanță de tip cluster HCI All-Flash compus din doua echipamente de interconectare dedicate, solutie software hiperconvergenta si noduri hiperconvergente recomandate de producatorul solutiei software propuse.

În vederea minimizării activităților operaționale și a numărului de probleme tehnice ce pot apărea în utilizarea/administrarea infrastructurii, se vor respecta următoarele cerințe:

Soluția ofertată trebuie să facă posibilă utilizarea discurilor din servere pentru prezentarea unui sistem de fișiere comun mașinilor gazdă din cluster, sistem ce trebuie să ofere performanțe și disponibilitate de tip Enterprise după cum urmează:

- Trebuie să permită repornirea automată a mașinilor virtuale în cazul defectării unui sistem gazdă din cluster pe celelalte sisteme disponibile;
- Trebuie să asigure protecția continuă a mașinilor virtuale contra defectărilor sistemelor gazdă;
- Trebuie să ofere migrarea în funcționare a mașinilor virtuale;
- Infrastructura trebuie să asigure o scalabilitate elastică și fără întrerupere, fie prin adăugarea de discuri pe sistemele gazdă din cluster, fie prin adăugarea de noi sisteme gazdă cu capacitate adițională de stocare în cluster;
- Disponibilitatea și redundanța datelor va fi asigurată prin replicarea datelor pe mai multe noduri ale sistemului sau prin alte mecanisme echivalente. Sistemul va permite configurarea nivelului de toleranță a clusterului la defecte și implicit numărul de replici ale datelor care vor fi realizate în cadrul sistemului;
- Sistemul trebuie sa asigure mecanisme de protecție a datelor la scriere, astfel confirmarea scrierii unui bloc de date va fi transmisă către aplicație numai după ce datele vor fi replicate pe unul sau mai multe discuri SSD aflate pe noduri diferite ale clusterului;
- Infrastructura trebuie să asigure un management simplificat, integrat cu sistemul de management al mediului virtual;

- Soluția trebuie să permită, în mod eficient, realizarea de cel puțin până la 32 de snapshot-uri și/ sau clone ale unei mașini virtuale;
- Pentru optimizarea spațiului ocupat pe disc și pentru eficientizarea operațiunilor de tip snapshot, platforma va putea realiza snapshot-uri bazate pe metadate de tipul zero-copy. Sistemul va permite actualizarea rapidă a snapshot-urilor (utilizând snapshot-uri de tip zero-copy bazate pe metadate - dacă apar modificări de date într-un snapshot aceste modificări sunt scrise într-o locație nouă, fără a fi nevoie de operațiuni de tip citit-modificat-scris). Sistemul va permite, de asemenea, ștergerea rapidă a snapshoturilor. Platforma va putea permite realizarea de snapshot-uri specifice la nivel de fișier;
- Sistemul va permite realizarea de clone ale volumelor de date prezentate către noduri. Prin utilizarea de mecanisme similare cu cele folosite în realizarea de snapshot-uri (zero-copy, clone bazate pe metadate) platforma va permite crearea/ștergerea extrem de rapidă a unui număr mare de clone. Copierea datelor la realizarea de clone va avea loc doar pentru operațiunile de scriere de date noi pe disc;
- Trebuie să permită prezentarea de volume de stocare tip bloc folosind protocolul iSCSI către alte sisteme (Ex: sisteme nevirtualizate din cadrul proiectului pe care rulează bazele de date);
- Trebuie să asigure prezentarea de volume de stocare de tip file și de tip object, de o dimensiune de cel puțin 1TB în configurația ofertată;
- Soluția trebuie să permită resincronizări adaptive pentru a nu afecta performanța aplicațiilor în cazul apariției unor defecte hardware ce afectează conformitatea cu politica de stocare;
- Caracteristicile tehnice trebuie să asigure deduplicarea și compresia datelor la nivelul întregului cluster, asigurând astfel reducerea spațiului ocupat;
- Soluția va permite rebalansarea clusterului și ajustarea distribuției datelor pe nodurile sistemului la adăugarea de noi noduri în cluster sau la scoaterea de noduri în mod automat, online și fără a afecta operațiunile și funcționarea normală a clusterului. Rebalansarea se va realiza atât la nivelul de cache cât și la nivelul cu drive-uri SSD. În momentul în care un nod se defectează, acesta trebuie scos automat din cluster și controller-ul software va reconstrui și distribui copii ale datelor de pe nodul căzut pe toate nodurile disponibile ale sistemului.
- În vederea unor extensii viitoare precum și pentru asigurarea mecanismelor de redundanță între centrele de date, sistemul trebuie să ofere mecanisme integrate de replicare asincronă la distanță la nivel de fișier - mașină virtuală între două sisteme similare pentru un număr nelimitat de mașini virtuale, fără a fi nevoie de licențe suplimentare la nivel de Hypervisor sau la nivelul sistemului integrat.
- Soluția va permite utilizarea unei părți a memoriei RAM instalate în nodurile clusterului pentru definirea unui nivel de stocare cache ce va permite accelerarea citirilor și scrierilor la nivelul sistemului;
- Sistemul va utiliza un mecanism ce va permite plasarea în mod dinamic a datelor pe diferitele niveluri de stocare de pe nodurile sistemului pentru optimizarea performanței și disponibilității sistemului și respectiv rebalansarea clusterului și ajustarea distribuției datelor la adăugarea de noi noduri în cluster.
- Sistemul va oferi integrări prin intermediul API-urilor cu sistemul de virtualizare;
- Soluția trebuie să ofere posibilitatea utilizării a minim 2 tehnologii de virtualizare (Hypervisor) diferite, oferind astfel flexibilitate din punct de vedere virtualizare;
- Clusterul trebuie să dețină capabilitatea de a crește liniar prin adăugarea de noduri noi până la cel puțin 32 noduri într-un singur cluster cu același storage partajat (un singur namespace), pentru a permite creșterea puterii de procesare

a sistemului, a capacității de stocare a datelor și a performanței de citire/scriere pe sistemul de stocare;

- Soluția va permite creșterea puterii de procesare a cluster-ului fără fi nevoie de creșterea în același timp a nivelului de stocare;
- Pentru monitorizarea performanței soluției se vor putea identifica resursele de procesare și memorie utilizate de către componenta de stocare.
- Soluția propusă va avea la bază un nivel de virtualizare a resurselor fizice pentru rularea resurselor în mașini virtuale (hypervisor).
- Soluția propusă pentru nivelul de virtualizare trebuie:
  - Să permită conectarea peste rețea printr-un concentrator de porturi seriale la consola serială a oricărei mașini virtuale (ex. Linux);
  - Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalități disponibile în noile versiuni de procesoare;
  - Să ofere posibilitatea creării unor profile pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri să se facă foarte rapid, respectând o configurație prestabilită și eliminând erorile de configurare și oferind totodată posibilitatea modificării parametrilor configurației;
  - Să dispună de capacități de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie repornite automat pe celelalte host-uri din cluster;
  - Să dispună de capacități de failover astfel încât, în cazul defectării parțiale a unui host, mașinile virtuale care rulau pe acel host să fie migrate automat pe celelalte host-uri din cluster;
  - Să ofere posibilitatea de integrare cu soluții 3rd party care să asigure funcții de failover la nivel de aplicații, astfel încât, în cazul defectării aplicațiilor instalate în interiorul unei mașini virtuale (ex. SQL server, IIS), respectivele aplicații să fie repornite în mod automat pe baza unui politici predefinite, fie local, fie pe un alt host din cluster.
  - Să ofere posibilitatea mutării simultane a mașinilor în funcționare de pe un host pe altul/altele fără afectarea funcționării acestora pentru a se putea executa activități de mentenanță pe host-ul respectiv;
  - Să ofere balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vederea asigurării resurselor optime pentru funcționare.
  - Să asigure rate mari de consolidare a mașinilor virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memorieri (ex „ Memory Ballooning”, „Swap to disk”) pentru reducerea costurilor asociate infrastructurii fizice (ex. Număr host-uri, număr porturi de rețea/switch-uri) și de licențiere precum și pentru asigurarea continuității în funcționare a aplicațiilor în cazul unor întreruperi parțiale neplanificate;
  - Sisteme de operare suportate pe mașinile virtuale: Windows, Linux;
  - Sistemul de fișiere va asigura posibilitatea migrării în timp real (fără întreruperea funcționarii) unei mașini virtuale de pe un host pe altul, de pe o capacitate de stocare pe alta;
  - Să ofere switch virtual distribuit care să permită configurarea centralizată a rețelei, eliminând greșelile de configurare;
  - Aplicația și sistemul de fișiere asociat trebuie să permită adăugarea de procesoare virtuale, memorie RAM, interfețe de rețea și disk-uri la mașinile virtuale fără a necesita oprirea acestora (dependenta de guest OS);
  - Aplicația de virtualizare trebuie să permită crearea de grupuri de mașini virtuale care să împartă aceleași resurse puse la dispoziție în comun (memorie și timpi de procesor);

- Software-ul instalat pe host trebuie să poată crea echipamente de rețea virtuale (switch-uri) la care să se conecteze mașinile virtuale și interfețele de rețea fizice de pe host.
- Să permită managementul salvării contextuale (snap-shot) ale mașinilor virtuale fără afectarea stării de funcționare, astfel încât o mașină virtuală se va putea restaura din orice salvare anterioară.
- Să ofere interfețe de programare pentru aplicații (API) care să permită producătorilor 3rd party de aplicații de securitate să ofere integrarea și optimizarea aplicațiilor lor cu mediul virtual pentru performanțe ridicate (exemplu: scanare anti-virus sau anti-malware);
- Să ofere posibilitatea de criptare a tuturor fișierelor asociate unei mașini virtuale, indiferent de sistemul de operare din mașina virtuală sau de tipul de stocare folosită.
- Sa asigure posibilitatea administrării centralizate dintr-o interfață unică pentru toate nodurile din Sistemul Hiperconvergent.

Sistemul Hiperconvergent All-Flash va include un număr de cel puțin **10 noduri de tip Nod Hiperconvergent**, ale căror caracteristici vor fi descrise la subcapitolul Noduri Hipeconvergente.
Sistemul de calcul modular va fi unul de tip cluster HCI All-Flash, ce va deservi cele două zone (zona de aplicații și zona componentei de gestiune și analiza a datelor), după cum urmează:
- Zona de aplicații va rula pe cel puțin 8 noduri de tip hiperconvergent, noduri în configurație hardware și software identică, configurate în arhitectură de cluster de tip NSPOF (no single point of failure),
- Zona componentei de gestiune și analiza a datelor va rula pe cel puțin 2 noduri de tip hiperconvergent, noduri în configurație hardware și software identică, configurate în arhitectură de cluster de tip NSPOF (no single point of failure).

Interconectare

Sistemul de calcul modular va include și două echipamente dedicate de interconectare a nodurilor hiperconvergente, echipamente de nivel înalt de performanță, echipamente ce sunt conectate redundant cu cele două switchuri ce compun platforma de interconectare – Switch Data Center.
Echipamente de interconectare a nodurilor sistemului - 2 Buc
Toate accesoriile necesare instalarii si bunei functionari a sistemului: cabluri, patch-uri fibra, module pentru switch-uri, elemente de fixare cabluri si echipamente sunt in responsabilitea furnizorului. Echipamentele trebuie livrate cu toate accesoriile necesare interconectării, instalării și punerii în funcțiune asigurând compatibilitatea și integrarea cu nodurile hiperconvergente, fără costuri suplimentare pentru beneficiar.
Pentru conectarea fiecărui nod hiperconvergent pentru zona de aplicatii și respectiv pentru zona componentei de gestiune și analiză a datelor se vor include cel puțin două cabluri optice active de 100GbE QSFP28.
Pentru fiecare nod hiperconvergent pentru zona de aplicatii și respectiv pentru zona componentei de gestiune și analiză a datelor se vor include cel puțin două cabluri de tip breakout 100Gb QSFP28 la 4 x 25Gb SFP28.
Fiecare echipament de interconectare a nodurilor sistemului va respecta următoarele cerințe tehnice minimale:

Nr	Descriere cerință	Cerința tehnică minimală
1	Format	Rackabil cu kit de rack-are inclus; Înălțime maximă 1RU, per switch
2	Interfețe fizice disponibile	• Minim 32 porturi QSFP56 incluse; • Viteză suportată per interfață fizică: cel puțin 40/100/100GbE; • Port de management 1GbE dedicat inclus/Port serial inclus
3	Funcționalități	• Echipamentul va avea caracteristicile unui switch destinat mediului de centru de date, care să asigure simultan următoarele funcționalități: o Switch Ethernet Layer 2; o Switch Ethernet Layer 3: • Rapid Per-VLAN Spanning Tree Plus sau echivalent; • Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s); • Link Aggregation Control Protocol (LACP) IEEE 802.3ad; • Multi chassis LAG sau echivalent ; • Suport inclus pentru protocolul VXLAN
4	Performante	• Capacitate switching: cel puțin 6.2Tb/s full duplex; • Throughput: cel puțin 8 Bpps full duplex; • Latență maximă: 500 ns
5	Capabilități hardware	Procesor: minim 1 procesor x86 quad core inclus; Memorie RAM: minim 8GB DDR4 RAM memorie inclusă; Capacitate de stocare internă: minim 32GB SSD capacitate de stocare internă inclusă
6	Conectarea în LAN	Se va face prin cel puțin 2 interfețe fizice la viteză fiecare de cel puțin 100GbE; Funcționalitate inclusă: - failover automat și mod de funcționare de tip „active – active”
7	Surse de alimentare	Surse de alimentare redundante incluse, de tip „hot-swap”, pentru utilizare în rețeaua de alimentare din România; Sursele se livrează cu cablu de alimentare tip C13/C14
8	Sistem de ventilație/ răcire	Ventilatoare redundante incluse, de tip „hot-swap”
	Sistem de operare	Sistem de operare instalat și licențiat inclus

Noduri hiperconvergente

Compatibilitate Hardware: Nodurile hiperconvergente ofertate trebuie să fie certificate sau listate pe Lista de Compatibilitate Hardware (HCL) publicată oficial de producătorul platformei software hiperconvergente. Ofertantul va furniza dovada acestei compatibilități (link-uri către HCL, capturi de ecran).

Livrare și Instalare: Nodul se va livra cu platforma software hiperconvergentă ofertată preinstalată, configurată conform bunelor practici ale producătorului software.
Suport Tehnic: Ofertantul va acționa ca punct unic de contact (Single Point of Contact - SPOC) pentru deschiderea și gestionarea tuturor tichetelor de suport, atât pentru componentele hardware, cât și pentru platforma software. Ofertantul trebuie să demonstreze existența unor acorduri de suport colaborativ între producătorul hardware și cel software pentru a garanta diagnosticarea și rezolvarea rapidă a incidentelor, indiferent de componenta cauzatoare (hardware sau software).

Noduri hiperconvergente - zona de aplicații 8buc

Nr	Componenta / Parametru	Cerința tehnică minimală
1	Platforma	Arhitectura: server montabil în rack standard de 19 inch; Tip platformă: multiprocesor; Nr de procesoare acceptate: minim 2;
2	Procesor	Număr de procesoare instalate: minim 2; Tip Intel Xeon minim generația a 4-a cu cel puțin 32 Core (exceptând Hyper Threading) și 60MB cache L3 sau echivalent; Frecvența de lucru: minim 2.2 GHz, exceptând Turbo Boost;
3	Memorie internă	Memorie instalată: minim 1024 GB RAM; Tip memorie: cel puțin DDR5 4800 MT/s
4	Interfețe de rețea	Minim un adaptor de rețea dual port QSFP56 care să asigure conectivitate la cel puțin 100GbE per port; Minim un adaptor de rețea dual port 10/25 GbE.
5	Stocare locală	Cel puțin 2 medii SSD M.2 sau echivalent cu capacitate de cel puțin 240 GB fiecare, cu controller RAID hardware cu suport pentru RAID 1; Cel puțin 4 medii SSD NVMe de tip U.2 sau echivalent cu capacitate de 15.3 TB fiecare, certificate pentru buna funcționare în Sistemul Hiperconvergent ofertat.
6	Accesul la nod	Suport pentru accesul de tip „out of band” prin interfață dedicată de management de capacitate cel puțin de 1GbE ; - Accesarea de la distanță a serverului folosind tastatura și mouse-ul de la o stație client la distanță;
7	Management	Sistem incorporat de monitorizare a sistemului cu modul de management de tip out-of-band cu toate functionalitățile activate și nelimitate în timp. Sistemul va permite: - Vizualizare video de la distanță cu rezoluții grafice de până la 1600x1200 la 75Hz cu până la 23bpp, indiferent de starea serverului ;

Nr	Componenta / Parametru	Cerința tehnică minimală
		- Accesarea de la distanță a serverului folosind tastatura și mouseul de la o stație client la distanță; - Alertare Syslog; - Redirectare consolă serială prin SSH; - Jurnal de înlocuire a componentelor (jurnal istoric de întreținere); - Restrictionarea accesului prin blocarea IP-urilor; - Administrarea cheilor de securitate SED; - Afișarea graficelor în timp real sau pentru date istorice cu privire la consumul de energie și de temperatură ; - Capturare și redare a imaginilor video atunci când sistemul pornește și/sau se blochează ; - Consolă la distanță; - Capabilități pentru maparea unor fișiere tip imagine (ISO) local sau de pe un sistem de la distanță ; - Capabilități de montare a unor fișiere de tip imagine cel puțin prin protocoale HTTPS/SFTP/CIFS și NFS ; - Limitarea puterii; - Vizualizarea datelor despre utilizare - Monitorizarea inventarului hardware pentru modificări neașteptate asupra componentelor prin înregistrarea evenimentului sau blocarea pornirii serverului; - Gestionarea și sincronizarea configurațiilor și a nivelurilor firmware-ului pe mai multe servere; - Sistemul de management trebuie să asigure administrare la distanță și prin interfețe standard în industrie, cel puțin prin: o Web-browser ; o IPMI v2.0; o SNMP v3; o CIM-XML; o REST API

Noduri dedicate componentei de gestiune și analiză a datelor - 2 buc

1 Platforma Arhitectura: server montabil în rack standard de 19 inch
Tip platformă: multiprocesor;
Nr de procesoare acceptate: minim 2;

2 Procesor - Număr de procesoare instalate: minim 2
Tip Intel Xeon minim generația a 4-a din familia Platinum cu cel puțin 32 Core (exceptând Hyper Threading) și 60MB cache L3 sau echivalent;
Frecvența de lucru: minim 2.8 GHz, exceptând Turbo Boost;

3 Memorie interna - Memorie instalată: minim 1024 GB RAM;

Tip memorie: cel puțin DDR5 4800 MT/s.

4 Interfețe de rețea - Minim un adaptor de rețea dual port QSFP56 care să asigure conectivitate la cel puțin 100GbE per port;
Minim un adaptor de rețea dual port 10/25 GbE.

5 Stocare locală - Cel puțin 2 medii SSD M.2 sau echivalent cu capacitate de cel puțin 960 GB fiecare, cu controller RAID hardware cu suport pentru RAID 1;
Cel puțin 4 medii SSD NVMe de tip U.2 sau echivalent cu capacitate de 15.3 TB fiecare, certificate pentru buna funcționare în Sistemul Hiperconvergent ofertat.

6 Accesul la nod - Suport pentru accesul de tip „out of band" prin interfață dedicată de management de capacitate cel puțin de 1GbE;
Accesarea de la distanță a serverului folosind tastatura și mouse-ul de la o stație client la distanță;

7 Management Sistem - incorporat de monitorizare a sistemului cu modul de management de tip out-of-band cu toate functionalitățile activate și nelimitate în timp.

Sistemul va permite:

- Vizualizare video de la distanță cu rezoluții grafice de până la 1600x1200 la 75Hz cu până la 23bpp, indiferent de starea serverului ;
- Accesarea de la distanță a serverului folosind tastatura și mouse-ul de la o stație client la distanță;
- Alertare Syslog;
- Redirectare consolă serială prin SSH;
- Jurnal de înlocuire a componentelor (jurnal istoric de întreținere);
- Restricționarea accesului prin blocarea IP-urilor;
- Administrarea cheilor de securitate SED;
- Afișarea graficelor în timp real sau pentru date istorice cu privire la consumul de energie și de temperatură ;
- Capturare și redare a imaginilor video atunci când sistemul pornește și/sau se blochează ;
- Consolă la distanță;
- Capabilități pentru maparea unor fișiere tip imagine (ISO) local sau de pe un sistem de la distanță ;
- Capabilități de montare a unor fișiere de tip imagine cel puțin prin protocoale HTTPS/SFTP/CIFS și NFS ;
- Limitarea puterii;
- Vizualizarea datelor despre utilizare
- Monitorizarea inventarului hardware pentru modificări neașteptate asupra componentelor prin înregistrarea evenimentului sau blocarea pornirii serverului;
- Gestionarea și sincronizarea configurațiilor și a nivelurilor firmware-ului pe mai multe servere;
- Sistemul de management trebuie să asigure administrare la distanță și prin interfețe standard în industrie, cel puțin prin:
    - Web-browser ;
    - IPMI v2.0;
    - SNMP v3;
    - CIM-XML;
    - REST API.

Platformă software de management centralizat

Sistemul va fi livrat cu o platformă software de management centralizat la nivelul infrastructurii de noduri de procesare, care va include funcționalități de descoperire și

inventariere a elementelor administrate, monitorizarea acestora, update-uri de firmware, verificări de complianță la nivel de firmware elemente administrate, managementul configurațiilor echipamentelor din inventar, instalarea hypervizorul-ui direct pe servere din inventar din consola de administrare.
Soluția va permite afișarea în mod vizual a elementelor din inventar.
Soluția va permite inventarierea tuturor nodurilor hiperconvergente ofertate sub forma de tabele de bord (dashboard).
Soluția va permite managementul și administrarea elementelor de inventar fără instalarea de agenți (agentless). Conexiunea între platforma de management și echipamentele aflate în administrare trebuie să fie una securizată, cel puțin prin protocol SSL.
Managementul echipamentelor trebuie să fie unul unitar și integrat la nivelul soluției care va permite definirea și aplicarea de profile asociate echipamentelor din inventar.
La nivelul soluției de management trebuie să fie diponibile informații granulare despre nodurile hiperconvergente aflate în administrare (cel puțin pentru configuratie procesor, memorie, adaptoare de rețea), versiunea de firmware ce rulează pe acestea și soluția software hiperconvergentă.
Soluția de management trebuie să dispună de funcționalități de integrare în platforme de orchestrare prin intermediul REST API. În cadrul platformei se va regăsi posibilitatea folosirii unei interfețe de tip PowerShell care va permite rulea de script-uri.
De asemenea, va permite conectori de integrare cu soluții de management al platformelor de virtualizare
Soluția propusă trebuie să dispună de mecanisme de autentificare ce permit conectarea la un server extern de tip LDAP/Active Directory.
Soluția trebuie să dispună de metode de vizualizare a consumului de energie a nodurilor hiperconvergente aflate în inventar.
Pentru instalarea și funcționarea platformei software de management centralizat se va include un server cu rolul de **Nod dedicat pentru management** cu următoarele caracteristici tehnice minimale:

- Procesor: minim un procesor instalat, Intel Xeon Gold sau echivalent cu minim 32 Core / 64Threads, frecvență de bază cel puțin 2.1Ghz, minim 60MB Cache, suport pentru memorie de tip DDR5 4800;
- Memorie RAM: minim 96 GB DDR5 4800 RDIMM;
- Stocare:
    - Controller RAID cu minim 4 GB cache;
    - Cel puțin două medii de stocare de tip SSD cu capacitate de cel puțin 3.8TB și performanță de scriere de tip 3 DWPD;
- Stocare adițională: cel puțin două medii de stocare de tip SSD M.2 sau echivalent cu capacitate minimă de 240 GB atașate la un controler RAID hardware;
- Adaptoare de rețea instalate: cel puțin 4 interfețe 10/25/50 GbE SFP+ prin unul sau mai multe adaptoare de de rețea;
- modul de securitate de tip TPM 2.0 instalat;
- surse de alimentare redundante, pentru funcționare în rețeaua de alimentare cu energie electrică din România, prevăzute cu cabluri de alimentare cu conector C13/C14.
- Licență Windows Server Standard 2025 sau echivalent.

Platforma unificata de securitate

Soluția va include un complet format din cel puțin două echipamente care să funcționeze într-un cluster care să ofere o disponibilitate înaltă a serviciilor de securitate de tip next generation firewall. Platforma trebuie să îndeplinească cel puțin următoarele cerințe funcționale specifice:

- Minim 4 porturi de 100 GE QSFP28/ 40 GE QSFP+
- Minim 24 porturi 25 GE SFP28/ 10 GE SFP+ / GE SFP
- Minim 2 porturi de Management RJ45
- Storage intern: minim 2 TB SSD
- Surse AC redundante de tip Hot swappable
- Performanța firewall pachete: 240 Gbps
- Performanța trafic firewall (pachete per secunda): 225 Mpps
- Performanța IPS: 44 Gbps
- Performanța Threat Protection: 23 Gbps
- Performanța SSL Inspection: 30 Gbps
- Performanța control de aplicatii: 86 Gbps
- Sesiuni concurente: 50.000.000
- Conexiuni noi pe secundă: 460.000
- Politici firewall: 200.000
- Procesare trafic de tip IPSec VPN: 140 Gbps
- Procesare trafic de tip SSL VPN: 11 Gbps;
- Tunele IPSec VPN (site-to-site): 100.000
- Tunele IPSEC VPN (gateway – gateway): 40.000
- Configurații HA : activ/activ, activ/pasiv.
- Suport pentru protocoale de rutare dinamice
- Suport pentru inspecția traficului bazat pe cel puțin următoarele module de securitate: IPS, Antivirus, Filtrare Web, Control Aplicații etc.
- Suport VPN de tip site-to-site și Remote Access
- Suport Traffic Shaping
- Suport SD-WAN
- Update-uri de securitate automate și în timp real
- Platforma hardware, sistemul de operare și licențele/update-urile de securitate trebuie să fie furnizate de la același producător
- Suport pentru rutare statică și rutare bazată pe sursă
- Protocoale dinamice de routare: OSPF, ISIS, BGP4
- Suport pentru trafic de tip Multicast
- Suport pentru funcționare în mod Virtual Wire
- Suport pentru funcționare în mod explicit web și FTP proxy: FTP, HTTP și HTTPS
- Suport IPsec VPN:
    - Site-to-site
    - Client-to-site (remote access)
- Suport SSL VPN
- Suport pentru VPN de tip Remote Acces bazat pe clientul sistemului de operare OSx
- Suport pentru definirea de mai multe instanțe/partiții virtuale
- Soluția trebuie să permită distribuirea procesării de trafic a instanțelor virtuale într-un cluster de tip HA: Activ-Pasiv.
- Soluția trebuie să permită activarea selectivă a traficului ce se dorește a fi procesat de ASIC-uri.
- Sistemul va fi livrat cu următoarele licențe: IPS, Application Control, Antivirus, Webfiltering, Antispam.

Platforma de balansare a traficului de aplicație

Soluția va include un complet format din cel puțin două echipamente care să funcționeze într-un cluster care să ofere o disponibilitate înaltă a serviciilor de aplicații. Acesta va

oferii servicii transparente de balansare, accelerare și protejare a aplicațiilor. Platforma trebuie să îndeplinească cel puțin următoarele cerințe funcționale specifice:

- Minim 8 interfețe 1Gbps, SFP, din care cel puțin 4 echipate cu conector de cupru;
- Minim 4 interfețe 10Gbps, SFP+, toate echipate cu optice multimode, short distance;
- Stocare internă de cel puțin 500GB;
- Memorie RAM, cel puțin 32GB;
- Sursa de alimentare AC redundantă, cu posibilitatea înlocuirii lor fără întreruperea funcționării;
- Performanța de minim 20Gbps de procesare a traficului la L4/7 per echipament;
- Performanța de minim 10Gbps la compresia traficului în hardware;
- Performanța de minim 12Gbps la criptarea traficului în hardware;
- Performanța de minim 1.100.000 cereri pe secunda la nivel 7;
- Performanța de minim 10000 tranzacții
- Distribuția încărcării de procesare pentru cel puțin protocoalele TCP și UDP;
- Suport pentru folosirea SNAT;
- Distribuția încărcării de procesare pe baza următorilor algoritmi: round robin, ratio, weighted ratio, dynamic ratio, least connections;
- Posibilitatea de monitorizare a serverelor de aplicații folosind mecanisme de verificare pentru protocoalele standard;
- Posibilitatea de configurare a mecanismului de verificare specific fiecărei aplicații;
- Monitorizarea disponibilității atât la nivel de nod, cât și la nivel de serviciu și nivel de aplicație;
- Posibilitatea de translatare atât a adreselor IP, cât și a porturilor pe care rulează serviciile furnizate de serverele de aplicații;
- Posibilitatea de manipulare a distribuției încărcării de procesare pe baza informațiilor din headerele protocoalelor de aplicație folosite;
- Capacitatea de trimite cereri gradual către serverele de aplicații nou adăugate;
- Capacitatea de a folosi o combinație mixtă de adrese virtuale și noduri IPv4 și IPv6;
- Capacitatea de inserție XFF în header HTTP, cu IP originator al clientului;
- Redirectare URL către mai multe servere virtuale în funcție de HTTP response code sau URL pattern;
- Capacitatea de a agrega și refolosi multiple sesiuni client într-o singură sesiune server-side;
- Capabilitate de compresie HTTP pentru reducerea traficului;
- Capabilitate pentru caching multi-store pentru conținut dinamic și static (RFC2616);
- Capabilitate “cookie encryption” pentru prevenirea “cookie session hijacking” și manipularea cookie-urilor;
- Capabilități pentru optimizarea traficului LAN/WAN conform: RFC2582 (optimizare Reno asimetrica), RFC1323 (extensii TCP pentru retele de mare viteza), RFC3042, RFC2018, RFC3168;
- Protecție împotriva atacurilor de tip SQL injection;
- Protecție împotriva atacurilor de tip Web Scraping;
- Protecție împotriva atacurilor de tip Cross Site Scripting;
- Protecție împotriva atacurilor de manipulare a parametrilor HTTP;
- Protecție împotriva atacurilor de tip Cross Site Request Forgery;
- Protecție împotriva atacurilor de tip Brute Force;
- Protecție împotriva atacurilor axate pe XML;

- Protecție împotriva scurgerilor de date sensibile din cadrul aplicației;
- Protecție împotriva modificărilor intenționate de parametrii la aplicații;
- Protecție împotriva atacurilor de tip Cookie Poisoning;
- Protecție împotriva atacurilor de tip Hidden Field Manipulation;
- Protecție împotriva atacurilor de tip Buffer Overflow;
- Protecție împotriva atacurilor de tip Cookie Manipulation;
- Protecție împotriva atacurilor de tip Request Smuggling;
- Protecție împotriva atacurilor de tip Session Hijacking;
- Protecție împotriva atacurilor de tip Broken authentication and session management;
- Ascunderea de către utilizator a erorilor furnizate de aplicații;
- Impunerea unor politici de securitate bazate pe GeoIP;
- Posibilitatea de securizare pentru tranzacțiile de tip web services;
- Furnizarea unui mecanism de rollback pentru politicile de securitate;
- Funcție de auto-învățare a parametrilor din cadrul unei politici de securitate în timp real;
- Furnizarea de politici predefinite pentru diferite aplicații;
- Posibilitatea generării automate a politicilor și mecanismelor de securitate;
- Posibilitatea de asimilare automată a parametrilor unei aplicații;
- Furnizarea de audit și raportare pentru fiecare politică de securitate;
- Posibilitatea de integrare cu soluții de evaluare a vulnerabilităților unor aplicații;
- Posibilitatea definirii centralizate a politicilor de acces pentru diferite resurse protejate de către sistem;
- Permite definirea de politici de acces pentru utilizatorii de la distanță;
- Suport pentru single sign on (SSO) distribuit pe mai multe domenii și resurse;
- Posibilitatea de definire a politicilor de acces folosind o interfață grafică intuitivă;
- Folosirea de ACL-uri dinamice pentru sesiunile autentificate și autorizare;
- Posibilitatea de integrare cu servere AAA de tipul Active Directory, LDAP, RADIUS;
- Posibilitatea de a face caching la credențialele utilizatorilor pentru care se folosește SSO;
- Posibilitatea de definire a politicilor de acces pentru un portal web, o aplicație tunelată sau acces la rețea;
- Posibilitatea definirii a politicii de acces în mod granular;
- Suport pentru certificate digitale pentru utilizatorii platformelor Microsoft Windows;
- Posibilitatea de a exporta și importa politicile de acces;
- Licența pentru minim 500 de utilizatori concurenți autentificați;
- Posibilitatea sincronizării configurațiilor în cluster și intre clustere diferite;
- Sistem de operare pentru management independent de sistemul folosit pentru procesarea traficului;
- Sistem de operare pentru procesarea traficului modular;
- Mecanisme de configurare folosind interfața Web și CLI sau mecanisme API
- Extinderea funcționalităților ADC prin limbaj de scripting capabil să folosească declarații condiționale (if/then) și bucle (for, while);
- Capacitatea de modificare/alterare cerere/răspuns în funcție de: parametri standard HTTP (header, cookie, hostname, URN, etc), username, parametri ai certificatelor X.509;
- Acces la un feed de securitate de tipul IP intelligence, oferit de producător, pe toată perioada garanției și suportului oferit pentru echipamente.

Rack pentru servere, gestionare cabluri, distribuție energie pentru servere și maximizare debit de aer.

Caracteristici tehnice:

Clasa produs	Rack/cadru 19"
Înălțime internă	42 U
Lățime	Maxim 750 mm
Adâncime	Maxim 1200 mm
Informații suplimentare	Uși rabatabile, Uși ventilate cu opțiuni variabile de răcire, Uși și panouri laterale care se pot bloca, Uși spate detașabile, Montare fără unelte, Compatibilitate cu echipament de la diverși producători, Adâncime de montare reglabilă, Panouri laterale detașabile. Accesorii pentru utilizare în zone cu cutremure, dacă sunt oferite de producător.

PDU Metered x2 per rack

- Număr de ieșiri: conform cu echipamentele propuse de ofertant
- Tipuri de conectori: Cuplaj C13 și sau Cuplaj C19, în funcție de tipul echipamentelor ofertate
- Curent (maxim): 16 A.

UPS – rack-abil

UPS de tip Smart, putere de ieșire dimensionată pentru echipamentele ofertate și distribuția echipamentelor în rack propusă de ofertant, tehnologie online cu dublă conversie, undă sinusoidală, Rack maxim 6U, tensiune de ieșire 230V, placă de rețea, kit montare în rack cu șină, acumulatori incluși, hot-swap, bypass intern inclus, conectori ieșire incluși cel puțin 4 x IEC 60320 C19, 6 x IEC 60320 C13, permite și conexiune PDU prin cablu rigid. Temperatura ambientală de funcționare: 0 – 40 grade Celsius. Interval pentru tensiunea de la rețea intrare: 100 - 275V și 173 – 476V. Alimentare de la rețea 230V/400V.

5.7.2. Platformă de virtualizare hiperconvergentă

Cerințe funcționale pentru platforma de virtualizare

- Soluția trebuie implementată pe baza unui sistem care utilizează:
  - software pentru infrastructură hiperconvergentă HCI All-Flash,
  - servere x86 standard, disponibile pe scară largă (noduri) fără utilizarea componentelor hardware specializate (de exemplu, FPGA),
  - dispozitive de stocare locale pentru a crea un sistem de stocare definit de software (Software Defined Storage).
- Nodurile trebuie combinate într-un cluster printr-o rețea Ethernet în configurație redundantă (NSPOF), utilizată pentru toate tipurile de trafic (trafic de management, de date, de stocare), fără a necesita o infrastructură dedicată de tip SAN sau LAN suplimentară pentru traficul serviciului SDS.
- Toate componentele software ale platformei hiperconvergente trebuie să fie preinstalate din fabrică, iar implementarea trebuie efectuată folosind un program de instalare integrat în soluție cu o interfață grafică, fără a fi nevoie de instrumente terțe.

- Componentele software de bază trebuie să includă o platformă de virtualizare și stocare definită de software.
- Instrumentele de management trebuie să fie complet integrate cu sistemul de management al platformei de virtualizare și SDS. Platforma de virtualizare trebuie gestionată dintr-o singură consolă bazată pe web, fără a fi nevoie de instrumente de administrare terțe.
- Platforma de virtualizare trebuie să fie complet redundantă și construită pe principiul NSPOF (no single point of failure). Toate nodurile trebuie să fie interschimbabile. Defectul sau indisponibilitatea oricărui nod din cluster nu trebuie să ducă la întreruperea serviciului sau să afecteze funcționalitatea platformei.
- Platforma de virtualizare trebuie să fie una parametrizabilă din punctul de vedere al nivelului de toleranță la defect în cluster, trebuie să permită toleranța la defect pentru un nod hiperconvergent precum și pentru două noduri hiperconvergente din cluster.
- Clusterele trebuie să accepte capacități de autoverificare pentru a respecta standardele STIG/DISA.
- Platforma de virtualizare trebuie să include funcționalitatea de auto reparare. În cazul unei defecțiuni a nodului sau a discului, sistemul trebuie să restabilească automat numărul necesar de copii de date redundante în conformitate cu politicile de stocare configurate.
- Hipervizorul trebuie să accepte migrarea în timp real a mașinilor virtuale între nodurile de calcul din același cluster și între clustere.
- În cazul unei defecțiuni a nodului, mașinile virtuale trebuie să repornească automat pe alte noduri din cluster.
- Platforma de virtualizare trebuie să accepte scalarea orizontală prin adăugarea de noi noduri și scalarea verticală prin actualizarea nodurilor existente cu componente hardware suplimentare. Scalarea nu trebuie să necesite modificări ale arhitecturii sistemului și trebuie efectuată fără întreruperi ale serviciului sau întreruperi ale sistemului.
- Actualizările tuturor componentelor hardware și software din trebuie efectuate fără întreruperea serviciului sau impact asupra funcționalității sistemului.
- Actualizările (inclusiv gestionarea ciclului de viață al software-ului de sistem, driverelor, firmware-ului și microcodului componentelor hardware), monitorizarea componentelor hardware și software și scalarea trebuie efectuate printr-o singură consolă de gestionare în browser web standard.
- Toate clusterele, inclusiv cele implementate în locații diferite, trebuie gestionate dintr-o singură consolă în browser web standard.
- Sistemul trebuie să accepte backup-ul încorporat al tuturor datelor sistemului de management prin protocol S3 și recuperarea din aceasta, fără a necesita instrumente terțe.
- Platforma de virtualizare trebuie să accepte noduri hiperconvergente cu diferite caracteristici tehnice și configurații hardware, inclusiv diferite generații de servere și componente fizice.
- Producatorul trebuie să publice în mod regulat recomandări de tipul cele mai bune practici pentru buna funcționare a soluției hiperconvergente, inclusiv versiunile recomandate ale software-ului de sistem, driverelor și firmware-ului pentru hardware.
- Pachetul de livrare trebuie să includă toate licențele necesare pentru funcționalitatea completă, așa cum este descris în această specificație: licențe pentru hipervizor, SDS, sisteme de management și monitorizare, în cantitățile necesare, pentru buna funcționare a soluției hiperconvergente ca un tot unitar.

Cerințe funcționale și tehnice suplimentare pentru platforma de virtualizare

- Consola de gestionare a clusterului trebuie să fie distribuită, să nu aibă un singur punct de defecțiune și să nu necesite instalarea sau configurarea de componente suplimentare.
- Trebuie să fie posibilă utilizarea nodurilor de diferite tipuri în cadrul aceluiași cluster, cum ar fi:
    - noduri cu medii de stocare interne SSD și HDD și noduri numai cu medii de stocare interne SSD;
    - noduri cu medii de stocare interne SSD și NVMe și noduri numai cu medii de stocare interne NVMe.
- Întreaga capacitate a subsistemului de stocare trebuie să fie utilizabilă, nu se acceptă soluții ce necesită unități de stocare interne dedicate pentru cache.
- Sistemul trebuie să accepte scalarea folosind noduri cu configurații diferite (calcul și stocare), indiferent de tipul sau dimensiunea unităților (PCIe SSD, NVMe SSD, SAS/SATA SSD, SAS/SATA HDD).
- Sistemul SDS trebuie să asigure protecția datelor prin crearea cel puțin a două sau trei copii pe noduri diferite. Cu două copii, o defecțiune a unui server sau a unei componente interne de stocare nu trebuie să ducă la pierderea datelor. Cu trei copii, trebuie tolerată defectul simultan a două servere sau componente interne de stocare.
- Trebuie să fie acceptate politici de replicare flexibile, inclusiv capacitatea de a atribui politici diferite volumelor logice individuale.
- Sistemul SDS trebuie să accepte distribuția automată a datelor, plasând datele cele mai accesate pe unități de stocare interne mai rapide. Distribuția trebuie să funcționeze pe noduri cu orice tip de mediu de stocare intern.
- Sistemul SDS trebuie să optimizeze stocarea datelor pe discuri fizice folosind următoarele metode:
    - compresie în linie și în repaus;
    - deduplicarea la nivel de cluster;
    - protecția datelor prin algoritm erasure coding,
    - Redirect-On-Write pentru clonare și crearea de copii snapshot,
    - distribuire automată (tiering) a datelor atunci când două tipuri diferite de media sunt prezente în cluster pentru asigurarea unui înalt nivel de eficiență și performanță în stocarea datelor.
- Deduplicarea și protecția datelor prin algoritm erasure coding trebuie să fie acceptate atât pentru nodurile all-flash, cât și pentru cele hibride.
- Orice combinație de tehnici de optimizare a stocării trebuie să fie configurabilă pe volum.
- Compresia și deduplicarea datelor în repaus trebuie să funcționeze la nivelul clusterului, inclusiv pe diferite tipuri de unități.
- Crearea și stocarea de copii snapshot și a clonelor de mașini virtuale și discuri în orice cantitate nu trebuie să degradeze performanța sau să crească latența I/O.
- Pentru a reduce latența pentru operațiile de citire precum și a traficului de rețea dintre nodurile hiperconvergente, platforma hiperconvergentă trebuie să pozitioneze automat datele unei mașini virtuale pe unitățile locale ale nodurilor hiperconvergente în care acestea rulează.
- Sistemul trebuie să permită replicarea mașinilor virtuale pe o locația la distanță fără alte componente software terțe, cel puțin trebuie să permită replicare asincronă

- Sistemul trebuie să includă instrumente atât pentru migrarea manuală, cât și pentru cea automată a mașinilor virtuale pe platforma hiperconvergentă nouă.

Platforma de virtualizare va fi licențiată pentru minim toate echipamentele livrate în cadrul proiectului (de ex: 20 CPU socket, 8 **Noduri Hiperconvergente (minim 8), Noduri dedicate bazei de date (minim 2)**. Pentru Nodurile Hiperconvergente destinate componentei de gestiune și analiză a datelor vor fi incluse toate licențele software necesare pentru asigurarea funcționării optime a soluției software de baze de date.

Platforma de virtualizare va fi instalată cu facilități de balansare și failover.

Toate componentele sistemului de management cloud (cum ar fi: sistemul de operare, elementele de gestionare a virtualizării, elementele de management al rețelei, elementele de gestionare a resurselor de stocare, elementele de gestionare a resurselor de calcul fizice) trebuie să aibă suport uniform de la producător/furnizor.

5.7.3. Scannere de mare viteză

Procesul de transformare digitală a fluxurilor operaționale ale APIA presupune, înainte de toate, ca documentele să circule în format exclusiv digital. Dată fiind previzibilitatea unei perioade de tranziție în care unii dintre fermieri vor continua să depună documentație în format fizic, se impune, așadar, o abordare sistemică pentru digitizare. Se va avea, în acest scop, în vedere și faptul că volumul de documente dintr-un dosar poate fi extrem de mare, deci soluția hardware va trebui să fie una de mare viteză, pentru a corespunde adecvat nevoilor practice. Achiziția va fi dimensionată pornind de la numărul punctelor de lucru ale APIA, la nivel național: **330 de scannere.**

Caracteristica	Cerința tehnică (minimală)
Scanner de mare viteză, A4, color, duplex	
Rezoluție scanare	600 x 600 dpi
Viteza scanare	standard minim 60ppm/120ipm duplex
Format maxim	A4
Senzor optic	CCD, CIS, color
Format scanare	JPEG; TIFF; PDF; PDF Compact; PDF criptat; XPS; XPS Compact
Funcții	Scanare către E-Mail, Scanare către FTP, Scanare către Box (SSD), Scanare către PC (SMB), Network Twain, Scanare catre WebDAV, Scanare către USB; compatibilitate SANE și ISIS; detectare documente capsate; detectare alimentare multiplă; îndreptarea mecanică a documentelor; detectare blocare hârtie
Alimentator automat de originale	100 coli la 80g/mp, 60–210 g/mp
Ciclu zilnic recomandat (Daily Duty Cycle)	9.000 pagini
Display echipament	Capacitiv, multi-touch, Web-browser standard
Procesor	Quad-Core, 1.6 GHz
Memorie	4 GB

Caracteristica	Cerința tehnică (minimală)
Unitate de stocare interna	250 GB SSD
Conectivitate	10/100/1000 BaseT 2.4GHz/5GHz dual band wireless USB 2.0
Administrare	
Conturi de acces	Suport Active Directory; Autentificare user name + password + e-mail + smb folder); Optional: autentificare Biometrica, ID card
Securitate	Filtrare IP și blocare porturi; SSL2; SSL3 și comunicare în rețea TLS1.0/1.1/1.2; suport IPsec; suport IEEE 802.1x; Autentificare utilizator; Raport autentificare; Kerberos; Suprascriere hard disk (8 tipuri standard); Criptare date hard disk (AES 256); Ștergerea automată a memoriei;
Certificări/standarde	
Conformitate cu standarde europene	Certificare CE conform directivelor UE: - Siguranța în exploatare: 2014/35/EU - Echipamente de joasă tensiune: 2014/35/EU - Compatibilitate electromagnetică: 2014/30/EU - Declarație RoHS: 2011/65/EU (se vor prezenta copii după certificatele emise de instituțiile acreditate să elibereze respectivele certificări sau alte documente relevante care atestă îndeplinirea cerinței)

Acestea trebuie să fie compatibile cu solutia propusă și să permită integrarea facilă în fluxul de lucru stabilit pentru scanarea și preluarea documentelor în sistemul informatic creat.

5.8. COMPONENTELE SOFTWARE

5.8.1. Componenta de portal

Soluția va dispune de o interfață de tip portal web, prin care vor fi puse la dispoziția cetățenilor și mediului de afaceri informații și servicii structurate în așa fel încât să permită utilizatorului să se ghideze singur către problematica dorită și să consulte astfel informații cu privire la actele necesare eliberării de documente, la autorizații sau certificate, și să ofere posibilitatea de a descărca formulare tipizate în format electronic, care să poată fi tipărite și predate la ghișee, în cazul serviciilor care nu pot fi implementate complet sub formă electronică.

Se vor implementa astfel atât servicii complet electronice, cu grad mare de sofisticare (transmitere integral electronică a dosarelor aferente solicitărilor, precum și primirea electronică a răspunsurilor sau a documentelor solicitate), cât și servicii parțial electronice, cu grad mai scăzut de sofisticare (transmitere electronică a solicitării și ulterior ridicare a documentelor emise de la ghișee sau doar accesul la formulare tipizate sau simpla informare cu privire la procedurile necesare în vederea obținerii unui anumit serviciu).

Interfața de tip portal va putea fi utilizată pentru accesarea serviciilor electronice atât pe baza unei autentificări prealabile (pe baza unui cont de utilizator), cât și fără

autentificare prealabilă.

Ca regulă generală, serviciile electronice vor fi disponibile utilizatorilor într-un mod cât mai accesibil, cu introducerea unui set cât mai restrâns de date (set limitat la cele absolut necesare în vederea finalizării solicitării, conform prevederilor legale aplicabile) și fără a solicita dovedirea identității solicitantului în situațiile în care acest lucru nu este solicitat în mod explicit prin lege.

În situația în care este necesară dovedirea identității solicitantului înaintea furnizării serviciului, atunci respectivul serviciu va fi accesibil numai după autentificarea prealabilă a solicitantului în cadrul Portalului și verificarea contului de utilizator. Numele de utilizator în cazul tuturor conturilor va fi adresa de email a utilizatorului contului respectiv, adresă care va fi utilizată și pentru realizarea corespondenței cu utilizatorul și care trebuie să fie unică la nivelul utilizatorilor Portalului.

În scopul personalizării serviciilor oferite cetățenilor, sistemul va pune la dispoziția utilizatorilor autentificați un spațiu privat destinat stocării datelor de contact și a diferitelor documente care trebuie să însoțească diferitele solicitări de servicii. De asemenea, utilizatorii vor putea salva și ulterior regăsi în cadrul spațiului lor privat din cadrul Portalului toate documentele care le-au fost eliberate în format electronic, ca urmare a utilizării serviciilor electronice. În cadrul spațiului privat al utilizatorilor se va salva și regăsi ulterior întregul istoric de utilizare a serviciilor electronice (solicitări transmise și documente primite). Fiecare utilizator care deține un cont în portal va putea astfel să își acceseze spațiul virtual privat pentru a-și actualiza informațiile stocate, a consulta istoricul solicitărilor proprii și documentele electronice emise de instituție în urma acestor solicitări.

Din secțiunea de servicii a portalului, utilizatorii vor avea posibilitatea de a iniția o solicitare către instituție, prin completarea de formulare electronice web, în vederea solicitării de informații, a depunerii online de documente, a depunerii de petiții sau a înscrierii în audiență. În funcție de tipul de serviciu electronic solicitat, va fi posibilă utilizarea acestor funcționalități în mod autentificat sau neautentificat.

Setul de informații personale pe care utilizatorii le vor putea completa în portal în cadrul profilului aferent spațiului lor virtual va putea fi utilizat ulterior pentru completarea automată a unor câmpuri din formularele web aferente diferitelor servicii electronice disponibile în cadrul portalului. Astfel, va exista o funcționalitate care, pentru fiecare serviciu electronic și formular web în parte, va permite pre-popularea acestuia cu datele existente în cadrul profilului utilizatorului respectiv sau prin preluarea acestor date din surse de date variate (atât din interiorul APIA, cât și de la alte instituții publice).

Serviciile electronice vor fi structurate în cadrul portalului într-un mod care să permită identificarea facilă de către utilizator a serviciilor care îi sunt necesare. Se va evita astfel structurarea serviciilor în funcție de (sau pornind de la) diferitele formulare sau tipizate existente în acest moment în cadrul instituției, întrucât o astfel de abordare presupune o cunoaștere prealabilă de către solicitant a tuturor pașilor necesari în cadrul unui anumit demers și apelarea punctuală a fiecărui astfel de pas. Se va utiliza în schimb o abordare care să plece de la obiectivul final dorit de către solicitant, urmând ca solicitantul să fie ulterior îndrumat către toți pașii intermediari necesari în vederea atingerii obiectivului final dorit.

În cazul în care, în vederea obținerii unui anumit document din partea instituției, este necesară prezentarea mai multor documente, atunci utilizatorul va fi ghidat în mod

automat către pașii necesari în vederea obținerii respectivului document. În cazul în care pentru furnizarea unui serviciu electronic este necesară achitarea unei taxe, atunci utilizatorul va fi ghidat în mod automat către pagina de plată electronică.

Interacțiunea cu utilizatorii se va realiza prin intermediul formularelor electronice de tip web, cu ajutorul cărora se vor colecta toate informațiile necesare în vederea prestării serviciului solicitat. Formularele web nu vor copia formularele tipizate existente în acest moment, ci vor conține numai informațiile pe care trebuie să le furnizeze solicitantul. După completarea formularelor web, Portalul va genera în mod automat fișiere PDF care vor replica formularele tipizate utilizate în relația de la ghișeu, pe care le va completa automat cu datele colectate prin formularele web completate de către solicitant. Fișierele PDF astfel obținute vor putea fi ulterior semnate electronic de către solicitant și transmise prin intermediul Portalului în vederea furnizării serviciilor solicitate sau imprimate și prezentate la ghișeu. În ambele situații se va avea în vedere preluarea automată a datelor structurate introduse inițial de către solicitant prin formularele web în bazele de date ale aplicațiilor de tip „back-office", astfel încât să nu fie necesară reintroducerea manuală a respectivelor informații de către funcționari în cadrul proceselor de rezolvare a respectivelor solicitări.

Toate aceste funcții ale Portalului vor permite cetățenilor inițierea unor demersuri administrative asistate de sistem în vederea atingerii următoarelor obiective, fără a fi necesară intervenția funcționarilor Autorității contractante:

- Îndrumarea solicitanților pe tot parcursul derulării demersului administrativ, din momentul identificării corecte a serviciului electronic relevant și până la primirea răspunsului din partea Autorității contractante.
- Solicitarea de informații relevante fiecărei categorii de solicitări printr-un sistem de formulare inteligente.
- Validarea și transformarea informațiilor structurate furnizate de cetățeni în vederea preluării lor automate în alte aplicații interne ale instituției
- Declanșarea automată a proceselor instituționale de rezolvare a solicitărilor primite prin Portal prin distribuirea sarcinilor către responsabilii din departamentele instituției, conform naturii demersului inițiat.
- Informarea automată a solicitantului (prin email) cu privire la stadiul rezolvării solicitării sale.

Întreaga interfață a sub-sistemului Portal va folosi tehnologii web în vederea utilizării acestuia folosind browserele cele mai răspândite pe calculatoarele desktop (Edge, Mozilla Firefox, Google Chrome). Pentru acele servicii electronice care nu necesită un flux de lucru complicat și încărcarea de documente (servicii de informare, de plată electronică sau de solicitare a eliberării unor documente strict în baza completării de formulare web), se va avea în vedere folosirea unor tehnologii web „responsive", în vederea obținerii unei experiențe de utilizare optime pe dispozitive mobile de tip smartphone și tabletă (adică adaptarea poziției informației și a câmpurilor în cadrul unui ecran sau formular web la dimensiunea și orientarea ecranului dispozitivului mobil utilizat).

Utilizatorul final al componentei de front-office nu va fi dependent de o anumită tehnologie pentru a accesa serviciile furnizate on-line și se va avea în vedere includerea de soluții care facilitează incluziunea categoriilor defavorizate.

Se vor implementa servicii electronice aferente doar competențelor exclusive ale administrației publice locale.

În cadrul sistemului informatic integrat se va implementa o soluție de securitate pentru asigurarea conformării GDPR, atât prin audit și rapoarte specifice directivei europene, executate la nivelul infrastructurii IT, cât și prin monitorizare activă a accesului utilizatorilor la informațiile ce conțin date cu caracter personal.

Integrarea software intre aplicațiile ofertate și aplicațiile interne din cadrul instituției va putea fi realizată prin servicii web. Informațiile ce vor face obiectul integrărilor software vor fi stabilite în mod concret în cadrul etapei de analiză a proiectului.

Demersurile respective vor fi preluate automat (sau după o triere manuală, în funcție de gradul de complexitate al fiecărui tip de demers) din Portal în sistemul de registratură și de management electronic al documentelor, pentru a li se aloca număr de înregistrare. Portalul va fi structurat atât pe categorii de problematici, cât și pe tipuri individuale de solicitări adresate diferitelor compartimente existente în cadrul instituției, astfel încât utilizatorul să poată regăsi ușor problematica dorită sau formularul necesar.

Portalul va include atât o secțiune de informare cu privire la procedurile aplicabile și la tipurile de acte necesare în cazul fiecărui tip de serviciu, la taxele care trebuie plătite, la programul de lucru la ghișeu, cât și o secțiune pentru accesarea directă a serviciilor electronice disponibile în cadrul portalului.

Serviciile electronice vor putea fi utilizate în mod autentificat sau neautentificat, în funcție de gradul de încredere considerat necesar din perspectiva naturii informațiilor transmise și a efectelor juridice asociate demersului întreprins.

Utilizarea unui serviciu electronic va presupune parcurgerea de către cetățean a unei succesiuni de activități asistate de sistemul portal. Serviciile electronice vor fi centrate pe activități și pe finalitatea acestora și nu pe formulare care să replice formularele off-line existente în cazul interacțiunii la ghișeu.

Fiecare serviciu electronic disponibil în portal va consta într-o succesiune de activități particularizate, configurate în etapa de implementare a sistemului conform reglementărilor și modului de organizare al instituției.

Activitățile care compun un serviciu electronic reprezintă o succesiune de pași care pot include:

- ecrane de informare
- ecrane care conțin formulare web care trebuie completate, eventual cu atașarea de fișiere (fotografii, documente scanate)
- ecrane de vizualizare a unor documente generate automat de către Portal, în baza informațiilor furnizate până la acel moment
- ecrane pentru realizarea unor plăți electronice.

Configurarea serviciilor electronice trebuie să se realizeze individual, astfel încât modificarea unui serviciu să poată fi realizată fără operațiuni de recompilare a întregii platforme Portal.

Platforma Portal va permite configurarea de noi servicii electronice, fără a necesita operațiuni de recompilare a întregii platforme Portal.

Formularele vor putea ascunde sau afișa condiționat texte informative sau câmpuri de editare în funcție de valorile introduse de utilizator în câmpuri anterioare ale aceluiași formular web sau ale unuia anterior.

Formularele web completate de utilizator vor fi interpretate în timp real de sistem, lucru care va indica utilizatorului următoarea activitate necesară în vederea finalizării demersului dorit, activitate care poate include:

- completarea altui formular
- atașarea de documente
- efectuarea unei plăți electronice.

Utilizatorii autentificați vor avea acces și vor putea vizualiza în mod organizat istoricul solicitărilor trimise. În cadrul unei solicitări se vor putea vizualiza, cronologic, toate etapele comunicării între utilizator și instituție și se va putea vizualiza stadiul rezolvării fiecărei solicitări în parte.

Portalul va include funcționalitățile necesare pentru realizarea de plăți electronice pentru demersurile ce presupun plata unei taxe.

Valoarea taxei care trebuie achitată va fi determinată automat de către platforma software pe baza regulilor asociate serviciului electronic respectiv și a selecțiilor realizate de către solicitant în cadrul formularelor web din pașii anteriori ai procesului.

În cazurile în care nu este posibilă automatizarea completă a serviciului electronic (adică furnizarea serviciului electronic strict în baza informațiilor completate de către solicitant, fără a fi necesară intervenția unui funcționar — operator uman), fluxul de execuție a serviciului solicitat va putea include și activități care vor fi efectuate off-line (manual) de către un funcționar — de exemplu: validarea conținutului documentelor transmise de către solicitant, evaluarea legalității sau oportunității unui demers, determinarea cuantumului unei taxe pentru care sistemul nu dispune de reguli automate de calcul.

În cazul în care este necesară intervenția manuală a unui funcționar în cadrul unei etape a unui proces de tratare a unei solicitări de servicii, atunci platforma Portal va genera și va înregistra în componenta de administrare a serviciilor electronice o sarcină, iar funcționarul responsabil va fi notificat automat prin email cu privire la necesitatea efectuării sarcinii respective. Sarcina înregistrată și notificarea primită vor conține un link care va permite accesul la dosarul solicitării electronice a cetățeanului din Portal, unde funcționarul va putea consulta formularele web completate, solicitarea generată și documentele suport atașate la aceasta.

După finalizarea activității manuale (off-line), funcționarul va procesa sarcina alocată de către Portal și va transmite solicitantului un răspuns generat automat în baza completării unui șablon de formular web de răspuns pre-completat cu datele relevante extrase din solicitarea cetățeanului. După completarea acestui formular de către funcționar, sistemul va transmite automat către solicitant un mesaj email care va conține un link către următoarea activitate pe care acesta trebuie să o parcurgă în vederea finalizării demersului (efectuarea plății sumei calculate de funcționar, atașarea altor documente justificative, completarea unui formular suplimentar).

Etapelor procesului care presupun o acțiune din partea cetățeanului li se vor putea configura termene maxime de așteptare a unui răspuns. Dacă în această perioadă cetățeanul nu realizează activitatea solicitată, atunci demersul inițial este anulat, cu notificarea cetățeanului.

La finalizarea procesului aferent unui demers, Portalul va genera un document

electronic care va cuprinde toate informațiile completate de către solicitant în formularele web aferente pașilor de proces deja urmați, document care va putea fi-semnat electronic de către solicitant și transmis prin Portal, fie transmis prin e-mail, fie imprimat în cazul în care se dorește depunerea sa la ghișeu, fie salvat în spațiul virtual personal al utilizatorului (în cazul utilizatorilor cu cont de portal).

Generarea documentelor electronice în baza informațiilor structurate completate de către solicitant în formularele web trebuie să fie bazată pe șabloane configurabile, în care vor putea fi incluse atât informații structurate culese din formularele aferente serviciului electronic cât și paragrafe formatate de text predefinit și informații referitoare la plățile efectuate în contextul respectivului demers.

Pentru serviciile electronice automate, Portalul va permite transferul automat al unei solicitări transmise prin Portal în sistemul de registratură și management al documentelor, în vederea înregistrării în registrul general al instituției.

Portalul va permite configurarea pentru fiecare serviciu electronic în parte a modului în care se realizează înregistrarea solicitării în sistemul de registratură electronică: automat sau manual (off-line), de către un funcționar.

Ulterior înregistrării solicitării în sistemul de registratură și management al documentelor, solicitantul va fi înștiințat automat prin email despre acest lucru și va putea vizualiza online stadiul finalizării acesteia, utilizând un link inclus în mesajul email primit. De asemenea, solicitantul va fi notificat automat prin email atunci când solicitarea sa a finalizat fluxul de tratare în cadrul sistemului de management al documentelor.

Modul de ajutor pentru utilizatori

Modulul va avea rolul de a furniza utilizatorilor interni și externi acces la informațiile din cadrul instituției dar și din alte surse externe prin intermediul unei interfete conversaționale (Chatbot). Setul de informații disponibile va fi multi-sursa (Site Web, platforma de management a documentelor și fluxurilor de lucru, website-uri ale altor instituții) și va putea fi gestionat printr-un proces controlat care va permite solicitarea și aprobarea modificărilor și a actualizărilor setului de informații disponibile prin interfața conversațională.
Modulul va cuprinde o componenta de management și o componenta de comunicare (de tip Chatbot) ce vor comunica pe baza unui motor de API, atât între ele cât și cu resursele externe. Atât platforma de administrare cât și cea de comunicare trebuie să permită Beneficiarului să modifice fluxurile de lucru fără cunoștinte de programare.
Soluția trebuie să permită dezvoltări ulterioare de către terți, beneficiarul avand posibiliatea de export/import în formate deschise (JSON, XML, YAML) si acces la mecanisme de personalizare (plugin-uri, microservicii) fără a necesita acces exclusiv la cod sursă proprietar. Soluția trebuie să permită clusterizare orizontală nativă și distribuirea sesiunilor între mai multe noduri astfel incat sa se poata instala pe infrastructura existenta la beneficiar

Din punct de vedere funcțional modulul va trebui să asigure minim:

- Accesul utilizatorilor externi și interni la o interfață conversațională de tip chatbot, in limba romana, integrată în site-ul institutiei;
- Posibilitatea de a integra SSO in interfata chatbot-ului, astfel incat sa poata fi transmis continut personalizat in functie de utilizatorul inregistrat

- Chatbotul va putea raspunde la un set extins de întrebari din baza de date de documente sau va raspunde cu raspunsuri predefinite disponibile in baza de date (Knowledgebase).
- Răspunsurile vor include text, imagini si link-uri catre resurse interne si externe;
- Întrebarile si răspunsurile vor putea fi organizate ierarhic (arborescent) pe cel putin trei niveluri;
- Baza de date cu întrebari si răspunsuri va fi definită central la nivelul componentei de management și va fi gestionata dinamic prin intermediul unui proces care va avea mai mulți pași - de exemplu:
    - solicitare adăugare/modificare, aprobare, pregătire raspuns, solicitare punct de vedere, aprobare finala, publicare);
    - In fiecare pas al procesului unul sau mai mulți actori vor putea interacționa cu procesul prin introducerea și modificarea datelor;
- La nivelul fiecarui pas și la nivelul tranzițiilor între pași se vor putea genera acțiuni predefinite (de exemplu: trimite mail, citește prin API, scrie prin API, etc);
- Procesul va putea fi modificat cu ușurință prin intermediul unui designer grafic (la nivelul componentei de management) ori de câte ori vor aparea schimbări, fără să fie necesare cunoștințe de programare;
- Baza de date cu întrebari și răspunsuri stocată la nivelul componentei de management, odată actualizată, va declanșa modificări automate în consecință prin intermediul API, la nivelul chatbotului.
- Solicitările de modificare/adaugare a bazei de date cu întrebări și răspunsuri se vor putea face atât la nivelul chatbotului cât și prin intermediul mailului iar acestea vor inițializa automat procesul de actualizare în componenta de management;
- Chatbotul intern va putea răspunde la un set extins de întrebări, suplimentar față de cele disponibile în chat botul extern.
- Chatbotul va putea raspunde la intrebari din baza de date de documente

Componenta de comunicare

Platforma de creare a chatbotilor (comunicare) trebuie să aibă următoarele caracteristici:

- Platforma trebuie sa fie portabila pe mai multe sisteme de operare, fara modificari de cod si sa respecte standardele deschise.
- Platforma de administrare trebuie sa permita integrarea SSO (Single Sign-On) cu mecanismele de autentificare ale beneficiarului.
- Platforma trebuie să permită dezvoltarea un număr nelimitat de chatboti;
- Platforma trebuie să fie “no code” - adică dezvoltarea unui chatbot să se poată face fără scriere de cod si să dețină instrumente de tip designere vizuale pentru conversatii și integrari;
- Platforma trebuie sa permita exportul de flow-uri in format deschis pentru audit independent, duplicare flow-uri sau migrare date
- Platforma trebuie să permită importul/exporturi de seturi întregi de intent-uri odata sau să actualizeze un flux existent printr-un mecanism simplu de import;
- Platorma trebuie sa permita importul de informatii in diverse formate (word, pdf, CSV, RSS) in baza de date de informatii necesara pentru a putea raspunde la intrebari.

- Platforma trebuie să permita integrarea altor tehnologii: traducere automată, semnatură digitală, solutii tip document management, semnare electronică de documente, tehnologii de voce;
- Platforma trebuie să includă suport NLP (Natural Language Processing) pentru conversații;
- Platforma trebuie să includă suport nativ NER (Name Entity Recognition) cu capacitate de extragere a intenției si a entităților în limba romana;
- Platforma trebuie să permită definirea unui model de entitati pentru extragerea obiectelor complexe din conversatie (de exemplu: beneficiar, problema, etc);
- Platforma trebuie să conțină instrumente de vizualizare a istoricului conversational;
- Platforma trebuie să permită suport pentru utilizatori pe multiple canale de comunicatie – Webpage , Facebook Messenger si WhatsApp pentru utilizatori externi.
- Platforma trebuie să permită setarea de teme, fonturi, culori, logo dar și crearea unor controale particularizate de tip HTML care să poată fi integrate în fluxurile conversationale;
- Platforma trebuie să aibă posibilitate de integrare cu alte sisteme software prin API si la nivel de baza de date.
- Platforma trebuie să permită acces securizat pe baza de rol pentru autorii de chaboti -
- Platforma trebuie să permită acces securizat pe baza de rol pentru utilizatorii de chatbot – să se poata defini roluri în funcție de care să se poată controla fiecare flux de conversație cu chatbotul;
- Platforma trebuie să conțină capabilități de analiza si raportare
- Platforma va contine în mod automat statistici privind modul în care a decurs conversația cu utilizatorii, care au fost cele mai des întâlnite întrebări sau la ce nu a fost pregătit chatbot-ul să răspundă;
- Platforma trebuie să includă capabilități de alertare – în cazul unui apariției unui eveniment să se poata inițializa în mod automat o conversație;
- Platforma trebuie să includă un control al învățării automate – autorii de chatbot pot revizui continutul de învățare automată si îl pot aproba sau respinge;
- Raport istoric privind utilizarea NLU (Natural Language Understanding), oferind statistici privind gradul de utilizare a motorului NLU si scoruri NLP; Acolo unde scorurile sunt scăzute, să existe posibilitatea de a adauga noi fraze de antrenament;
- Platforma trebuie să permită antrenarea chatbotului cu întrebări noi de tip întrebare-răspuns neconectate, să se poată face de către departamentul IT al Beneficiarului prin încărcarea unui fișier excel în conversatie;
- Platforma va avea capabilitati si mecanisme de augumentare cu date proprii RAG si NLP pentru a putea raspunde la intrebarile pentru care nu a detectat un raspuns prestabilit in baza de date sau pentru a putea sugera intrebari similare care se afla in baza de date cunostiinte.
- Modelele folosite trebuie sa permita sa fie finetuned pe date proprii (dupa politici stricte de confidentialitate) pentru a imbunatati rezultatele oferite.

5.8.2. Componenta pentru managementul documentelor

Cerințe specifice aplicație de management al documentelor

Aplicația software de management al documentelor va avea cel puțin următoarele module, proiectate pentru o funcționare împreună în același sistem:

- Depozit și captură de documente
    - Constituirea și gestionarea depozitului de documente electronice operaționale.
    - Funcționalități minimale:
        - Încărcarea și stocarea documentelor în diverse formate (PDF, DOCX, XLSX, imagini etc.).
        - Indexarea automată/manuală a documentelor cu metadate relevante (tip document, dată, autor etc.).
        - Căutare avansată și filtrare după metadate și conținut.
        - Controlul versiunilor documentelor (versioning).
        - Audit trail pentru modificările efectuate asupra documentelor.

- Registratură electronica
    - Înregistrarea automată și gestionarea documentelor primite și transmise.
    - Funcționalități minimale:
        - Generarea numerelor de înregistrare și urmărirea fluxului documentelor.
        - Asocierea documentelor cu destinatari și departamente.
        - Istoricul complet al documentelor (modificări, transferuri, aprobare).

- Fluxuri de lucru
    - Automatizarea proceselor interne și a traseelor documentelor.
    - Funcționalități minimale:
        - Definirea și personalizarea fluxurilor de aprobare, revizuire și semnare.
        - Notificări automate pentru utilizatori la fiecare etapă a fluxului.
        - Urmărirea stadiului fiecărui document în cadrul fluxului de lucru.

- Management arhivă fizică de documente
    - Gestionarea documentelor în format fizic, integrate cu aplicația electronică.
    - Funcționalități minimale:
        - Evidența locației și stării documentelor fizice.
        - Legarea documentelor fizice de corespondentele electronice.
        - Rapoarte privind disponibilitatea și circulația documentelor fizice.

- Rapoarte
    - Generarea de rapoarte standard și personalizate privind activitatea documentelor.
    - Funcționalități minimale:
        - Rapoarte de volum, tip document, fluxuri finalizate/în curs.
        - Exportul rapoartelor în formate comune (PDF, XLSX).
        - Dashboard de monitorizare a stării și termenelor documentelor.

- Administrare
    - Configurarea și gestionarea sistemului și a utilizatorilor.
    - Funcționalități minimale:
        - Gestionarea drepturilor și rolurilor utilizatorilor.
        - Configurarea fluxurilor de lucru și a șabloanelor de documente.
        - Monitorizarea activității și audit log pentru toate modulele.
-

Modulul depozit și captura de documente trebuie să asigure constituirea depozitului de documente electronice operaționale, asigurând funcționalitățile minimale enumerate în cadrul acestui capitol, grupate pe categorii.

Organizare

- stocarea documentelor într-un spațiu centralizat și organizat și posibilitatea de a asocia metadate pentru fiecare document în parte
- toate funcționalitățile vor fi disponibile prin intermediul unui client web
- organizarea documentelor într-o structură ierarhică intuitivă, de tip arborescent, similară sistemelor de fișiere.
- organizarea documentelor în structuri care să simuleze modalitatea reală de organizare în dosare și documente.
- model de date în care conținutul unui document și metadatele asociate formează un obiect fără limitări asupra numărului de documente și metadate stocate sau asupra capacității de stocare pe care o poate gestiona
- arhivarea documentelor în funcție de tip și termen de păstrare
- selectarea anumitor documente cu care se lucrează frecvent și gruparea lor într-o zonă de documente de tip favorite
- mecanisme de identificare a fișierelor duplicat, atât după denumire cât și după conținutul acestora
- definirea de colecții de documente ce conțin documente din depozit grupate după diverse criterii, cu scopul de a oferi acces temporar unui set de utilizatori create pentru diverse scopuri precum comisii de examinare, echipe de proiect, comitete tehnico-economice, etc.
- definirea de seturi de metadate specifice aferente fiecărui document care vor fi afișate sub formă de listă la accesarea acestuia și vor putea fi utilizate la căutări rapide
- Definire structură organizatorică organigramă care să conțină elementele organizaționale din cadrul instituției, responsabilii de aceste departamente și relațiile de subordonare. Sistemul trebuie să permită:
  - definirea organigramei într-o interfață grafică generată pe baza datelor configurate
  - posibilitatea de import a organigramei din fișiere xls
  - posibilitate de mutare post pe diferite ramuri ale organigramei cu actualizare drepturi de acces.

Indexare

- indexarea automată a documentelor
- stocarea și indexarea automată a documentelor în foldere/dosare predefinite în funcție de tipul documentelor
- indexează atât metadatele documentelor, cât și conținutul acestora, atât pentru fișiere text, cât și pentru fișiere word, excel, XML, imagine, pdf, jpeg, tiff, bmp. Pentru fișierele de tip imagine, se vor executa operațiuni de OCR în vederea indexării.

Încărcarea/descărcarea documentelor electronice

- Încărcarea oricăror tipuri de documente indiferent de tipul de fișier în care este stocat (de exemplu pdf, tiff, jpeg, bmp, gif, doc, docx, rtf, txt, html, etc.);
- adăugarea de documente electronice printr-un mecanism de tip ”drag-and-drop”;
- permite utilizatorilor adăugarea și ștergerea documentelor electronice;
- popularea sistemului utilizând modulul de captură documente;

- expune un driver de imprimantă virtuală care va fi disponibil utilizatorilor pentru încărcarea documentelor în cadrul aplicației, prin utilizarea funcționalității “Print To”;
- permite importul automat în arhiva electronică a fișierelor existente de pe suport de stocare electronic, organizat în foldere și subfoldere, împreună cu fișiere excel asociate care conțin tipul documentelor și valorile metadatelor pentru fiecare fișier;
- importul în arhivă al documentelor scanate în format electronic pdf semnate digital cu semnătură electronică extinsă;
- funcționalitate de semnare a documentelor cu semnătură electronică cu valoare legală (token) direct din aplicație, fără a fi nevoie ca utilizatorul sa descarce documentul local și să îl încarce iar în sistem, atât pentru documente de tip word, cât și pdf.

Existența unei mape de semnături, sub forma unui client local, unde:
- Fiecare utilizator logat va avea afișate toate documentele primite spre semnătură din cadrul aplicației, indiferent de modalitate;
- Utilizatorul poate semna documentele din aplicația web, caz în care acestea vor dispărea din mapa locală;
- Utilizatorul poate accesa direct mapa locală fără a se loga și în aplicația web pentru a realiza doar semnarea documentelor, individual sau bulk. Odată semnate, documentele vor fi trimise automat în aplicație împreună cu informații despre semnare: autor, data, rezoluție.

Existența în cadrul aplicației a unei liste de semnături și rezoluții la nivel de document, care se va completa automat în momentul semnării acestuia:
- semnarea electronică cu certificat calificat și stocarea în același loc atât a documentelor sursț, cât și a fișierelor de semnătură digitală valide cu aceiași indecși de căutare,
- Ștergerea automată a semnăturilor de pe un document la trimiterea sa din nou pe un flux de aprobare,
- încărcarea bulk automată a documentelor prin monitorizarea anumitor foldere locale,
- încărcarea bulk automată a documentelor prin monitorizarea anumitor căsuțe de mail.

Aplicația trebuie să permită încărcarea de fișiere mari pe post de atașament, oferind suport pentru încărcarea acestora din internet. Spre exemplu, dacă se întrerupe conexiunea la aplicație în momentul importului, la reluarea conexiunii să se realizeze importul din punctul în care s-a oprit.

În cazul fișierelor de dimensiune mare, pentru a nu bloca lucrul cu documentele, aplicația trebuie să permită accesul și lucrul cu documentul, în timp ce încărcarea fișierului se face în background, fiind disponibil utilizatorului după încărcarea acestuia.

Trebuie să se permită operațiuni de download bulk pe baza căutărilor salvate.

Navigare, căutare și filtrare
- interfețe de căutare accesibile din browser: cel puțin Microsoft Edge, Google Chrome și Mozilla firefox;
- posibilitatea de salvare și reutilizare a seturilor de criterii de căutare avansată;
- definirea de “liste filtrate” de documente, vizibile pentru utilizator ca niște foldere, 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) și a modului de afișare a rezultatelor (grupate după un an, sau după orice alt câmp, de exemplu);
- utilizatorii sa poată vizualiza, pentru fiecare document în parte, istoricul modificărilor, cu evidențierea modificărilor în fiecare nou context;
- interfață de vizualizare a detaliilor și descărcare a conținutului fișierelor zip (pentru fiecare din fișierele arhivate într-o arhivă format zip);
- afișarea direct în browser a documentelor de tip imagine, fără a fi nevoie de achiziționarea de licențe pentru programe software auxiliare care să fie instalate pe stația de lucru. Pentru fișierele de tip video trebuie să se poată rula fișierul direct în viewer-ul respectiv;
- vizualizarea documentelor pe diferite niveluri de zoom, de la ansamblu până la cele mai mici detalii;
- căutarea automată a documentelor, inclusiv după textul conținut cel puțin pentru: documentele scanate utilizând OCR, fișiere office (Word, Excel), fișiere PDF și emailuri;
- fișierele de tip PDF / imagine se vor putea converti automat de către sistem în fișiere de tip PDF Searchable, pentru a se putea permite căutarea textului direct în cadrul documentului;
- salvarea căutărilor 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 (metadata), după titlul documentului și după conținutul acestuia (full text);
- căutări utilizând operatori logici booleni (”and” și ”or”) și de comparație ”egal”, "conține”, ”mai mic”, ”mai mare”, căutări de proximitate (de exemplu sunt căutați doi termeni, condiția fiind ca între aceștia să nu existe mai mult de 3 cuvinte) etc;
- căutări doar în ultima versiune a documentelor sau în toate versiunile acestora;
- “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;
- mecanism de subliniere a termenilor după care a fost efectuata căutarea, atât în metadate cât și în interiorul documentului;
- exportarea listei de obiecte 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 precum și gruparea rezultatelor “on-the-fly”.

Operații asupra documentelor/colaborare
- Susține ciclul de viață al unui document (crearea, modificarea, validarea, aprobarea, publicarea, arhivarea). În funcție de starea unui document sunt disponibile spre utilizare diferite acțiuni asupra documentelor.
- operații multiple executate asupra documentelor: versionarea automată a documentelor, permițând păstrarea tuturor versiunilor prin care trece un document/ înregistrare;
- check-out/ check-in, pentru asigurarea modificării coerente a documentelor (în lucrul colaborativ); un document aflat în statusul de “check-out” (în editare), va rămâne în continuare vizibil pentru ceilalți utilizatori, doar în mod vizualizare (read-only);
- etichetarea fiecărei versiuni, pentru a permite utilizatorilor să identifice facil versiunea căutată;

- “Roll back”, adică de revenire la o versiune anterioară;
- posibilitatea de anexare la documentul inițial și a altor documente;
- urmărirea și trasabilitatea modificărilor efectuate pe un document;
- versionarea documentelor prin funcționalități de tip „Check In - Check Out”. Formatul de stocare al documentelor electronice trebuie să fie cel nativ, astfel se exclude păstrarea documentelor în formatul propriu sistemului, pentru a asigura recuperarea facilă a datelor în caz de defecțiune;
- modificarea metadatelor documentelor electronice direct din interfața de utilizare;
- asigură un cadru integrat de colaborare pe documente prin scrierea de mesaje de colaborare pe document adresate anumitor utilizatori și păstrarea istoricului;
- operațiuni de “ On The Fly OCR” pe documentele din arhivă, fără utilizarea de aplicații terțe;
- vizualizarea și editarea documentelor de tip word direct în browser, fără a necesita alte softuri instalate local;
- semnarea electronică a documentelor direct din aplicație cu certificate intern generat de către sistem;
- transmiterea pe email a documentului direct din interfața de acces a sistemului;
- să permită definirea șabloanelor direct în aplicația Microsoft Word sau Excel. Astfel, orice document existent în format Word sau Excel va putea fi transformat în șablon, prin definirea zonelor în care vor fi precompletate valorile din metadate.

Captura documente

Permite scanarea documentelor pe format hârtie și încărcarea acestora în sistem, utilizând scanarea locală sau la distanță pentru a asigura următoarele funcționalități:

- scanare asincronă - realizarea legăturii fișierului scanat la informațiile de înregistrare în funcție de codul de bare aplicat pe document;
- capabilitatea de a imprima coduri de bare și numere de înregistrare cu imprimante de coduri de bare speciale și aplicarea pe documente;
- indexarea documentelor electronice va fi realizată atunci când imaginile scanate sunt convertite în documente .pdf în care se pot efectua căutări.
- operațiuni automate de OCR pentru toate fișierele de tip imagine și PDF;
- indexarea și căutarea automată a documentelor inclusiv după textul conținut pentru documentele scanate utilizând OCR;
- validarea metadescriptorilor asociați la nivel de imagine scanată se va realiza automatizat, pe baza unor reguli de validare, sau manual;
- înregistrarea și rutarea automată a documentelor pe flux în timpul procesului de scanare către compartimentul de destinație;
- fluxuri de scanare multiple și rutarea documentelor pe fluxuri pot fi definite și întreținute vizual, direct în aplicație, fără necesitatea de a scrie cod;
- 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);
- validarea manuală pentru documentele care nu au trecut de extragerea automată a textului și validare acestuia;
- extragerea datelor utilizând OCR full text sau OCR pe zone speciale ale documentelor / zone de document;
- preluare conținut direct din viewer-ul în care este afișat documentul ocr-izat prin drag and drop în medatatele aferente;
- indexarea documentelor pentru căutare rapidă și recuperare prin metadate;

- asigură conversia automata a fișierelor de tip PDF imagine în PDF Searchable la încărcarea în aplicație;
- permite extragerea textului scris de mână pe formulare;
- definirea de template de preluare date din documente OCR-izate pe baza cărora să se preia automat în metadatele sistemului informațiile din documentul supus procesului de OCR cu posibilitatea de definire de chei de validare a conținutului preluat. În cazul în care conținutul preluat nu respectă cheile de validare, documentul respectiv va fi marcat în mod distinct.
- permite salvarea fișierelor de output în format: PDF, PDF/A Searchable, DOCX, JSON.

Funcționalitate de recunoaștere a întrebărilor/documentelor similare

- Sistemul să detecteze automat dacă un document/întrebare introdusă a mai fost primit anterior de la același beneficiar.
- Sistemul va semnala utilizatorului existența documentului anterior și va afișa detaliile relevante (număr de înregistrare, data, statusul).
- Utilizatorul va avea opțiunea de a:
    1. Continua înregistrarea ca document nou.
    2. Marca documentul ca **duplicat** și să îl lege de documentul anterior, evitând duplicarea fluxului.
    3. Casare/archivare automată a documentului, dacă este cazul, cu păstrarea trasabilității și a istoricului în sistem.
- Funcționalitatea trebuie să permită configurarea nivelului de alertă (de exemplu, comparație după text, expeditor, subiect, tip document).

Funcționalitate de alertă și blocare a răspunsurilor către beneficiari cu dosare/procese în curs

Aplicația va asigura că **nu se răspunde automat sau manual unui beneficiar (fermier) dacă există unul sau mai multe situații care impun restricții sau atenție specială**.

Cerințe funcționale:

1. **Identificare situații critice** Sistemul va recunoaște automat orice document/eveniment relevant pentru beneficiar, cum ar fi:
    - Dosare sau procese în curs (inclusiv titluri de creanță, constituire de parte civilă).
    - Blocaje la plată sau alte restricții financiare.
    - Sesizări sau reclamații aflate în proces de soluționare.
2. **Alertă la înregistrarea sau transmiterea răspunsului**
    - La încercarea de a genera un răspuns către beneficiarul respectiv, sistemul va afișa o **alertă clară** pentru utilizator.
    - Alertă va include tipul situației critice, referințele documentelor și statusul procesului.
3. **Blocarea răspunsului**
    - Sistemul va bloca trimiterea răspunsului până când situația critică este soluționată sau aprobată de un responsabil.
    - Posibilitatea ca un utilizator cu drepturi speciale să aprobe trimiterea răspunsului, cu păstrarea evidenței deciziei.
4. **Corelare cu dosarul/beneficiarul**

- Toate documentele, titlurile de creanță, sesizările și blocajele vor fi asociate **unitar cu beneficiarul**, astfel încât sistemul să poată evalua automat riscul sau interdicția de a răspunde.

5. **Trasabilitate și audit trail**
   - Toate acțiunile (alertă, blocare, aprobări speciale) vor fi înregistrate în jurnalul de audit al sistemului.
   - Se asigură evidența completă și verificabilă a motivelor pentru care nu s-a emis răspuns.

Avantaje:

- Evită **erori de comunicare** cu beneficiarii aflați în situații juridice sau financiare sensibile.
- Crește **siguranța decizională** și respectarea procedurilor interne și legale.
- Permite menținerea **trasabilității și responsabilității** în procesul de comunicare.

Protecția datelor cu caracter personal

- asigură anonimizare asupra datelor personale aferente utilizatorilor persoane fizice dar și a persoanelor juridice din cadrul aplicației, în conformitate cu recomandările standardului GDPR;
- asigură pentru fiecare fișier, asocierea a cel puțin următoarelor informații standard de natură GDPR:
  - Categoria de date personale conținută
  - Scopul prelucrării
- asigură o funcționalitate care va procesa automat orice fișier PDF sau Imagine din cadrul aplicației și va determina automat dacă acel document conține date cu caracter personal, precum: copie de buletin sau carte de identitate, copie alt document de identitate;
- să aibă capacitatea sa fie configurat și să învețe să proceseze automat fișiere de tip PDF sau imagine pentru a detecta dacă conține date cu caracter personal prin extragerea automată a textului din fiecare document încărcat în aplicație și căutarea de termeni sensibili din punct de vedere GDPR cum ar fi CNP, adresa etc.
- asigură marcarea fișierelor identificate.

Modulul de registratură electronică

- permite înregistrarea și distribuția de documente curente în format electronic în cadrul organizației, fiind integrat cu celelalte componente ale sistemului, pentru a asigura următoarele funcționalități:
- definirea structurii organizaționale în formă arborescentă;
- definirea de noi tipuri de entități la nivelul structurii organizaționale
- definirea de registraturi multiple;
- definirea de utilizatori cu rol de "registrator" din punctele de intrare / ieșire a documentelor din organizație în vederea înregistrării de documente, cu scopul de a le distribui în interiorul sau în afara organizației;
- înregistrarea documentului va genera acțiunea de a acorda unui document un număr unic de identificare la nivelul organizației, putând fi astfel urmărit în cadrul organizației și în relația cu terții;
- să permită ca numărul de înregistrare sa fie acordat automat în momentul creării unui document în sistem, numai dacă utilizatorul folosește această opțiune;

- aplicația trebuie să permită înregistrarea documentelor și asignarea de număr de înregistrare din orice locație din sistem sunt create, chiar dacă acestea nu sunt create în cadrul registrului;
- să ofere și posibilitatea de a stoca documente fără număr de înregistrare;
- gestionarea centralizată și unicitatea numerelor de înregistrare, pe baza unui sistem de numerotare centralizat la nivelul întregii organizații;
- crearea și gestionarea de registre de către administrator, care pot fi de mai multe tipuri și vor deține serii de numere secvențiale care se vor asocia cu tipuri de documente;
- un registru să poată fi asociat la mai multe tipuri de documente, iar în același timp un tip de document sa poată fi asociat la mai multe registre;
- va gestiona documente de intrare, de ieșire sau informative, oricare dintre acestea putând fi trimise către unul sau mai mulți destinatari;
- să permită fiecărui destinatar, pentru documentele ce necesită rezolvare, crearea de răspunsuri la documentul primit și transmiterea acestora către alte unități organizaționale, inclusiv trimitere automată pe email-ul solicitatului, la finalizarea răspunsului;
- să se poată afișa harta de proces a documentului, care va indica utilizatorii și data la care au primit documentul pentru a furniza rezoluții, precum și statusul la fiecare utilizator;
- crearea și gestionarea de registre de către administrator, care pot fi de mai multe tipuri și vor deține serii de numere secvențiale care se vor asocia cu tipuri de documente. Pentru secvențe se va putea defini prefix, sufix sau pasul secvenței;
- va gestiona documente de intrare, de ieșire sau informative, oricare dintre acestea putând fi trimise către unul sau mai mulți destinatari;
- să permită fiecărui destinatar, pentru documentele ce necesită rezolvare, crearea de răspunsuri la documentul primit și transmiterea acestora către alte unități organizaționale sau pe email, la finalizarea răspunsului;
- configurarea coloanelor care să apară în fiecare registru în funcție de nevoile specifice ale beneficiarului;
- copierea automată a valorilor de pe metadatele documentelor înregistrate în coloanele din registrul în care sunt înregistrate documentele;
- vizualizarea hărții de proces a documentului, care indică utilizatorii, datele de primire și statusul la fiecare utilizator;
- opțiune de resetare automată secvență numere de înregistrare la început de an, pentru fiecare registru în parte;
- importul și exportul configurărilor unui registru;
- sistemul trebuie sa dețină certificare de arhivare electronică cu valoare legală conform legii 135/2007 de la ADR, conform **ORDIN nr. 20.717 din 9 mai 2024 pentru aprobarea Normelor tehnice privind procedura de acreditare a administratorilor de arhivă electronică și procedura de avizare a sistemelor electronice de arhivare sau un echivalent european.**

Modulul fluxuri de lucru

Permite gestiunea proceselor cu documente, asigurând circulația documentelor pe trasee ierarhice sau pre-configurate, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea și circulația informațiilor și a documentelor interne în cadrul organizației, precum și a celor generate în relația cu terți.

Funcționalități:
- definirea și întreținerea vizuală (prin procedeul “drag&drop”), direct în aplicație, a fluxurilor de lucru aplicabile documentelor înregistrate;

- proiectarea fluxurilor de lucru bazate pe organigrama companiei;
- definirea de termene limită pentru fiecare etapă a fluxului de lucru;
- proiectarea fluxurilor de lucru cu sarcini singulare sau sarcini paralele;
- definirea condițiilor de terminare pentru o activitate paralelă;
- definirea de comenzi condiționale în cadrul fluxurilor de lucru;
- definirea variabilelor pentru fluxurile de lucru;
- modificarea cu ușurință a fluxurilor de procese, regulilor și logicii de rutare fără intervenția utilizatorilor IT și fără activități de tip IT, ca instalarea de noi pachete ale aplicației sau modificări în schema bazei de date;
- definirea de tipuri de documente permise pentru fiecare flux de lucru;
- să permită stabilirea declanșării 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;
- programarea unui timp expirare pentru un flux de lucru;
- blocarea editării documentelor după anumite etape a fluxului de lucru;
- grupuri și roluri pentru definirea fluxurilor de lucru;
- definirea și validarea metadatelor ca obligatorii într-o etapă din fluxul de lucru;
- escaladarea automată a pașilor dacă nu există un răspuns într-un anumit interval de timp;
- exportul definiției fluxurilor de lucru în format de tip imagine, pentru a-l putea prezenta spre avizare;
- exportul și importul definiției fluxurilor de lucru într-un format standardizat;
- redirecționarea automată a sarcinilor în cazul în care utilizatorul și-a delegat sarcinile;
- informarea utilizatorilor prin e-mail despre o nouă sarcină primită pe un flux de lucru;
- notificarea utilizatorilor pe e-mail despre o sarcină de efectuat sau neefectuată;
- deschiderea sarcinilor de către utilizatori din notificări primite pe e-mail;
- să permită utilizatorilor să scrie un comentariu la terminarea unei sarcini a unui flux de lucru;
- să permită administratorului să genereze un tabel cu toate fluxurile de lucru și toate informațiile necesare;
- să permită administratorilor să oprească un flux de lucru;
- administrarea de delegări pentru utilizatorii în concediu medical sau de odihnă;
- trimiterea documentelor pe fluxuri de lucru în mod automat în timpul procesului de scanare;
- editarea documentelor de către utilizatorii din fluxul de lucru;
- mutarea automată a fișierului într-un dosar pre-selectat, după o etapă a fluxului de lucru;
- selectarea etapei fluxului de lucru în cazul în care documentul este returnat prin respingere și întoarcerea la etapa anterioară sau în altă etapă a fluxului de lucru;
- selectarea persoanei din grupul de lucru, pentru ca documentele să nu fie trimise întregului grup;
- generarea unui istoric al fluxurilor de lucru pentru utilizatori individuali și întreaga organizație;
- selectarea etapei fluxului de lucru în cazul în care documentul este returnat prin respingere și întoarcerea la etapa anterioară sau în altă etapă a fluxului de lucru;
- selectarea persoanei din grupul de lucru, pentru ca documentele să nu fie trimise întregului grup;
- marcarea separată a operațiunii de începere lucru pe un document, distinct de primire, și contorizarea separată a timpului de când a primit și de când a început lucrul pe document;

- generarea unui istoric al fluxurilor de lucru pentru utilizatori individuali și întreaga organizație;
- marcarea cu culori diferite care să reflecte progresul acestora pe fiecare pas de flux;
- marcarea cu roșu a documentelor respinse de la aprobare;
- semnarea electronică a documentelor la aprobarea pe flux de fiecare utilizator;
- aplicarea opțională de semnături sau ștampile scanate pe documente word și pdf la aprobarea pe flux de fiecare utilizator;
- Utilizatorii vor putea iniția fluxuri ad-hoc de comunicare către mai multe niveluri de aprobare/avizare, având opțiunea de a alege, pe fiecare nivel, mai mulți utilizatori și/sau grupuri de utilizatori din organigramă împreună cu operațiunea aferentă fiecărui nivel: aprobare, avizare, recepție, informare;
- permite definirea de fluxuri de lucru prin interfața vizuală grafică și publicarea de fluxuri fără a necesita modificarea codului sursă și restartarea aplicației;
- permite inițierea de alte fluxuri din fluxul curent;
- permite vizualizarea în format grafic a traseului documentului ilustrând pasul la care s-a ajuns la momentul curent;
- motorul de fluxuri de lucru respectă un standard consacrat în domeniu precum BPMN2 sau echivalent.

Pe durata contractului de implementare a sistemului informatic, Ofertantul devenit Prestator va asigura implementarea și configurarea tuturor fluxurilor de lucru (procese) în cadrul aplicației instalate, în măsura în care aceste fluxuri sunt cunoscute și furnizate de către autoritatea contractantă, conform competențelor exclusive ale acesteia din prezentul proiect.

Rapoarte

Sistemul trebuie să includă integrat un modul de tip business intelligence, în care utilizatorii își pot defini rapoarte custom, direct din aplicație, printr-un configurator vizual, pe bază de opțiuni predefinite, fără a fi nevoie să scrie interogări în baza de date.

Rapoartele standard oferite de către aplicație trebuie:

- Să permită aflarea numărului de documente gestionat de aplicație precum și a dimensiunii acestora, prin punerea la dispoziție a unui set de rapoarte predefinite dintre care:
    - Situația ocupării dispozitivelor de stocare atât per unitate cât și per utilizator;
    - Documente create sau modificate de către utilizatori într-o anumită perioadă.
- Să permită definirea și planificarea livrării rapoartelor de tip alertă pe documente în cadrul sistemului, ca exemplu, dar fără a se limita la: număr de documente nou create în ultima lună pe fiecare tip, documente ce urmează să expire în următoarele 7 zile, număr de documente modificate de fiecare utilizator din departament în ultima săptămână.
- Rapoartele se vor putea livra automat pe email: zilnic/săptămânal/lunar, specificând și ora la care se dorește livrarea acestora împreună cu grupurile de utilizatori sau căsuțele de mail de livrare,
- Eficiența fluxurilor de lucru - Utilizatorul să poată vedea pentru fiecare tip de flux de lucru definit în sistem, durata medie a finalizării acestuia (pe interval selectabile) și durata medie de rezolvare a sarcinilor de lucru pentru fiecare utilizator implicat în flux pentru a se identifica blocajele în procesul de aprobare.
- Rapoartele se vor putea livra în format configurabil de către administrator.

5.8.3. Componenta de business process management (BPM)

Componenta trebuie să ofere funcționalități de automatizare a proceselor de afaceri și să integreze tehnologii pentru a automatiza fluxurile de lucru, în vederea îmbunătățirii eficienței integrării cu alte instituții sau aplicații din infrastructura curentă.
Cerințe funcționale:

- Componenta trebuie să permită coordonarea activităților procesate de utilizatori umani simultan cu activități automate procesate de computer;
- Trebuie să pună la dispoziție un mediu de creare și configurare a aplicației;
- Trebuie să ofere un set de îndrumări sau modele de delegare a activităților manuale;
- Componenta trebuie să ofere posibilitatea de a interacționa cu funcționalitățile de lucru, prin intermediul unei interfețe grafice, vizuale;
- Trebuie să permită standardizarea proceselor, în vederea reutilizării în cadrul unor departamente sau aplicații diferite;
- Pentru administrare, trebuie să pună la dispoziția utilizatorilor, posibilitatea de a optimiza ciclurile de execuție, versionarea proceselor și gestiunea configurărilor de securitate.

Instrumente de proiectare

- Trebuie să permită modelarea și testarea proceselor, într-un mediu unitar.
- Componenta trebuie să ofere o interfață de proiectare a capabilităților de integrare, pentru dezvoltarea serviciilor interne din procese, sau prin adăugarea unor servicii externe (ex: servicii web sau alte aplicații).
- Interfața de proiectare trebuie să fie disponibilă atât prin accesarea unui navigator web, cât și prin intermediul unei aplicații de tip desktop.
- Interfața de proiectare trebuie să permită modelarea, implementarea sau analiza procesului de business.
- Trebuie să permită crearea și gestiunea aplicațiilor, a modelelor, a rapoartelor și a serviciilor în cadrul aceleiași interfețe aplicative.
- Trebuie să permită crearea unei secvențe de acțiuni care compune procesul de business, precum și reproiectarea secvenței, dacă se produc schimbări în timp.
- Dacă una sau mai multe activități din secvență necesită date din alte aplicații, aceste integrări trebuie proiectate în interfața de integrare și preluate în secvența de activități a procesului de business.
- Activitățile din procese trebuie să poată apela serviciile proiectate în interfața de integrare.
- Serviciul de integrare poate utiliza fluxuri de mediere, în vederea transformării, rutării, sau să se conecteze la mai multe sisteme.

Instrumente de integrare

- Prin acest instrument, componenta permite crearea unor procese complexe și servicii (ex: module SCA, procese BPEL).
- Trebuie să fie proiectate având la bază o arhitectură orientate pe servicii – SOA.
- Un serviciu de integrare poate să conțină mai multe servicii de integrare.

Depozit de procese

- Componenta trebuie să ofere un depozit central pentru toate procesele/serviciile de integrare și orice altă componentă creată în mediul integrat de gestiune a proceselor.
- Trebuie să permită salvarea și analiza datelor de performanță referitoare la procesele executate în platformă.

- Trebuie să permită gestiunea procesului colaborativ de lucru, prin configurarea accesului comun la componente, drepturi de acces.

Mediu de execuție
- Componenta trebuie să ofere un mediu de execuție a proceselor centralizat, unic, în vederea execuției proceselor de business, orchestrării proceselor și a capabilităților de integrare.

Federalizare procese de business
- Componenta trebuie să asigure un mediu de procesare federalizată a proceselor la nivelul întregii organizații, pentru a permite utilizatorilor accesarea unei singure liste de task-uri, indiferent dacă în organizație sunt mai multe instanțe, cu medii de execuție separate.

Integrare
- Utilizează inteligența artificială și algoritmi avansați de învățare, pentru a îmbunătăți eficiența și reduce erorile în procesele automate.
- Se integrează nativ cu baze de date precum: Microsoft SQL Server, Oracle sau DB2.
- Permite operarea într-o arhitectură centralizată sau distribuită.
- Suportă rularea în cadrul unei platforme de containere, atât în infrastructura locală, cât și în Cloud.
- Se integrează cu sisteme avansate de securitate, control acces și gestiune a identităților.
- Suportă autentificare Kerberos, LDAP sau autentificare bazată pe utilizator.
- Suportă autorizare Role-Based Access Control (RBAC) sau autorizare bazată pe reguli.
- Oferă criptare AES-256, SSL/TLS sau criptare bazată pe certificat.
- Oferă posibilitatea de a opera volume mari de procese cu un număr mare de utilizatori.
- Oferă caracteristici ridicate de performanță, precum timp de răspuns scăzut la un număr ridicat de cereri, timp de latență scăzut și optimizare a consumului de resurse de prelucrare.

5.8.4. Componenta integrată de gestiune și analiză a datelor

In vederea implementării unei soluții complete pentru organizarea, analiza și managementul datelor, se va avea în vedere o componentă integrata de servicii de date – pentru gestiunea și analiza datelor, care să conțină funcționalități pentru analiza și raportare, tablouri de bord, guvernanta datelor, managementul surselor de date.
Sistemul de gestiune al bazelor de date trebuie să fie un sistem de gestiune a bazelor de date de tip relațional.

Componenta de gestionare a bazelor de date trebuie să îndeplinească următoarele cerințe minime obligatorii:
- trebuie să fie un sistem de gestiune a bazelor de date de tip relațional;
- trebuie să aibă posibilitatea rulării pe arhitecturi cu procesoare pe 64 biți;
- trebuie să permită instalarea bazei de date pe mai multe noduri (arhitectură de tip cluster) pentru a asigura toleranța la căderi de noduri, fără a necesita achiziția de componente adiționale;
- trebuie să aibă posibilitatea definirii de indecși pentru accesarea rapidă a datelor;
- trebuie să aibă posibilitatea stocării datelor în mod tranzacțional;
- trebuie să asigure nivelurile de izolare specifice bazelor de date;

- trebuie să ofere posibilitatea de a face salvare și restaurare automată de date;
- trebuie să includă capabilități de căutare complexă la nivel de text, folosind indecși specializați în efectuarea rapidă a căutărilor în acest tip de date;
- trebuie să ofere posibilitatea stocării datelor mari, păstrând consecvența tranzacțională;
- trebuie să ofere scheme de prioritizare în modul de accesare a bazei de date în funcție de tipul de utilizator;
- trebuie să ofere suport pentru proceduri stocate și triggeri;
- trebuie să permită execuția operațiilor de tip SELECT, INSERT, UPDATE, DELETE;
- trebuie să permită definirea de tabele de tip index și indecși de tip ,,cluster" pentru acces rapid la anumite tabele;
- trebuie să ofere suport pentru folosirea de expresii regulate sau patern-uri de căutare;
- trebuie să permită recuperarea tranzacțiilor aflate în lucru în momentul în care intervine o cădere;
- trebuie să ofere suport Unicode UTF-8 sau echivalent;
- trebuie să ofere suport pentru replicarea bidirecțională a datelor între două instanțe ale bazei de date;
- trebuie să permită restricționarea accesului la nivelul obiectelor bazei de date;
- trebuie să ofere mecanisme de restricționare a accesului utilizatorilor;
- trebuie să permită salvarea/restaurarea precum și arhivarea/dezarhivarea datelor prin intermediul unor instrumente de back-up în regim de lucru online;
- trebuie să ofere suport scalabil și sigur pentru baze de date relaționale.

Din punct de vedere al operațiunilor de administrare, soluția trebuie să ofere mecanisme de monitorizare și diagnosticare continuă, care să pună la dispoziția administratorilor informații pentru ușurarea luării deciziilor în administrare, automatizând colectarea de parametri de funcționare ai bazei de date, precum și stocarea acestora pentru a putea furniza o imagine pe termen lung a modului de funcționare a bazei de date.

Cerințe funcționale:
- Suport pentru instalarea într-o platformă de containerizare, cu funcționalități avansate de gestiune și înaltă disponibilitate a serviciilor componente
- Componenta trebuie să fie accesibilă prin intermediu unui set de instrumente de dezvoltare “low-code/no-code”, instrumente de programare cod sursă, modelare și rulare modele ML/AI.
- Trebuie să includă optimizări specifice, care îmbunătățesc performanța în cazul unor sarcini de lucru complexe și a volumelor mari de date.
- Trebuie să permită scalarea bazei de date, pentru a face față creșterii cererii, fără a compromite performanța.
- Trebuie să ofere mecanisme robuste de control al accesului pentru a proteja datele sensibile.
- Trebuie să ofere funcționalități care să permită respectarea standardelor de securitate și conformitate precum PCI DSS și GDPR.
- Trebuie să ofere un set complet de instrumente pentru monitorizarea, gestionarea și întreținerea bazei de date.
- Trebuie să ofere funcționalități pentru a asigura disponibilitatea continuă a bazei de date, chiar și în cazul unor defecțiuni hardware sau software.
- Trebuie să ofere dezvoltarea de extensii personalizate pentru a satisface cerințele specifice ale aplicațiilor.

Cerințe de Performanță și Scalabilitate

- Trebuie să ofere un modul dedicat, de optimizare inteligentă, care analizează complexitatea interogărilor și generează planuri de execuție eficiente, reducând timpul de răspuns.
- Trebuie să poată executa în paralel multiple operațiuni, precum scanări de tabele, sortări și agregări, îmbunătățind semnificativ performanța pe hardware multi-nucleu.
- Trebuie să ofere un sistemul de indexare automată, care se adaptează la modelele de acces ale datelor, asigurând că sunt utilizate întotdeauna indexurile optime.
- Trebuie să ofere configurații cluster, permițând distribuirea sarcinii pe mai multe servere și scalarea liniară a performanței.
- Trebuie să ofere mecanismele de replicare, care asigură redundanța datelor și permit scalarea citirilor prin adăugarea de replici.
- Trebuie să ofere partiționarea datelor pe baza unor criterii specifice pentru a îmbunătăți performanța interogărilor și a facilita gestionarea datelor mari.
- Trebuie să ofere vederi materializate, pentru stocarea rezultatelor interogărilor complexe, reducând timpul de răspuns la interogările repetitive.
- Trebuie să ofere suport pentru tipuri de date geometrice și funcții spațiale, permițând gestionarea eficientă a datelor geografice.

Cerințe de Securitate și Conformitate
- Trebuie să ofere control granular asupra accesului la date, permițând atribuirea de privilegii specifice fiecărui rol.
- Trebuie să ofere configurarea numărului maxim de conexiuni simultane pentru a preveni atacurile de tip brute-force.
- Trebuie să ofere restricționarea accesului la baza de date doar de la adrese IP autorizate.
- Trebuie să ofere criptarea automată pentru toate datele la nivel de bloc, protejând informațiile confidențiale chiar și în cazul unei compromiteri a serverului.
- Trebuie să ofere securizarea comunicării între client și server, protejând datele în tranzit, prin criptarea conexiunilor SSL/TLS
- Trebuie să protejeze datele stocate pe disc, împiedicând accesul neautorizat.
- Trebuie să înregistreze toate acțiunile utilizatorilor, inclusiv interogări SQL, modificări ale datelor și erori.
- Trebuie să ofere configurarea de alarme pentru evenimente specifice, cum ar fi încercări de autentificare nereușite sau modificări ale configurației.
- Trebuie să ofere identificarea rapidă a anomaliilor și a potențialelor vulnerabilități.
- Trebuie să ofere verificarea integrității datelor și detectarea modificărilor neautorizate prin utilizarea hash-urilor.
- Trebuie să ofere redundanță și disponibilitate ridicată a datelor, prin utilizarea replicării sincrone și asincrone.
- Trebuie să ofere crearea de copii de rezervă regulate pentru restaurarea datelor în caz de dezastru.
- Trebuie să ofere transferul automat al sarcinii către un server de rezervă în caz de defecțiune.
- Trebuie să ofere restricționarea accesului la anumite rânduri dintr-un tabel în funcție de rolul utilizatorului.
- Trebuie să ofere ascunderea informațiilor confidențiale în rezultatele interogărilor.
- Trebuie să ofere eliminarea selectivă a datelor dintr-un set de rezultate.
- Trebuie să ofere utilizarea unor sisteme de autentificare, precum LDAP sau Active Directory.

Cerințe Administrare și Întreținere

- Trebuie să ofere posibilitatea de gestionare a obiectelor din baza de date, vizualizarea planurilor de execuție și monitorizarea performanței prin intermediul unei interfețe grafice.
- Trebuie să ofere un client de linie de comandă puternic pentru interacțiunea cu baza de date.
- Trebuie să ofere un set de instrumente de administrare și dezvoltare specifice, precum un depanator SQL, etc..
- Trebuie să ofere informații detaliate despre utilizarea resurselor, performanța interogărilor și activitatea utilizatorilor.
- Trebuie să ofere configurarea de alerte pentru evenimente specifice, cum ar fi spațiu pe disc insuficient sau utilizare ridicată a procesorului.
- Trebuie să ofere funcționalități care permit identificarea și optimizarea interogărilor cu performanțe scăzute.
- Trebuie sa înregistreze toate activitățile, facilitând depanarea și analiza.
- Mențin statisticile despre datele din tabele, îmbunătățind performanța interogărilor.
- Creează și întreține automat indexuri pentru a accelera accesul la date.
- Trebuie să ofere ajustarea fină a comportamentului serverului pentru a optimiza performanța.
- Trebuie să ofere flexibilitate în crearea de copii de rezervă.
- Trebuie să ofere restaurarea bazei de date la un moment specific din trecut.
- Trebuie să ofere redundanța datelor și permite recuperarea în caz de dezastru.
- Trebuie să ofere instrumente pentru gestionarea creșterii bazei de date și pentru recuperarea spațiului.

Prelucrări analitice de volum

- Componenta trebuie să asigure integrarea cu un cluster Apache Spark;
- Trebuie sa permită crearea mediilor analitice, prin simpla comandă de instalare a mediului;
- Permite rularea de joburi și notebook-uri Jupyter în paralel cu mediul curent;
- Permite rularea de Spark SQL sau alte activități de transformare a datelor, în paralel cu mediul existent.

Simplificarea procesării datelor de volum

- Componenta trebuie să asigure funcționalități de prelucrare a datelor brute de volum ridicat;
- Trebuie să dețină funcționalități de prelucrare și fluxuri de date, care pot transforma volume mari de date brute în date consumabile, de calitate, care se pot utiliza direct în procesele analitice;
- Trebuie să permită descoperirea, analiza, curățarea și transformarea datelor, fără a necesita intervenția programatorilor sau cunoștințe de cod sursă;
- Utilizatorii trebuie să aibă acces la rapoarte, grafice și statistici asupra calității și distribuției datelor;
- Componenta trebuie să ofere detectarea automată a tipurilor de date și a clasificării de business/procese operaționale;
- Componenta trebuie să ofere programarea automată a rulării proceselor de prelucrare a datelor.

Interogarea datelor

- Componenta trebuie să asigure interogarea analitică a datelor, prin intermediul unui motor SQL cloud-nativ și distribuit;

- Componenta trebuie să ofere accesarea mediilor Hadoop, HDFS, Hive, Ranger;
- Componenta trebuie să ofere accesarea și optimizarea interogării surselor deschise de fișiere de date, precum Parquet, ORC, Avro sau CSV.

Confidențialitatea datelor
- Componenta trebuie să ofere mascarea și păstrarea confidențialității datelor, menținând utilitatea și însemnătatea lor, în timpul utilizării în cadrul aplicațiilor;
- Componenta trebuie să ofere definirea și rularea fluxurilor de mascare a datelor;
- Componenta trebuie să ofere configurarea regulilor de protecție a datelor și maparea cu fluxurile de mascare;
- Componenta trebuie să ofere mascarea permanenta a datelor în copia din catalogul centralizat.

Catalog de date
- Componenta trebuie să ofere organizarea și guvernanța datelor;
- Automatizează descoperirea, clasificarea, profilarea și protecția datelor, pentru identificarea și utilizarea rapida a informațiilor;
- Conține și permite definirea de artefacte pentru guvernanta datelor și pentru îmbunătățirea datelor valorificate;
- Componenta trebuie să ofere extinderea setului de proprietăți, relații sau a tipurilor de date referitoare la datele din catalog, prin crearea unor noi proprietăți sau legături.

Depozit de date
- Componenta trebuie să ofere procesarea și depozitarea datelor în memorie sau în depozitul de date;
- Componenta trebuie să ofere suport arhitectural pentru multiprocesarea simetrică SMP sau pentru procesarea paralelă masivă – MPP;
- Componenta trebuie să ofere suport pentru stocarea pe diverse medii de stocare;
- Componenta trebuie să ofere posibilitatea de a gestiona depozitul de date, prin intermediul consolei de administrare dedicate depozitului de date.

De-duplicarea datelor
- Componenta trebuie să asigure agregarea datelor din multiple surse, pentru crearea unei vederi unice asupra entităților de date;
- Componenta trebuie să ofere funcții de tip master pentru datele de tip entități;
- După crearea datelor de tip master, componenta trebuie să ofere funcționalități de decizie pentru măsurarea calității datelor;
- Trebuie să asigure validarea și analiza datelor și a scorului asociat calității, precum și un scor de încredere detaliat, a vederii centralizare;
- Trebuie sa dețină instrumente de identificare a posibilelor probleme de calitate a datelor, să permită crearea de task-uri pentru guvernanța datelor, precum și remedierea acestora.

Orchestrare fluxuri de date
- Componenta trebuie să asigure crearea unui flux complet de prelucrare a datelor, în vederea utilizării analitice sau în algoritmi de învățare automată, de la crearea modelelor, până la adaptarea acestora prin intermediu unor funcții dedicate;
- Componenta trebuie să ofere crearea, rularea și monitorizarea fluxurilor prin intermediul unui instrument grafic și care permite adaptarea scripturilor Python în cadrul fluxurilor sau utilizarea unor noduri predefinite în editor;
- Trebuie să permită orchestrarea fluxurilor, de la colectarea datelor, executarea scripturilor, antrenarea modelelor, până la stocarea rezultatelor;

- Să permită configurarea și programarea unor job-uri care să ruleze automat și care să efectueze schimbări ale condițiilor din nodurile fluxurilor.

Generare date sintetice
- Componenta trebuie să asigure crearea de date sintetice, fie prin amestecarea datelor existente concomitent cu generarea de date noi, fie prin generarea de date fără o sursă inițială de informații;
- Modelarea fluxului de generare a datelor sintetice trebuie să ofere capabilități de generare sintetică, bazate pe algoritmi statistici sau pe modele de învățare automată;
- Operarea funcționalităților trebuie să se facă într-un mod vizual, prin intermediul unui instrument grafic, care permite proiectarea fluxurilor de generare a datelor sintetice.

Învățare automată
- Componenta trebuie să asigure instrumentele necesare proiectării, antrenării și instalării în producție a modelelor de învățare automată;
- Proiectarea modelelor trebuie să se poată face prin intermediul unei interfețe grafice, în mod vizual, pentru tot ciclul de viață, de la proiectare la instalare în producție, dar și prin intermediul unui mediu de dezvoltare cu cod sursă;
- Trebuie să dețină capabilități similare Automated machine learning (AutoML)/AutoAI (AI automatizat). Este o tehnologie care automatizează procesul de construire și implementare a modelelor AI care permite de la experimentarea utilizării modelelor de învățare automată, până la generarea modelor și a fluxurilor de modelare. Modelele și fluxurile trebuie să poată fi salvate pe baza propunerilor automate de model-candidat.
- Trebuie să permită utilizarea funcționalităților într-un mediu de dezvoltare și programare de tip notebook, cu cod sursă, care să îmbine utilizarea datelor cu testarea modelelor, pentru realizarea de prototipuri rapide;
- Componenta trebuie să dețină capabilități de învățare avansată, pentru experimentarea automatizării unor fluxuri multiple de antrenare, urmărire și stocare a rezultatelor;
- Pentru pregătirea modelelor de producție, componenta trebuie să ofere spații de lucru dedicate, care să permită vizualizarea și managementul modelelor;
- Procesul de pregătire și învățare a modelelor trebuie să permită accesul federalizat la surse de date disparate sau chiar deconectate. Sursele federalizate pot contribui la crearea unui model de învățare automată, fără a compromite securitatea datelor sau a modelului;
- Componenta trebuie să asigure instrumente de gestiune și control al modelelor de învățare automată.

Transparența modelelor
- Componenta trebuie să dețină funcționalități de monitorizare a încrederii și a transparenței modelor de învățare automată, prin înțelegerea și trasabilitatea modului în care acestea prelucrează decizii;
- Componenta trebuie să asigure funcționalități de detectare și mitigare a bias-urilor;
- Componenta trebuie să poate opera și modele externe, deschise, importate în platformă.

Guvernanța modelelor
- Componenta trebuie să asigure organizarea și urmărirea evenimentelor, în vederea creșterii transparenței și a guvernanței modelelor;

- Trebuie să permită crearea unui depozit central de modele disponibile și a parametrilor pentru monitorizare;
- Trebuie să permită captarea și urmărirea meta-datelor specifice modelelor, în întregul ciclu de viață, de la creare până la utilizarea în medii de producție;
- Asigură trasabilitatea evenimentelor și a acțiunilor, de la crearea modelului la utilizarea în producție.

Medii integrate de dezvoltare
- Componenta oferă un mediu dedicat de dezvoltare pentru limbajul R, care să permită reutilizarea scripturilor R existente în APIA, precum și dezvoltarea tehnicilor statistice, precum modelarea liniară și neliniară, execuția testelor statistice clasice, analize pe serii de timp și/sau clasificări;
- Componenta oferă instrumente care permit crearea de notebook-uri și experimentarea modelelor, în cadrul proiectelor analitice.

Componenta de modelare, antrenare și inferența a modelelor generative
- Componenta trebuie să ofere funcționalități avansate de analiză a datelor, prin utilizarea modelelor generative.

Cerințe funcționale pentru analiza datelor:
- Componenta trebuie să pună la dispoziție instrumente de prelucrare a datelor și modelare AI
- Componenta trebuie să ofere rularea în cadrul platformelor de gestiune a containerelor, în infrastructura locală;
- Componenta trebuie să ofere experimentarea modelelor generative, îmbunătățirea modelelor fundaționale și scrierea aplicațiilor care utilizează modele generative în limbaj Python;
- Componenta trebuie să ofere integrarea cu modele generative proprii dar și cu modele deschise, precum Meta Llama 3, Mistral AI sau similare din categoria „large language model (LLM);
- Componenta trebuie să pună la dispoziția utilizatorilor un mediu integrat, accesibil prin interfața grafică, pentru experimentare a prompt-urilor;
- Componenta trebuie să vină integrată cu șabloane/exemple de prompt-uri, pentru interogarea modelelor generative;
- Trebuie să permită salvarea prompt-urilor sub formă de șabloane, pentru utilizarea ulterioară sau partajarea în cadrul echipelor de lucru;
- Textul prompt-urilor, referința la model și parametrii prompt-ului trebuie să fie salvate și formatate în cod Python, într-un notebook, în vederea utilizării la nivel programatic;
- Componenta trebuie să ofere un mediu de tip ‘studio’, pentru reglarea modelelor generative, în vederea îmbunătățirii răspunsului acestor modele (fine tuning);
- Componenta trebuie să ofere o viziune completă asupra trasabilității datelor, de la sursa inițială de date utilizată pentru antrenare până la explicarea rezultatului final, produs de modelul generativ;
- Componenta trebuie să ofere conexiuni multiple la o varietate de API-uri, SDK-uri sau biblioteci;
- Componenta trebuie să ofere simplificarea dezvoltării proceselor generative, prin utilizarea unui flux de gestiune natural;
- Componenta trebuie să pună la dispoziția utilizatorilor:
    - fluxuri predefinite de RAG (Retrieval-Augmented Generation - tehnică care îmbunătățește acuratețea și fiabilitatea modelelor AI generative, cum ar fi modelele lingvistice mari (LLM), permițându-le să acceseze și să încorporeze informații relevante din baze de cunoștințe externe) sau

sumarizare, care permit utilizatorilor integrarea nativă în procesele de business;
    - fluxuri predefinite de clasificare, extragere și evaluare a sentimentului din text;
    - fluxuri de extragere, identificare nume entități, termeni sau condiții.
- Componenta trebuie să ofere un mediu interactiv de creare automată a fluxurilor de prelucrare și generare a modelelor;
- Componenta trebuie să ofere rapoarte de analiză pentru îmbunătățirea deciziilor, planificare, programare și analiză a costurilor;
- Componenta trebuie să ofere un motor de analiză decizional, care poate transpune decizii de business în formule matematice.

5.8.5. Componenta de analiză și raportare avansată a datelor

Componenta trebuie să asigure analiza datelor, prin conectarea la multiple surse de date, pentru analiza și vizualizarea datelor. Pune la dispoziție capabilități de analiză predictivă, inclusiv modelare predictivă, forecasting și suport decizional.

Specificații funcționale:

Interfața utilizator
- Componenta trebuie să ofere utilizatorilor, indiferent de rolul acestora, accesul la aplicație printr-un singur punct de acces, interfața de tip portal, atât pentru dispozitive desktop, cât și pentru dispozitive mobile;
- Aplicația portal trebuie să permit accesul centralizat, din care se poate naviga către aplicațiile specifice pentru raportare sau administrare;
- Componenta trebuie să ofere administratorilor posibilitatea de a gestiona utilizatorii în funcție de rolul din organizație sau permisiuni acces specifice;
- Componenta trebuie să ofere posibilitatea de a oferi acces anonim pentru utilizatorii care nu sunt autentificați;
- Utilizatorii pot avea drept de acces la mai multe spații de lucru, în aceeași sesiune, în care trebuie să se conecteze cu credențiale specifice;
- Componenta trebuie să ofere o viziune completă, la prima autentificare în sistem, asupra conținutului din aplicație, asupra fișierelor de date încărcate manual, pentru analiză;
- Componenta trebuie să ofere posibilitatea ca utilizatorii să navigheze prin fișiere, directoare, rapoarte, tablouri de bord sub forma unor vederi predefinite;
- Trebuie să ofere o interfață de căutare în toate fișierele sau rapoartele definite, la care utilizatorii au acces, inclusiv în tabele sau nume coloane – pentru sursele de date.

Securizarea informației
- Componenta trebuie să permită configurarea accesului utilizatorului la anumite acțiuni, funcționalități sau obiecte din aplicație;
- Administratorii componentei, trebuie să poată combina permisiunile specifice unui utilizator, cu permisiunile unui grup și roluri din grupurile din care utilizatorul face parte;
- Pentru controlul accesului – componenta trebuie să permită configurarea permisiunilor;
- Componenta trebuie să suporte configurarea accesului specific la rapoarte, tablouri de bord, pachete.

Surse de date

- Componenta trebuie să asigure integrarea și accesul la module de date, pachete, seturi de date sau fișiere de date – pentru încărcarea informațiilor în vederea exploatării analitice.

Explorarea datelor
- Componenta trebuie să permită explorarea informațiilor plecând direct din modul de vizualizare (ex: din tabloul de bord);
- Trebuie să permită explorarea datelor plecând de la o sursă de date existentă sau care poate fi adăugată în analiză.

Raportare
- Componenta trebuie să ofere un spațiu dedicat pentru conținutul de tip rapoarte, organizat sub forma unui fișier virtual, accesibil prin intermediu interfeței web;
- Trebuie să permită rularea unui raport și variații ale acestuia, în funcție de variabile, valori, preluate din consola/mod prompt;
- Utilizatorii trebuie să poată vizualiza raportul curent, cu ultimele date din sursa de date, sau pot accesa versiuni de rapoarte salvate anterior;
- Oferă posibilitatea de a proiecta, vizualiza sau de a analiza structura vizuală pentru raportul final;
- Utilizatorii pot configura formatul vizual pentru fiecare raport și adăuga componente specifice, precum liste, grafice sau hărți;
- Componenta oferă modele de rapoarte și posibilitatea de a adăuga modele specifice unor nevoi pentru fiecare tip de raport – pe care utilizatorii le pot prelua ca model pentru un nou raport;
- Trebuie să permită adăugarea surselor de date la un raport existent;
- Permite afișarea și adăugarea în raport a unui singur rând din sursa de date;
- Componenta oferă posibilitatea de a configura rapoarte care să își facă refresh automat, la un interval de timp;
- Oferă posibilitatea de a valida rapoartele, pentru a asigura lipsa erorilor.

Tablouri de bord
- Utilizatorii trebuie să poată agrega diverse sub-componente vizuale, precum tablouri de bord cu rapoarte, grafice, în cadrul aceleiași analize;
- Tablourile de bord trebuie să permită configurarea parametrilor și analiza de adâncime (driling-up și drilling-down);
- Trebuie să permită crearea de secvențe analitice sub forma unor slide-uri, care să se deruleze automat.

Scop: să ai o imagine de ansamblu asupra datelor relevante într-un singur loc, fără să schimbi fereastra sau modulul.

Conectare, colaborare echipe de lucru, integrare
- Pe lângă conectarea la surse de date, componenta se poate conecta pentru preluarea sau livrarea de date direct către aplicații precum Jupyter Notebook;
- Componenta trebuie să permită conectarea la aplicații de colaborare, precum Slack sau Teams – pentru a permite distribuirea rapoartelor către alți utilizatori;
- Permite integrarea avansată cu soluții de colaborare prin posibilitatea de a expune mediul componentei în interfața soluției de colaborare;
- Permite integrarea avansată cu soluții de gestiune a guvernanței;
- Permite integrarea avansată cu soluții de productivitate, precum Microsoft Office;
- Oferă o interfață pentru echipamente mobile, tablete și telefoane, de accesare a rapoartelor și a tablourilor de bord, posibilitatea a analiza separata accesul mobil

la informații, proiectarea și publicarea de rapoarte specifice pentru interfața mobilă;
- Suportă integrarea nativă cu aplicații pentru modelarea și antrenarea modelelor de ML/AI;
- Oferă suport pentru rularea în infrastructura clientului, cloud AWS, Azure, GCP, în containere sau mediu virtualizat.

5.8.6. Componenta de integrare și pregătire a datelor (ETL)

Componenta de integrare și pregătire a datelor asigură funcționalități de proiectare și executare a unor procese de transformare și curățare a datelor, pentru a pregăti datele spre analize simple, în cadrul rapoartelor, sau utilizarea lor în procese de analiză avansată. O caracteristică importantă a componentei este capabilitatea de a rula în mod paralel, simultan, o serie de procese de încărcare, transformare și curățare a datelor. Funcționalitățile disponibile utilizatorilor trebuie să fie accesibile prin intermediul unei interfețe vizuale, într-o manieră low code/no code, pentru a facilita utilizarea și de către persoane care nu dețin cunoștințe tehnice.

Cerințe:
- Componenta trebuie să asigure, prin intermediul unor conectori, conectarea la diverse surse de date, precum baze de date relaționale, platforme big-data sau aplicații disponibile în cloud. De asemenea trebuie să permită instalarea în mediul clientului fie în mediu virtualizat, mediu containerizat sau în mediu cloud.
- Trebuie să permită pregătirea datelor în vederea exploatării analitice, prin funcționalități dedicate etapelor de ingestie, transformare, prelucrare a calității datelor și livrare de date, de la / către alte surse de date.
- Pune la dispoziție un motor de transformare a datelor din surse multiple, pentru standardizare, cu suport pentru maparea, formatarea, agregarea și normalizarea datelor;
- Pentru identificarea și corectarea erorilor din date, precum date lipsă sau informații duplicate, componenta trebuie să asigure acuratețea, completitudinea și consistenta datelor.
- Componenta trebuie să ofere funcționalități pentru încărcare, streaming și publicare a datelor, în diverse destinații precum: baze de date, Data Warehouse, Datalake sau alte aplicații disponibile în Cloud.
- Oferă posibilitatea de a clasifica date sensibile și accesul la ele, doar pentru persoanele autorizate.
- Suportă integrarea cu surse și date de volum mare, precum Hadoop, Spark și baze de date NoSQL.
- Se integrează cu aplicații în cloud, precum și cu alți producători de soluții în cloud: AWS și Azure.
- Oferă funcționalități de virtualizare a datelor, prin crearea de view-uri din surse de date diverse, incluzând baze de date relaționale, platforme big-data, aplicații în cloud.
- Pentru depozitele de date specializate pe departamente sau nevoi de business, componenta oferă capabilități de a crea datamart-uri pentru raportare și analitice.
- Componenta oferă o interfață vizuală, cu funcționalități de drag-and-drop, pentru crearea de flux-uri ETL pentru transformarea și livrarea datelor prelucrate.
- Oferă capabilități de trasabilitate a datelor (data-lineage) pentru a trasa originea, procesarea și livrarea datelor intre sursa originala și destinația finală.

- Componenta trebuie să dețină încorporate metrici de analiză a calității datelor, pentru a măsura acuratețea și completitudinea datelor și trebuie să permită recomandarea de măsuri corective sau măsuri de îmbunătățire a metricilor.
- Componenta trebuie să dețină încorporate metrici de analiză a guvernanței datelor, pentru a măsura eficacitatea și eficiența politicilor și a procedurilor specifice organizației.
- Componenta trebuie să dețină încorporate metrici de analiză a catalogului de date, pentru a măsura eficiența și a identifica arii de îmbunătățire a modului de clasificare și identificare a datelor.
- Componenta trebuie să dețină încorporate metrici de analiză a trasabilității datelor (data-lineage), pentru a măsura eficienta și auditul trasabilității datelor.

5.8.7. Componenta de interoperabilitate

Componenta de integrare trebuie să ofere un set cuprinzător de capabilități de integrare pentru a conecta aplicații și date în medii hibride și multi-cloud.
Cerințe minime:

- Pentru integrare aplicații și date, componenta trebuie să dispună de API Management și gateway, Enterprise Service Bus (ESB), Messaging și event streaming, File transfer securizat și Transformare și rutare de date.
- Arhitectură cloud native Kubernetes cu instalare flexibilă bazată pe microservicii și containere cu scalare automată bazată pe cerere.
- Permite dezvoltare low-code sau no-code pentru integrări rapide.
- Mediu de dezvoltare unificat pentru productivitate și eficiență maximă.
- Suport nativ pentru CI/CD și DevOps.
- Monitorizare și jurnalizare centralizată pentru vizibilitatea completă și diagnosticarea rapidă a infrastructurii.
- Suport extins pentru multiple protocoale, asigurând conectivitate universală.
- Streaming de evenimente în timp real pentru decizii prompte și acțiuni imediate.
- Comunicare flexibilă prin publish/subscribe și point-to-point messaging.
- Adaptoare pre-construite pentru sisteme comune;
- Motor avansat de transformare a datelor și rutare inteligentă care automatizează conversia formatelor și direcționarea optimă a mesajelor în funcție de conținut și reguli de business.
- Orchestrare inteligentă a proceselor de business.
- Tratare automată a excepțiilor și recuperare pentru fiabilitate maximă.
- Transferuri rapide și eficiente pentru volume mari de date.
- Compresie și criptare integrată pentru transfer securizat.
- Permite urmărirea performanței infrastructurii IT și generarea de rapoarte privind disponibilitatea și timpul de răspuns al sistemelor.
- Recomandări inteligente pentru mapări de date și transformări automate.
- Detectare proactivă a anomaliilor pentru fiabilitate maximă în integrări.
- Monitorizare și auditare detaliată a tuturor fluxurilor de date.
- Management avansat al politicilor de securitate pentru control granular.
- Vizualizare interactivă completă a fluxurilor de integrare.
- Debugging distribuit pentru identificarea și rezolvarea rapidă a problemelor.
- Analitică avansată pentru optimizarea continuă a performanței.
- Sistem inteligent de scalare automată pentru toate componentele, care ajustează dinamic resursele în funcție de cererea în timp real, asigurând performanță optimă și eficiență a costurilor în întreaga infrastructură.
- Capabilități avansate de high availability și disaster recovery.

- Managementul întregului ciclu de viață API, de la creare și publicare până la monitorizare și depreciere, incluzând versionare, securizare, documentare și analitică pentru optimizarea continuă a serviciilor.
- Gateway API robust și securizat care oferă funcționalități avansate de rate limiting, caching inteligent și control granular al securității, asigurând performanța, disponibilitatea și protecția optimă a serviciilor expuse.
- Portal comprehensiv pentru dezvoltatori care oferă documentație interactivă, mediu sandbox pentru testare, exemple de cod și API Explorer, facilitând adoptarea rapidă și experiența optimă de dezvoltare.
- Sistem avansat de versionare API și management al schimbărilor care asigură evoluția controlată a serviciilor, cu suport pentru multiple versiuni active, migrări transparente și backward compatibility pentru integrări existente.
- Platformă avansată de monetizare API care oferă modele flexibile monitorizare granulară bazată pe consum, și raportare detaliată.
- Informații analitice pentru API-uri, care oferă vederi complete despre pattern-urile de utilizare, performanță, latență și comportamentul consumatorilor, facilitând optimizarea continuă și decizii informate bazate pe date.
- Suport pentru messaging persistent și non-persistent pentru gestionarea mesajelor cu garanții de livrare pentru date critice și procesare optimizată pentru comunicare în timp real.
- Suport pentru protocoale comune de messaging (AMQP, MQTT, JMS, Kafka), asigurând interoperabilitate maximă și flexibilitate în integrarea cu diverse sisteme și aplicații din ecosistemul companiei.
- Event streaming pentru procesare și analiză în timp real a fluxurilor de evenimente, suportând volume mari de date și oferind capabilități de filtrare, transformare și agregare pentru decizii instant.
- Comunicare asincronă care suportă atât modelul publish/subscribe cât și comunicare point-to-point pentru scenarii dedicate, asigurând scalabilitate și decuplare optimă între componente.
- Scalare automată care monitorizează și răspunde în timp real la fluctuațiile volumului de mesaje, ajustând dinamic resursele pentru a menține performanța optimă și a preveni blocajele în procesarea mesajelor.
- Suport extins pentru protocoale comune de comunicare și formate de date (REST, SOAP, GraphQL, JSON, XML, AVRO), asigurând interoperabilitate maximă și flexibilitate în integrarea cu orice tip de sistem sau aplicație
- Mecanism avansat de tratare a excepțiilor, cu jurnalizare detaliată, care capturează și documentează automat toate erorile, oferind context complet, trasabilitate și informații diagnostice pentru rezolvarea rapidă a problemelor.
- Pattern-uri de integrare predefinite pentru dezvoltare rapidă și eficientă.
- Sistem pentru transferul rapid și sigur al fișierelor de mare dimensiune, cu optimizări pentru throughput maxim, compresie inteligentă și transfer paralel, asigurând mișcarea eficientă a volumelor mari de date.
- Protecția datelor prin criptare avansată, atât în tranzit cât și în repaus, utilizând algoritmi de ultimă generație și management securizat al cheilor pentru asigurarea confidențialității în toate stadiile procesării informației.
- Compresie automată a datelor care optimizează în timp real raportul între dimensiune și performanță, selectând dinamic algoritmii optimi în funcție de tipul conținutului și cerințele de transfer.
- Mecanism inteligent de reîncărcare și recuperare automată care asigură continuitatea operațiunilor prin reluarea controlată a proceselor eșuate și recuperarea din erori.
- Sistem avansat de autentificare și autorizare granulară bazat pe roluri (RBAC), asigurând control precis asupra accesului la resurse și funcționalități.

- Integrare nativă cu sisteme de management al identității (Active Directory, LDAP, SSO), oferind autentificare centralizată, management unificat al identităților și control granular al accesului bazat pe roluri.
- Criptare completă robustă care asigură protecția completă a datelor pe întregul circuit informațional, de la sursă până la destinație, utilizând algoritmi avansați de criptare și management securizat al cheilor pentru confidențialitate maximă.
- Sistem de auditare și logging care înregistrează și monitorizează toate operațiunile și evenimentele sistemului, oferind trasabilitate completă și istoricul detaliat al activităților pentru conformitate și investigații de securitate.
- Conformitate nativă și certificată cu standardele majore de securitate și reglementări (minim GDPR), implementând automat controalele necesare pentru protecția datelor, confidențialitate și guvernanță conform cerințelor specifice fiecărui standard.
- Sistem avansat de management al certificatelor și cheilor criptografice, cu suport pentru generare, rotație automată, revocare și distribuție securizată, asigurând gestionarea completă a ciclului de viață al credențialelor de securitate.
- Tablouri de bord unificate care oferă vizibilitate completă asupra componentelor sistemului, cu monitorizare în timp real, metrici personalizabile și vizualizări interactive pentru luarea rapidă a deciziilor operaționale.
- Monitorizare în timp real a performanței sistemului, oferind vizibilitate instantanee asupra metricilor critice, detecție automată a anomaliilor și alertare proactivă pentru optimizarea continuă a performanței operaționale.
- Sistem flexibil de alertare cu notificări complet configurabile, permițând definirea precisă a pragurilor, condițiilor și canalelor de comunicare, cu suport pentru escaladare automată și rutare inteligentă a alertelor în funcție de severitate și context.
- Sistem avansat de trace-uri distribuite care oferă vizibilitate completă asupra fluxurilor de execuție, permițând urmărirea și diagnosticarea precisă a problemelor în arhitecturi complexe prin colectarea și corelarea informațiilor de debugging din toate componentele.
- Sistem avansat de analitică predictivă care identifică proactiv potențiale probleme, analizează pattern-uri comportamentale și generează alerte preventive pentru evitarea incidentelor înainte de a impacta operațiunile.
- Consolă centralizată de administrare care oferă control unificat asupra tuturor aspectelor sistemului, cu interfață intuitivă și acces rapid la funcționalități de configurare, monitorizare și management din punct unic de control.
- Permite automatizarea taskurilor administrative care elimină operațiunile manuale repetitive, orchestrează procese complexe și optimizează eficiența operațională prin fluxuri predefinite și reguli de automatizare inteligente.
- Backup și restore pentru configurații care asigură salvarea automată, versionarea și recuperarea rapidă a setărilor sistemului, cu capacități de rollback și restore point-uri pentru management sigur al schimbărilor.
- Management al resurselor și capacității care optimizează automat alocarea și utilizarea resurselor, oferind planificare predictivă, monitorizare în timp real și ajustare dinamică pentru eficiență operațională maximă.
- Suport nativ pentru standarde și protocoale de industrie (REST, SOAP, GraphQL, OpenAPI, MQTT, AMQP), asigurând interoperabilitate maximă și integrare flexibilă.
- Performanță ultra-rapidă în procesarea mesajelor cu latență garantată sub milisecundă, asigurând transmiterea instantanee a datelor critice și comunicare în timp real pentru aplicații cu cerințe stricte de performanță.
- Sistem inteligent de auto-scalare care analizează simultan multiple metrici (CPU, memorie, throughput, latență) pentru a lua decizii optimizate de scalare, asigurând performanța și eficiența resurselor în orice condiții de încărcare.

- Sistem inteligent de balansare automată a încărcării care distribuie dinamic și optimal încărcările între resurse disponibile, asigurând utilizare echilibrată, performanță constantă și reziliență maximă în condiții variabile de trafic.
- Motor inteligent de sugestii pentru mapări de date care utilizează ML pentru a recomanda automat transformări și corelații optime între câmpuri, accelerând procesul de integrare și reducând erorile de mapare.
- Sistem inteligent de detectare automată a anomaliilor bazat pe algoritmi avansați de ML, care identifică proactiv pattern-uri neobișnuite și deviații de la comportamentul normal, permițând intervenția rapidă înainte ca problemele să escaladeze.
- Sistem inteligent de optimizare a rutării, care selectează și ajustează dinamic cele mai eficiente căi de transmitere a datelor, bazându-se pe analiza în timp real a condițiilor de rețea, latență și încărcare pentru maximizarea performanței.
- Sistem inteligent de auto-healing care detectează, diagnostichează și remediază automat problemele comune, implementând acțiuni corective predefinite și mecanisme de recuperare pentru minimizarea timpilor de nefuncționare și reducerea intervenției manuale.
- Rapoarte predefinite și personalizabile adaptate pentru fiecare rol organizațional, oferind vizibilitate specifică și relevantă asupra metricilor cheie și KPI-urilor importante pentru diferite categorii de utilizatori.
- Permite configurarea și personalizarea completă a vizualizărilor, metricilor și formatelor de raportare, oferind flexibilitate maximă în generarea de vederi relevante pentru orice necesitate de business.
- Capacități comprehensive de export al datelor în multiple formate standard de industrie (CSV, JSON, XML, Excel, PDF), asigurând compatibilitate maximă și facilitând integrarea cu diverse sisteme și instrumente de analiză.
- Rapoarte care oferă detalii despre pattern-urile de utilizare și metricile de performanță, combinând analize în timp real cu predicții și recomandări pentru optimizarea continuă a sistemului.
- Permite vizualizări interactive care transformă date complexe în reprezentări grafice intuitive și explorabile, permițând analiza detaliată prin drill-down dinamic, filtrare contextuală și perspective multiple asupra informațiilor.

Soluția pentru identificarea și blocarea atacurilor și consolidarea securității la nivelul API-urilor.

- Soluția trebuie să determine cu precizie numărul total de API-uri disponibile în cadrul sistemului.
- Soluția trebuie să descopere și să documenteze automat structura tuturor punctelor finale API, inclusiv metode, parametri de sarcină, parametri de interogare și tipul lor de date, fără configurare manuală.
- Soluția trebuie să folosească tehnici de descoperire activă, imitând tacticile de recunoaștere ale atacatorilor API pentru a identifica și valida punctele finale API expuse.
- Soluția trebuie să permită utilizatorilor administrativi să adauge și să configureze clasificări și categorii personalizate de date sensibile, care vor fi aplicate automat la învățarea API.
- Soluția trebuie să ofere scorul de risc pe endpoint-urile API pentru a evidenția zonele cu risc ridicat. Scorul de risc trebuie să se bazeze pe protocol, autentificare, expunere la date sensibile și să poată fi personalizat.
- Soluția trebuie să identifice și să raporteze automat toate datele sensibile/PII din punctele finale API și locațiile lor specifice, inclusiv identificarea datelor sensibile din cerere și răspuns.

- Soluția trebuie să poată aplica un hash unidirecțional datelor sensibile ale dashboard-ului, prevenind expunerea informațiilor brute analiștilor SOC în timpul investigațiilor.
- Soluția trebuie să poată identifica API-urile "zombie" (de exemplu, al căror volum de trafic a scăzut semnificativ recent).
- Soluția trebuie să aibă capacitatea de a personaliza și grupa API-uri similare pentru o mai bună vizibilitate și raportare.
- Soluția trebuie să poată identifica și bloca atacatorii (persoana care generează traficul API rău intenționat) și nu anomalii individuale disparate.
- Soluția trebuie să afișeze toate caracteristicile atacatorului (de exemplu, ip, token, identificator de utilizator, chei API, locație geografică) în dashboard pentru a simplifica investigarea și remedierea.
- Soluția trebuie să fie capabilă să coreleze și să asocieze activități dispersate cu un singur utilizator, în ciuda eforturilor atacatorilor de a utiliza diferite ID-uri, adrese IP și dispozitive pentru a-și propaga atacurile.

Guvernanța posturii și reducerea riscurilor

Guvernanța posturii API se referă la procesul de supraveghere și gestionare a securității, conformității și stării generale a API-urilor (interfețe de programare a aplicațiilor) pentru a se asigura că acestea sunt configurate, monitorizate și protejate corect împotriva potențialelor vulnerabilități și riscuri.

- Soluția trebuie să permită API public pentru a exporta periodic inventarul activelor API într-o platformă centralizată de gestionare a activelor.
- Soluția trebuie să permită notificări atunci când sunt descoperite noi active API și noi puncte finale.
- Soluția trebuie să permită etichetarea personalizată a punctelor finale API, eficientizând organizarea și raportarea și să permită gruparea cu ușurință a API-urile după proprietar, funcție sau versiune, pentru o vizibilitate îmbunătățită.
- Soluția trebuie să folosească un API pentru gestionarea cuprinzătoare a etichetelor pentru a eficientiza fluxurile de lucru de securitate și automatizarea.
- Soluția trebuie să aibă capacitatea de a utiliza o filtrare complexă.
- Soluția trebuie să permită ca filtrele avansate să poată fi salvate pentru a oferi o perspectivă imediată asupra diferitelor părți interesate. (Arhitect, SecOps, AppSec etc.)
- Soluția trebuie să permită organizațiilor să definească și să aplice propriile standarde de securitate, asigurându-se că toate API-urile respectă politicile interne și cele mai bune practici din industrie.
- Soluția trebuie să aibă un motor robust de guvernanță a posturii care să ofere un set de reguli de bune practici gata de utilizare.
- Soluția trebuie să aibă capacitatea de a crea reguli complexe, compuse, care aderă la cadrele de guvernanță existente, inclusiv PCI, PSD2, NIST și altele.
- Soluția trebuie să permită clasificarea și filtrarea regulilor de guvernanță a posturii pentru a se concentra doar pe regulile relevante pentru un anumit user.
- Soluția trebuie să monitorizeze continuu API-urile pentru respectarea regulilor de postură și să ridice alerte cu privire la orice abateri sau potențiale riscuri de securitate.
- Soluția trebuie să permită identificarea de riscuri în inventarul API și crearea de reguli Posture Gap pentru a identifica și monitoriza API-urile riscante.
- Soluția trebuie să aibă capacitatea de a rula fluxuri de lucru automate de remediere pe alertele Posture Governance care se leagă de Jira, ServiceNow, Splunk și alte sisteme.

- Soluția trebuie să poată aplica regulile existente Posture Gap API-urilor de pre-producție pentru a identifica riscurile și a aplica standardele de codare înainte ca un API să ajungă în producție.
- Soluția trebuie să ofere un hub centralizat de bune practici de securitate actualizate continuu (de exemplu, protecția autentificării) și să pună la dispoziție cele mai recente îndrumări pentru protecția activelor.

Raportare și management

- Soluția trebuie să permită utilizatorilor să genereze rezumate detaliate ale atacatorilor, eficientizând procesul de triere prin reducerea semnificativă a timpilor de investigație și facilitând luarea deciziilor mai rapide și mai informate.
- Soluția trebuie să permită corelarea amenințărilor atacatorului într-o singură vizualizare, nu prin tranzacții individuale sau anomalii, pentru a reduce timpul mediu de rezolvare.
- Soluția trebuie să fie capabilă să ridice alerte în cazul unor utilizatori rău intenționați și nu pentru toate anomaliile care pot apărea.
- Soluția trebuie să permită clasificarea severității vulnerabilităților API descoperite.
- Soluția trebuie să ofere alerte în timp real care conțin toate informațiile necesare pentru înțelegerea incidentului, inclusiv identificatorul atacatorului (IP, token etc.), endpoint-urile API, tipul de atac, cronologia atacului, solicitarea completă și informațiile de răspuns, numărul de încercări, data și ora exactă și contextul.
- Soluția trebuie să ofere informații continue de remediere bazate pe activitatea rău intenționată și să le prezinte împreună cu informații despre activitatea normală.
- Soluția trebuie să ofere posibilitatea unor acțiuni automate de urmărire ca răspuns la un eveniment de securitate (de exemplu, trimiterea IP-urilor pentru a fi blocate într-un WAF; trimiterea evenimentelor către SIEM; definirea webhook-ului pentru sistemul intern etc.).
- Soluția trebuie să permită identificarea automată a celor mai critice puncte finale, permițând alocarea de resurse și prioritizarea remedierilor pe cele mai vulnerabile API-uri.
- Soluția trebuie să permită ca scorurile de risc să poată fi reglate de utilizator prin ajustarea severității regulilor de decalaj de postură.
- Soluția trebuie să includă reguli predefinite pentru a sprijini guvernanța API și pentru a reduce riscurile (de exemplu, JWT fără expirare).
- Soluția trebuie să permită reguli personalizate pentru guvernanța unică a API-ului (de exemplu, format UserID ghicit).
- Soluția trebuie să includă reguli de decalaj de postură care identifică și alertează cu privire la atacurile de uzurpare a identității OAuth.
- Soluția trebuie să includă reguli de decalaj de postură care identifică și alertează atacurile de injecție de cod OAuth.

Detectare și protecție

- Soluția trebuie să poată genera informații detaliate despre comportamentul atacatorilor, inclusiv originile, metodele, țintele și motivațiile potențiale, pentru a permite echipelor de securitate să înțeleagă tacticile și obiectivele atacatorilor, facilitând un răspuns mai rapid și mai eficient la incidente și atenuarea amenințărilor.

- Soluția trebuie să analizeze continuu atributele utilizatorilor, comportamentul trecut și interacțiunile dintre toate API-urile și să creeze un profil cuprinzător al tiparelor tipice de comportament ale fiecărui utilizator.
- Soluția trebuie să permită o înțelegere profundă a contextului din jurul fiecărui apel API, aceasta include istoricul utilizatorului, API-ul specific accesat, datele transmise și modelele generale de trafic.
- Soluția trebuie să poată distinge între anomalii benigne (de exemplu, modificări ale preferințelor utilizatorului) și acțiuni potențial dăunătoare (de exemplu, încercări de a exploata vulnerabilitățile).
- Soluția trebuie să identifice vulnerabilitățile din implementările OAuth, permițând consolidarea posturii de securitate.
- Soluția trebuie să poată detecta un singur ID BOLA (Enumerarea identificatorilor în afara utilizării normale).
- Soluția trebuie să poată detecta Double ID BOLA (pierderea corelației observată de obicei între doi parametri. ex: Authorization.userid: 12345 și https://api.domain.com/user/12345).
- Soluția trebuie să poată detecta autentificarea utilizatorului întrerupt - forță brută sau umplere a credențialelor pe operațiuni precum autentificare, schimbarea parolei, resetarea parolei, 2FA etc.
- Soluția trebuie să poată detecta manipularea Json Web Token (algoritm de downgrade, încercări de escaladare a privilegiilor).
- Soluția trebuie să poată detecta atacul de redirecționare OAuth - învățând valorile obișnuite de redirecționare și abaterea de la acesta.
- Soluția trebuie să poată detecta detalii de autentificare sensibile, cum ar fi tokenurile de autentificare și parolele din URL.
- Soluția trebuie să poată detecta utilizări excesive.
- Soluția trebuie să poată detecta și raporta valorile parametrilor anormal de lungi specificate ca parte a interogărilor API și răspunsurile mai mari decât se aștepta care pot duce la refuzul serviciului.
- Soluția trebuie să poată detecta când utilizatorii trimit apeluri API către punctele finale API la care nu ar trebui să aibă acces, permițând atacatorilor să acceseze funcționalități neautorizate.
- Soluția trebuie să poată detecta funcții care leagă automat intrarea de la client în variabile de cod și obiecte interne.
- Soluția trebuie să demonstreze mecanisme robuste pentru a preveni atacurile SSRF (Server Request Forge). Aceasta include capacitatea de a detecta manipularea intrării pentru a se asigura că intrarea controlată de utilizator nu poate fi utilizată pentru a manipula solicitările serverului.
- Soluția trebuie să poată detecta ori de câte ori un API preia o resursă la distanță fără a valida URL-ul furnizat de utilizator.
- Soluția trebuie să poată detecta configurațiile greșite de securitate, cum ar fi mesajele de eroare care pot expune date sensibile ale utilizatorilor și detalii de sistem care pot duce la compromiterea completă a serverului.
- Soluția trebuie să poată detecta configurațiile greșite de securitate, cum ar fi mesajele de eroare care pot expune date sensibile ale utilizatorilor și detalii de sistem care pot duce la compromiterea completă a serverului.
- Soluția trebuie să poată detecta când atacatorii trimit date ostile către API prin diverși vectori de injecție (de exemplu, SQL Injection, Remote Code Execution, Cross site scripting, Path Traversal).
- Soluția trebuie să poată detecta lipsa inventarului activelor și a strategiilor de retragere, care ar putea duce la rularea sistemelor fără patch-uri și la scurgerea de date sensibile.
- Soluția trebuie să poată detecta comunicarea API pe canale nesecurizate.

- Soluția trebuie să poată evalua postura de securitate a tuturor API-urilor utilizate de organizație, oferind o imagine de ansamblu a riscurilor potențiale.
- Soluția trebuie să poată detecta când atacatorii profită de lipsa de înregistrare și monitorizare pentru a abuza de sisteme fără a fi observați.
- Soluția trebuie să ofere o vizualizare agregată a tuturor mediilor prin intermediul panoului de administrare, afișând jurnale de audit globale pentru activități precum configurarea rolurilor, aplicarea SSO și altele.
- Soluția trebuie să permită controlul granular al vizibilității și accesului utilizatorilor în dashboard.
- Soluția trebuie să permită definirea propriilor roluri personalizate cu permisiuni de acces precise permițând utilizatorilor să acceseze doar resursele de care au nevoie.
- Soluția trebuie să permită setarea de roluri pe persoană sau grup care se aliniază cu rolurile definite în directorul furnizorului de identitate și setarea de reguli pentru fiecare mediu, astfel încât să permită implementarea segregata la nivel de acces.
- Soluția trebuie să permită separarea în mai multe medii în funcție de propriile nevoi, de exemplu, în funcție de domeniul API, diferite departamente, responsabilități separate ale utilizatorilor sau seturi specifice de API-uri.
- Soluția trebuie să permită executarea fluxurilor de lucru de acțiune bazate pe criterii complexe și specifice, mergând dincolo de simplii declanșatori de evenimente.
- Soluția trebuie să permită fluxuri de lucru automatizate în mai mulți pași.
- Soluția trebuie să suporte un număr de cel puțin 1000 API calls/lună.

5.8.8. Componenta pentru administrarea identității utilizatorilor

Soluția va cuprinde o platformă de gestiune a identității utilizatorilor în cadrul sistemelor și aplicațiilor din cadrul instituției, asigurând administrarea centralizată a rolurilor și permisiunilor utilizatorilor, provizionarea identității și a conturilor de utilizator în aplicații.

Soluția trebuie să fie un instrument disponibil comercial (COTS) și să ofere posibilitatea de a rula pe infrastructura pusă la dispoziție pentru proiect, pe sistemele de operare majore existente pe piață (Windows, Linux), precum și posibilitatea de a rula într-o infrastructuri Kubernetes. Componenta de management centralizat a identității utilizatorilor trebuie să îndeplinească următoarele cerințe funcționale:

- Automatizează procesul de acordare și eliminare a conturilor, drepturilor de acces și a rolurilor de aplicație către utilizatori în sistemele și aplicațiile din cadrul instituției;
- Stochează informații despre profilul utilizatorilor precum și conturile, permisiunile acestora în raport cu funcția pe care o au în cadrul instituției;
- Asigură sincronizarea și reconcilierea automată a informațiilor de identitate utilizatori între sisteme;
- Garantează eliminarea conturilor de acces, a drepturilor și permisiunilor utilizatorilor în sistemele și aplicațiile interne atunci când angajatul părăsește instituția;
- Propaga și sincronizează automat modificările apărute în profilul utilizatorilor în sistemele gestionate;
- Oferă o interfață unică de tip self-service pentru utilizatori, prin care aceștia pot solicita conturi și permisiuni în aplicații și sisteme;
- Facilitează dezvoltarea de fluxuri de acordare și aprobare conturi în sistemele și aplicațiile interne;
- Facilitează integrarea cu sistemele existente prin intermediul de conectori specifici fiecărui sistem în parte;
- Oferă capabilități de monitorizare și auditare.

Pentru îndeplinirea acestor cerințe funcționale, platforma trebuie să fie o soluție robustă, performantă și flexibilă, care să permită administratorilor să gestioneze centralizat politicile de acces, fluxurile de aprobare și propagare a conturilor și permisiunilor în aplicațiile și sistemele instituției, oferind în același timp capabilități de auditare și raportare asupra activităților efectuate în cadrul platformei.

Componenta de management centralizat al identității utilizatorilor

Componenta de management centralizat al identității utilizatorilor trebuie să includă un portal prin intermediul căruia utilizatorii pot să solicite accesul la aplicații, sisteme, roluri și permisiuni. Portalul trebuie să includă instrumente de tip wizard prin intermediul cărora se pot realiza cereri de acces, utilizatorul având la dispoziție instrumente personalizate în funcție de poziția pe care acesta o îndeplinește în cadrul instituției. Pentru a crește eficiența operațiilor de administrare, componenta trebuie să includă mecanisme care să permită previzionarea simultană de conturi și drepturi de acces pentru mai mulți utilizatori. Utilizatorii vor putea să își modifice datele personale de profil și să delege către alte persoane din cadrul instituției activitatea de aprobare a cererilor de acces. Rolurile și drepturile de acces în aplicațiile și sistemele instituției vor fi gestionate printr-un catalog centralizat, gestionat de către administratorul platformei.

Componenta de management centralizat al identității utilizatorilor trebuie să permită definirea de politici de aprobare care s poată fi gestionate centralizat pentru următoarele activități efectuate de către administratori:

- Creare, activare, modificare, ștergere și dezactivare utilizator;
- Creare, modificare, atribuire, ștergere rol asociat utilizatorilor;
- Activare, modificare, eliminare, dezactivare cont;
- Activare, modificare, eliminare permisiuni de aplicație;
- Modificare profil utilizator.

În funcție de importanța fiecărui sistem și aplicație în cadrul instituției, platforma de gestiune a utilizatorilor trebuie să permită definirea de politici de aprobare care să necesite aprobarea atât manuală, cât și automată a conturilor și permisiunilor de aplicație.

Componenta de management centralizat al identității utilizatorilor trebuie să ofere posibilitatea de a defini politici asociate parolelor utilizatorilor în funcție de cerințele specifice de securitate ale aplicațiilor și sistemelor, având criterii precum:

- Număr minim, maxim de caractere;
- Număr minim de caractere numerice, alfanumerice;
- Lista caractere obligatorii, permise sau interzise;
- Număr minim de caractere speciale;
- Posibilitatea de a interzice folosirea anumitor cuvinte în definirea parolei precum nume, prenume.

Componenta de management centralizat al identității utilizatorilor trebuie să ofere posibilitatea de a defini în mod grafic atribute asociate utilizatorilor, rolurilor, precum și tipul de date al atributelor (ex: minim șir de caractere, numeric, lista de valori, tip data). Acordarea de drepturi de acces trebuie să se realizeze pe baza organigramei instituției, platforma de gestiune utilizatori trebuie să permită în mod grafic definirea unei structuri organizatorice și atribute specifice care să fie utilizate în procesul de creare conturi în aplicații și sisteme.

Procesul de creare conturi pentru angajații instituției trebuie să se realizeze pe baza unor scripturi specifice fiecărui tip de sistem sau aplicație și care să poată fi gestionat centralizat, scripturile putând fi lansate atât manual, de către administratori, cât și programat, la intervale predefinite evidențiindu-se istoricul rulărilor.

Componenta de management centralizat al identității utilizatorilor trebuie să ofere posibilitatea de a certifica periodic rolurile, aplicațiile, permisiunile și utilizatorii definiți în cadrul platformei. Procesul de certificare trebuie să utilizeze ca parametri în determinarea intervalului de atestare informații precum gradul de confidențialitate atribuit fiecărui sistem sau aplicație în parte, rezultatele ultimului proces de atestare sau tentativele de violare a politicilor de acces de către utilizatori. Platforma trebuie să includă un portal cu fluxuri predefinite pentru a gestiona întregul proces de atestare, inclusiv fluxuri pentru revocarea automată a conturilor și permisiunilor în funcție de rezultatele procesului de atestare. Stabilirea persoanei care va realiza procesul de atestare trebuie să se realizeze dinamic în funcție de profilul utilizatorului și rolul în instituție, pe bază de reguli definite de către administrator. Platforma trebuie să fie capabilă să trimită notificări automate către persoanele care vor realiza certificările la intervalele predefinite și să ofere posibilitatea de a urmări starea procesului de atestare în orice moment. Persoana care realizează atestarea conturilor utilizatorilor trebuie să poată delega către alte persoane din cadrul instituției activitatea de atestare pentru anumite conturi specifice.

De asemenea, trebuie să includă un mecanism de segregare și validare a drepturilor pe care un utilizator le are, astfel încât cumulul de permisiuni să nu ofere posibilitatea de a efectua operații în cadrul sistemelor și aplicațiilor la care aceștia nu ar trebui să aibă acces.

Componenta trebuie să includă minim conectori pentru Microsoft Active Directory și Oracle Internet Directory. De asemenea, trebuie să includă un framework pentru dezvoltarea de conectori specifici care să poată fi utilizați pentru managementul utilizatorilor și permisiunilor în aplicații dezvoltate intern și pentru care nu există conectori predefiniți.

Componenta de management centralizat al identității utilizatorilor va include nativ o soluție de management centralizat a cererilor de acces prin intermediul căreia utilizatorii pot solicita conturi și permisiuni, iar administratorii delegați validează cererile de acces. Validarea cererilor trebuie să se realizeze atât pe baza datelor introduse de către utilizatori, cât și prin preluarea de date din sisteme externe pe bază de protocoale și formate de date diferite.

Componenta de management al cererilor de acces trebuie să îndeplinească următoarele cerințe:

- Trebuie să fie bazată pe standardul BPEL;
- Trebuie să permită aprobări în serial și paralel;
- Trebuie să ofere adaptări standard pentru baze de date relaționale, cozi de mesaje, servicii web;
- Trebuie să ofere posibilitatea de a implementa următoarele modele de interacțiuni între servicii: sincron cerere/răspuns, asincron one-to-one, asincron one-to-many, asincron cerere/răspuns;
- Trebuie să permită trimiterea de notificări către administratorii delegați folosind canale multiple de comunicare precum email;

- Trebuie să includă un modul dedicat de stocare și evaluare a regulilor de business pe care personalul non-tehnic le va putea accesa și modifica on-line prin intermediul unei console web, fără să fie nevoie de modificarea procesului de aprobare cereri de acces;
- Trebuie să permită escaladarea automată a fluxurilor de aprobare;
- Trebuie să permită delegarea manuală către alți administratori, precum și atribuirea automată bazată pe reguli a activității de aprobare a cererilor de acces;
- Trebuie să permită ca administratorii delegați să seteze perioade de vacanță, activitatea de aprobare a cererilor de acces putând fi redirecționată către alți administratori, în funcție de politicile de aprobare definite;
- Trebuie să permită definirea de fluxuri ad-hoc pentru a solicita informații suplimentare;
- Interfețele definite în cadrul fluxurilor de aprobare să poată fi dezvoltate pe baza unui limbaj precum Java și să ofere o gamă largă de controale predefinite și apelarea de servicii web.
- Trebuie să ofere posibilitatea de a audita procesele de aprobare a cererilor de acces evidențiindu-se actorii participanți, intervalul de timp și datele pe baza cărora au fost luate deciziile pe fluxul de aprobare.

Soluția trebuie să includă în mod standard o listă de rapoarte predefinite:
- Raport politici de acces asociate rolurilor, raport politici de acces asociate aplicațiilor din instituție;
- Rapoarte de atestare utilizatori, roluri, permisiuni de aplicație, aplicații instituției precum și rapoarte pentru lista de atestări efectuate și drepturi și conturi eliminate în urma procesului de certificare;
- Raport lista conturi orfane pe aplicație;
- Raport cereri de acces în aplicații instituției;
- Raport istoric permisiuni de acces utilizatori;
- Rapoarte asociate parolelor utilizatorilor (ex: parole expirate);
- Raport istoric profil utilizatori;
- Raport utilizatori șterși, dezactivați;
- Rapoarte asociate rolurilor, precum lista utilizatori dintr-un rol, lista roluri asociate unui utilizator, istoric cu lista utilizatori dintr-un rol;

Sistemul de raportare trebuie să ofere posibilitatea de a exporta rapoartele generate în formate diverse, minim csv, PDF și HTML. Generarea de rapoarte se va realiza la cererea administratorilor sau automat la o dată și un interval de timp predefinit, iar livrarea rapoartelor se va realiza pe email, server FTP, HTTP.

Componenta de control acces

Soluția trebuie să includă un sistem centralizat de management a accesului la aplicații și să ofere funcționalități de single sign-on, autentificare, autorizare, administrare centralizată, managementul agenților de autorizare și al politicilor de acces, management în timp real al sesiunilor de aplicații și audit.

Soluția trebuie să fie un instrument disponibil comercial (COTS) și să ofere posibilitatea de a rula pe infrastructura pusă la dispoziție de beneficiar, pe sistemele de operare majore existente pe piață (Windows, Linux), precum și posibilitatea de a rula într-o infrastructură Kubernetes.

Rolul acestui sistem este de creștere a securității prin politici globale de securitate și eliminarea riscurilor potențiale, prevenirea accesului neautorizat la sistemele și aplicațiile instituției, simplificarea operațiilor de administrare, prin reducerea și automatizarea numărului de operațiuni administrative.

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

- utilizator și parola,
- X.509 Digital certificates,
- Windows Native Authentication,
- Federated tokens – SAML (Security Assertion Markup Language),
- Autentificare de tip multi-factor prin introducerea unui mecanism secundar de autentificare.

Acțiunile de autentificare efectuate de către utilizatori, dar și activități administrative precum creare, modificare, vizualizare, ștergere scheme de autentificare, module și politici de acces vor trebui să fie auditate, platforma colectând minim adresa IP, data acțiunii și ID login. Complementar, componenta va permite filtrarea autentificării și autorizării pe baza unor reguli avansate, utilizând diverse criterii: adresa IP, dispozitivul folosit, tipul de browser folosit, interval orar.

Componenta trebuie să includă o consolă web pentru crearea politicilor de acces, aceasta trebuind să permită 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 server. De asemenea, trebuie să permită definirea de politici de acces în funcție de atribute de utilizator, atribute cerere de acces, date de sesiune.

Componenta trebuie să ofere capabilități de grupare politici de acces pe zona funcțională și să permită delegarea procesului de administrare a politicilor de acces către administratori locali, fiecare administrator local putând să gestioneze doar grupul de politici de acces alocate.

Componenta trebuie să ofere administratorilor posibilitatea de a administra centralizat toate sesiunile deschise către aplicații, având vizibilitate în timp real asupra datelor de sesiune ale utilizatorilor. Administratorii trebuie să poată 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 monitorizarea sesiunilor deschise de către utilizatori, platforma trebuie să implementeze un mecanism de caching date sesiune utilizatori. Mecanismul de caching trebuie să asigure confidențialitatea datelor prin criptare automată, având și capabilități de failover automat și reconciliere. Sistemul de caching va conține, pe lângă datele de sesiune, și informații despre configurarea sistemului și politicile de acces la sistemele protejate. De asemenea, mecanismul de caching trebuie să asigure disponibilitate ridicată printr-o arhitectură de tip cluster activ-activ.

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.

Stocarea configurațiilor și a politicilor de acces la resursele web să se realizeze în baza de date a sistemului, fără a exista necesitatea unui depozitar proprietar de date.

De asemenea, soluția trebuie să permită definirea mai multor scheme de autentificare simultană la o aplicație (ex: autentificare pe baza de server LDAP, user și parolă stocată în baza de date, certificat digital), respingerea autentificării la una din scheme determinând ca utilizatorul să fie autentificat cu celelalte scheme disponibile.
Componenta de control acces, prin funcționalitățile de raportare, va oferi posibilitatea de a exporta rapoartele generate în formate diverse, minim PDF și HTML. Generarea de rapoarte se va realiza la cererea administratorilor sau automat la o dată și un interval de timp predefinit, livrarea rapoartelor se va realiza pe email, server FTP, HTTP.

Soluția trebuie să permită accesarea simultană a mai multor surse de identități pentru realizarea autentificării și autorizării, fără a implica duplicarea informației sau crearea unui metadirector.

Soluția trebuie să suporte procesul de federalizare între furnizori de identitate pentru utilizatori diferiți, facilitând schimbul de informații despre profilul utilizatorilor între furnizori diferiți. În acest sens, trebuie să suporte standardele SAML 1.1 și SAML 2.0, OPEN ID 2.0.

Componenta de federalizare a identității trebuie să suporte următoarele scenarii de implementare:

- distribuirea datelor de sesiune între domeniile de identitate fără să fie nevoie de trimiterea sau consumul informațiilor de identitate utilizatori;
- schimbul de informații despre profilul utilizatorilor și maparea informațiilor de profil între doi furnizori de identitate;
- permite accesul la resursele protejate pe bază de politici de acces la nivel de atribute despre profilul utilizatorilor.

Nivelul de auditare trebuie să fie configurabil (succes, nereușită).

Soluția trebuie să includă în mod standard o listă de rapoarte predefinite:

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

Componenta de stocare profil utilizatori

Soluția trebuie să includă și să implementeze un modul de stocare standardizată a profilurilor de utilizatori într-un director de tip LDAP și sî ofere posibilitatea de a rula pe diverse platforme hardware și sisteme de operare.

Administrarea și editarea profilurilor de utilizatori trebuie să se realizeze printr-o interfață web accesibilă doar administratorilor de sistem. Accesarea datelor de profil utilizator trebuie să se realizeze prin protocoale securizate precum LDAPS cu posibilitatea de a configura porturile de comunicație. Profilurile utilizatorilor trebuie să poată fi extinse prin adăugare de noi atribute pentru a asigura compatibilitatea sistemului cu module suplimentare.

Componenta de stocare centralizată a profilurilor de utilizatori trebuie să fie conformă cu standardul LDAP v3. De asemenea, va permite filtrarea accesului astfel încât fiecare

utilizator să poată citi doar datele de care are nevoie. Filtrarea trebuie să se poată realiza la nivel de atribut LDAP.

Astfel, soluția va permite implementarea de reguli de acces definite până la nivelul de atribut prin mecanism ACI, precum și mecanisme avansate pentru asigurarea unei granularități cât mai mari în definirea regulilor de acces.

Soluția oferă mecanisme de unificare pentru mai multe servicii de directoare fără a copia datele, astfel modulul de virtualizare trebuie să prezinte date agregate din surse multiple de identitate reprezentând un punct unic de autentificare către aplicațiile consumatoare, având și capabilitatea de a transforma și ruta datele schimbate între aplicații și sursele de identitate.

Soluția oferă o flexibilitate maximă prin includerea unor mecanisme de schimb al identității, SCIM sau REST API precum și posibilitatea de a efectua operațiuni de administrare și configurare prin REST API. De asemenea, oferă suport pentru TLS 1.2, 1.3.
Parolele stocate în cadrul directorului vor fi criptate, stocarea datelor trebuie să se realizeze într-o structură de tip bază de date. Profilurile de utilizator vor putea fi extinse prin adăugarea de noi atribute, acestea fiind administrate și editate prin intermediul unor profiluri de utilizatori.

Soluția va oferi mecanisme de extindere a funcționalităților standard utilizând plug-în-uri și REST APIs.

În vederea creșterii nivelului de flexibilitate în administrarea soluției, aceasta va trebui să ofere o componentă de tip command line interface (CLI).

Soluția va permite configurarea și rularea în mod înaltă disponibilitate pentru componentele active ale soluției, atât nivelul de prezentare (server LDAP), cât și cel de stocare (bază de date cu profilurile și parole de utilizatori).

Platforma pentru administrarea identității utilizatorilor trebuie să fie licențiată pentru un număr minim de 50 de utilizatori interni și minim 4500 de utilizatori tip externi (utilizatori din toata structura APIA).

5.8.9. Componenta de securizare a accesului privilegiat

Această componentă are rolul de a proteja, gestiona și monitoriza accesul privilegiat la resursele critice ale sistemului. Accesul privilegiat se referă la permisiunile și drepturile speciale care sunt acordate utilizatorilor, conturilor sau aplicațiilor pentru a accesa, administra și controla sisteme, rețele și informații sensibile.

Această componentă trebuie să îndeplinească următoarele cerințe de bază:

- Soluția trebuie să aibă posibilitatea de a oferi acces pe bază de roluri definite pentru a evita accesul neautorizat sau al unui utilizator cu rol diferit la serverele critice.
- Soluția trebuie să permită integrarea cu un server LDAP extern unde sunt ținuți utilizatorii.
- Soluția trebuie să ofere posibilitatea de a oferi accesul la resurse pe baza unui program de timp care sa poată fi definit.

- Soluția trebuie să ofere posibilitatea de a reduce controlat și granular privilegiile conturilor de tip ”superuser” pentru administratorii de aplicații Microsoft și ”root” pentru UNIX/Linux.
- Soluția trebuie să permită definirea de politici de acces la resurse pe baza criteriilor multiple: interval orar, metoda de acces, metoda de logare etc.
- Soluția trebuie să monitorizeze integritatea fișierelor și a programelor utilizând cel puțin următoarele criterii: informații aferente HDD (dimensiune fișier, proprietar fișier etc), precum și algoritmi de digital hashing. În cazul în care un fișier monitorizat se dovedește a fi diferit de parametrii inițiali, soluția trebuie să genereze un eveniment înregistrat în fișierul de log și/sau o alertă e-mail. În cazul în care fișierul care a fost modificat reprezintă un program executabil, soluția trebuie să poată fi configurată pentru a bloca executarea programului până la momentul în care fișierul este considerat din nou de încredere.
- Soluția trebuie să permită definirea de politici de acces individualizate pentru sisteme, în funcție de rolul acestora.
- Soluția trebuie să asigure suplimentarea controalelor native furnizate de sistemul de operare pentru Fișiere și Directoare (atât pentru sisteme Windows, cât și Linux/Unix), astfel încât să asigure cel puțin controlul operațiilor de: read, write, execute, create, delete, rename, chown și chmod asupra fișierelor și directoarelor.
- Soluția trebuie să dețină o certificare de securitate emisă de o instituție independentă recunoscută internațional – Common Criteria sau echivalent.
- Soluția trebuie să ofere posibilitatea eliminării conturilor administrative comune prin implementarea funcționalităților de delegare a sarcinilor administrative, administratorii având drepturi doar la componentele necesare îndeplinirii sarcinilor.
- Soluția trebuie să ofere politici predefinite care să fie în conformitate cu bunele practici de securitate.
- Soluția trebuie să permită definirea de politici pentru implementarea unei funcționalități de tip firewall în funcție de porturi, adresa sursă, tipul conectării precum și timp. Această funcționalitate trebuie oferită atât pentru conexiunile egress, cât și pentru cele ingress.
- Soluția trebuie să permită definirea de politici de securitate ce pot fi distribuite pe grupuri de servere, indiferent de domeniul din care acestea fac parte.
- Soluția trebuie să ofere posibilitatea administrării și definirii de politici într-un mod centralizat, indiferent de sistemul de operare care rulează pe sisteme.
- Soluția trebuie să suporte definirea de roluri, astfel încât pe baza grupurilor din care face parte utilizatorul, să i se permită accesul la diferite funcționalități.
- Soluția trebuie să suporte criptarea datelor transmise prin rețea și a datelor aplicației;
- Soluția trebuie să ofere funcționalități de administrare a parolelor conturilor partajate și privilegiate.
- Soluția trebuie să permită accesul utilizatorilor la parolele conturilor privilegiate pe bază de reguli de acces. Regulile de acces trebuie să poată fi create și modificate de către administratorul soluției.
- Soluția trebuie să ofere posibilitatea integrării cu aplicații dezvoltate în-house în vederea schimbării parolelor.
- Soluția trebuie să ofere suport pentru a putea extrage parolele din sistem, folosind linia de comandă și API.

- Soluția trebuie să asigure funcționalități pentru a permite aplicațiilor care necesită acces la conturi privilegiate să primească datele de conectare în mod programatic, eliminând necesitatea de a transcrie ("hardcode") credențialele de acces în script-uri sau în aplicații.
- Soluția trebuie să permită utilizatorilor folosirea conturilor înregistrate în sistem, fără ca aceștia să poată vedea parola prin folosirea unei metode de tip login automat.
- Soluția trebuie să suporte cel puțin protocolul RDP, SSH și Telnet pentru login automat.
- Soluția trebuie să ofere posibilitatea autentificării utilizatorului în mod automat pentru sesiunile SSH, Telnet, RDP prin folosirea interfeței web, întreaga sesiune fiind înregistrată și stocată. Soluția trebuie să pună la dispoziție opțiunea de a vizualiza din interfață web sesiunile înregistrate.
- Soluția trebuie să extragă comenzile rulate în cadrul sesiunilor SSH și Telnet și să le atașeze înregistrării sesiunii. Pentru fiecare sesiune, atât înregistrarea, cât și lista comenzilor executate trebuie să poată fi vizualizate în interfața web.
- Pentru conturile cu un grad mare de risc, soluția trebuie să ofere posibilitatea definirii unui proces de aprobare, astfel încât înaintea folosirii contului, utilizatorul să ceară aprobarea unei alte persoane. Accesul la cont se va permite numai după obținerea aprobării.

5.8.10. Componenta de monitorizare a performanței aplicațiilor

Componenta de monitorizare a aplicațiilor va trebui să monitorizeze aplicațiile sistemului, cum ar fi: baze de date, servere web, sisteme de virtualizare, servere de aplicații.

Cerințe minime:

- Componenta trebuie să fie instalată on premise.
- Componenta trebuie să aibă un panou de comandă de tip WEB și să aibă o interfață grafică ușor de utilizat și simplă pentru ca administratorii de sistem să nu aibă dificultate în a folosi componenta.
- Interfața trebuie structurată în subpanouri pentru simplificarea folosirii soluției și executarea de operațiuni.
- Componenta trebuie să identifice elementele problematice din codul aplicației.
- Componenta trebuie să monitorizeze operațiunile bazei de date și identificarea instrucțiunilor SQL.
- Componenta trebuie să utilizeze capabilități de urmărire distribuită pentru a reduce timpul de depanare în mediile de microservicii.
- Componenta trebuie să permită vizualizarea dependențelor de arhitectură a aplicației cu ajutorul hărților automate ale serviciilor.
- Componenta trebuie să permită monitorizarea parametrilor de server:
    - Utilizarea memoriei,
    - Disc I/O,
    - Sarcini programate,
    - Erori Syslog,
    - Jurnale de evenimente etc.
- Componenta trebuie să permită monitorizarea infrastructurii virtuale și gazdelor virtuale:
    - Utilizarea memoriei,
    - Disc I/O,

    - Interfața și adaptoarele de rețea,
    - Sănătatea hardware,
    - Sarcini programate,
    - Erori Syslog,
    - Jurnale de evenimente etc.
- Componenta trebuie să identifice mașinile virtuale care consumă cele mai multe resurse.
- Componenta trebuie să permită monitorizarea containerelor: Docker, Kubernetes, Red Hat OpenShift;
- Componenta trebuie să permită consumul de resurse al containerelor.
- Componenta trebuie să permită monitorizarea bazei de date.
- Componenta trebuie să permită vizualizare consumului de resurse al bazelor de date: RAM, HDD, CPU etc.
- Componenta trebuie să permită vizualizarea comenzilor trimise către bazele de date.
- Componenta trebuie să creeze o hartă a dependențelor dintre aplicații și resursele software și hardware.
- Componenta trebuie să monitorizeze interacțiunile utilizatorilor cu aplicațiile.
- Componenta trebuie să identifice blocările de performanță înainte de a fi sesizate de utilizatori.
- Componenta trebuie să suporte tehnologii NoSQL.
- Componenta trebuie să permită monitorizarea de servere web.
- Componenta trebuie să permită monitorizarea de: tranzacții sintetice, interacțiune utilizator-aplicație, URL-uri, conținut website, API-uri rest.
- Componenta trebuie să permită monitorizare de aplicații utilizând byte-code instrumentation (java, .NET, PHP, Node.js și Python).
- Componenta trebuie să permită diagnoza de tip root cause la nivel de cod.
- Componenta trebuie să permită praguri de alertare de tip static și adaptive.
- Componenta trebuie să permită detectare de anomalii cu suport pentru linii de bază dinamice.
- Componenta trebuie să permită acțiuni automatizate, cum ar fi executarea de scripturi corective, comenzi către mașini virtuale, cum ar fi start, stop, restart etc.
- Componenta trebuie să permită configurație de failover și virtual IP.
- Componenta trebuie să permită scalabilitate ridicată și arhitectura de monitorizare distribuită.
- Componenta trebuie să permită rapoarte de tip analiza de trend și forecast.

5.8.11. Componenta inteligentă de optimizare automată a resurselor

Componenta de management și optimizare a resurselor utilizează inteligența artificială pentru a asigura performanța aplicațiilor în timp ce optimizează costurile computaționale și eficiența în medii complexe de cloud și on-premise.

Cerințe:

- Componenta trebuie să asigure ajustarea dinamică și în timp real a resurselor.
- Decizii inteligente și automate de scalare bazate pe cererea reală, optimizând dinamic resursele pentru a asigura performanță și eficiență a costurilor.
- Balansare inteligentă și automată a încărcărilor între medii diferite, optimizând distribuția sarcinilor pentru performanță maximă și utilizare eficientă a resurselor.
- Modelare avansată și automată a dependențelor aplicațiilor, oferind vizibilitate completă asupra relațiilor și impactului modificărilor în arhitectura sistemului.

- Predicții precise și automate ale cererii de resurse bazate pe ML, optimizând alocarea și planificarea capacității pentru eficiență maximă.
- Simulări avansate de tip 'what-if' pentru planificarea capacității, permițând analiza scenariilor și optimizarea proactivă a resurselor în funcție de diferite ipoteze de creștere.
- Optimizare unificată și inteligentă pentru medii hibride și multi-cloud, asigurând performanță consistentă și management eficient al resurselor în toate mediile de operare.
- Migrare inteligentă și automatizată a încărcărilor între furnizorii de Cloud, optimizând costurile și performanța prin redistribuirea dinamică a sarcinilor în funcție de condițiile specifice fiecărui provider.
- Recomandări inteligente de cost-optimizare pentru servicii cloud, identificând automat oportunități de reducere a costurilor și sugerând ajustări pentru utilizarea eficientă a resurselor.
- Alocare precisă a resurselor la toate nivelurile infrastructurii: containere și pod-uri Kubernetes, mașini virtuale, stocare și rețea, asigurând optimizarea și eficiența utilizării.
- Componenta trebuie să dețină o arhitectură distribuită, scalabilă, disponibilă pentru platforma pusa la dispoziție de beneficiar.
- Componenta trebuie să permită definirea de reguli și constrângeri de business.
- Automatizare inteligentă în deplină conformitate cu politicile de guvernanță IT, asigurând eficiență operațională și respectarea standardelor de securitate și control.
- Raportare avansată cu vizibilitate completă asupra consumului de resurse și tendințelor, permițând decizii informate pentru optimizare și planificare strategică.
- Analiză avansată a trendurilor și pattern-urilor de consum, oferind vederi predictive pentru optimizarea resurselor și anticiparea nevoilor viitoare de capacitate.
- API-uri robuste pentru integrarea cu pipeline-uri CI/CD, facilitând automatizarea completă a proceselor de dezvoltare, testare și instalare în medii de CI.
- Suită de plug-în-uri pentru integrare cu instrumente populare de dezvoltare, oferind extensibilitate și compatibilitate cu ecosistemele majore DevOps.
- Algoritmi avansați de AI/ML pentru analiză predictivă, identificând automat pattern-uri și tendințe pentru optimizarea proactivă a performanței și prevenirea incidentelor.
- Sistem inteligent de luare a deciziilor în timp real, care analizează și acționează instant pe baza datelor curente pentru optimizarea continuă a performanței.
- Optimizare inteligentă și simultană a performanței, conformității și costurilor, asigurând echilibrul perfect între eficiență operațională, respectarea reglementărilor și eficiență financiară.
- Executare automată și inteligentă a acțiunilor de optimizare, implementând ajustări în timp real pentru maximizarea performanței sistemului fără intervenție manuală.
- Capabilități avansate de rollback pentru toate acțiunile executate, asigurând reversibilitatea sigură a modificărilor și restaurarea rapidă la stări anterioare stabile.
- Programare flexibilă a acțiunilor pentru perioade specifice, permițând planificarea și executarea automată a operațiunilor în intervalele optime de timp.
- Limitare inteligentă a acțiunilor în conformitate cu politicile definite, asigurând executarea operațiunilor în parametrii securizați.
- Scalare automată și inteligentă a serviciilor containerizate, ajustând dinamic resursele în funcție de cerere pentru performanță optimă și eficiență a costurilor.

- Garantarea calității serviciilor (QoS) pentru aplicații containerizate prin monitorizare continuă și ajustare automată a parametrilor de performanță și disponibilitate.
- Sistem avansat de autentificare și autorizare granulară bazat pe roluri (RBAC), asigurând control precis asupra accesului la resurse și funcționalități.
- Audit logging comprehensiv pentru toate acțiunile și deciziile sistemului, asigurând trasabilitate completă și conformitate cu cerințele de guvernanță și reglementare.
- Securitate avansată prin criptare completă a datelor, atât în tranzit, cât și în repaus, asigurând protecția completă a informațiilor sensibile în toate stările.
- Suport complet și scalabil pentru medii complexe, asigurând performanța, fiabilitatea și securitatea necesare operațiunilor la scară mare.
- Procesare optimizată a datelor în timp real, oferind analiză instantanee și vederi acționabile pentru luarea rapidă a deciziilor critice.
- Monitorizare cu impact minim asupra performanței sistemelor țintă, asigurând colectarea eficientă a datelor cu o amprentă de resurse sub 1%.
- Sistem flexibil de definire a politicilor cu control granular, permițând configurarea detaliată a regulilor și comportamentelor la nivel de componente individuale.
- Implementare flexibilă a constrângerilor de business, asigurând alinierea operațiunilor tehnice cu regulile și cerințele specifice ale organizației.
- Management inteligent al încărcării prin priorități configurabile, asigurând alocarea optimă a resurselor conform importanței și urgențelor operaționale.
- Reguli inteligente, bazate pe afinități, optimizând distribuția încărcărilor în funcție de cerințele de proximitate și compatibilitate pentru performanță maximă.
- Calcul granular și detaliat al costurilor, oferind vizibilitate completă asupra cheltuielilor la nivel de serviciu, aplicație și resursă, facilitând optimizarea și controlul bugetar eficient.
- Monitorizare și analiză completă a costurilor cu detaliere la nivel granular, oferind transparență totală asupra cheltuielilor și facilitând luarea deciziilor informate pentru eficientizarea investițiilor IT.
- Optimizare inteligentă a resurselor în funcție de constrângerile bugetare definite, asigurând maximizarea performanței în limitele financiare stabilite și distribuirea eficientă a investițiilor IT.
- Sistem inteligent de recomandări pentru optimizarea costurilor cloud prin analiza automată a pattern-urilor de utilizare, sugerând cea mai eficientă combinație de instanțe rezervate și plan de reducere costuri pentru maximizarea economiilor.
- Fluxuri optimizate și simplificate pentru operațiunile frecvente, reducând complexitatea și timpul de execuție prin automatizarea pașilor repetitivi și ghidare intuitivă în procesele operaționale.
- Sistem flexibil de notificări configurabile care alertează proactiv asupra evenimentelor importante, permițând personalizarea completă a canalelor, pragurilor și destinatarilor în funcție de severitate și context operațional.
- Acces securizat și optimizat la funcționalitățile cheie prin interfață mobilă, permițând monitorizarea și gestionarea sistemelor de oriunde, cu experiență consistentă pe orice dispozitiv.

5.8.12. Componenta de mascare a datelor

Componenta trebuie sa asigure confidențialitatea informațiilor necesare pentru operare, accesul la interfața de administrare făcându-se pe bază de nume de utilizator și parolă.

Totodată sistemul asigură integritatea datelor transmise, actualizate, vizualizate sau înregistrate.

Toate informațiile despre utilizatori vor fi confidențiale în limitele stabilite prin politica de securitate. Aceste limite sunt stabilite în funcție de rolul pe care îl are fiecare utilizator în cadrul sistemului informatic propus. De asemenea, se vor respecta legislația și reglementările internaționale privind protecția intimității și a datelor personale.

Prin intermediul unei componente specializate de administrare, persoanele acreditate (administratori de sistem) vor putea restricționa accesul în anumite zone ale sistemului informatic, la anumite documente sau date, după cum va fi necesar, pentru a acorda drepturi doar anumitor utilizatori sau grupuri de utilizatori.

Cu ajutorul acestei politici, utilizatorii vor putea vizualiza, modifica sau adăuga documente/înregistrări numai în limita drepturilor de acces asociate, asigurându-se confidențialitatea datelor.

Din motive de securitate, parolele utilizatorilor nu vor fi păstrate în baza de date, ci se vor păstra criptate într-un director LDAP centralizat.

Clasificarea datelor

Soluția trebuie să ajute la identificarea și clasificarea datelor sensibile stocate în baze de date.

Soluția trebuie să faciliteze găsirea oricăror informații sensibile care trebuie protejate și să se asigure că aceste date sunt clasificate corespunzător pentru anonimizare, astfel încât să poată fi gestionate în siguranță.

Caracteristici necesare:

- Soluția trebuie să includă metode predefinite de descoperire a datelor sensibile pentru cele mai frecvente scenarii:
  - Nume complet,
  - Prenume,
  - Nume de familie,
  - Carte de identitate personală (inclusiv carte de identitate regională, carte de identitate fiscală și pașaport),
  - E-mailuri,
  - Numere de telefon,
  - Oraș,
  - Stradă,
  - Cod poștal,
  - Țară,
  - Adresa completă,
  - Text sensibil,
  - IBAN,
  - Carte de credit,
  - Licență,
  - Înmatriculare.
- Soluția trebuie să ofere cel puțin 4 tipuri de clasificatori de date care pot fi utilizați pentru a adăuga noi reguli de clasificare a datelor:
  - Expresii regulate,
  - Căutare în dicționar cu potrivire exactă,

    - Căutare în dicționar cu potrivire liberă,
    - Căutare în mai multe dicționare.
- Clasificarea datelor ar trebui să acopere atât datele în sine, cât și metadatele acestora. Datele trebuie să fie analizate pentru a determina dacă sunt sensibile, în timp ce metadatele trebuie să poată fi utilizate pentru a îmbunătăți acuratețea clasificării.
- Soluția trebuie să permită adăugarea/dezvoltarea metodelor de descoperire a datelor pentru a scana anumite tipuri de date.
- Soluția trebuie să aibă reguli predefinite de detecție și clasificare conform reglementărilor (GDPR, PCI-DSS și altele).
- Soluția trebuie să aibă posibilitatea de a atribui etichete/categorii datelor clasificate.
- Soluția trebuie să fie capabilă să gestioneze și să reducă rezultatele fals pozitive.
- Soluția trebuie să permită crearea de politici și alerte de clasificare a datelor.
- Soluția trebuie să permită exportul rezultatelor scanării în excel / pdf.
- Soluția trebuie să permită integrarea cu motorul de mascare – adăugarea de tabele și coloane din modulul de clasificare la modulul de mascare.
- Soluția trebuie să aibă capabilități de dashboard.

Mascarea datelor

- Soluția trebuie să ofere mai multe metode de mascare încorporate, permițând anonimizarea datelor prin următoarele tehnici: **Mascare** – Înlocuirea parțială a valorilor cu * sau conform parametrilor predefiniți; **Shuffle** – Generarea unei liste distincte de valorile care urmează să fie mascate, apoi schimbarea aleatorie a valorilor între perechi până când toate datele sunt înlocuite; **Maparea cifrelor** – înlocuirea aleatorie a fiecărei cifre dintr-un șir sau număr cu o cifră alternativă predefinită; **Dicționar** – înlocuirea fiecărei valori cu o valoare aleatorie preluată din dicționar; **Număr universal** – generarea unui număr unic / neunic care păstrează formatul original; **Text aleatoriu** – generarea aleatorie a unui text sau număr pe baza valorii originale; **IBAN** – mascarea IBAN-urilor păstrând atât regiunea, cât și formatul; **Telefoane** – generarea aleatorie de numere de telefon pe baza numărului original; **Nume complet** – mascarea în mod constant de nume complete în funcție de numele și prenumele mascate.
- Soluția trebuie să aibă capacitatea de a adăuga metode de mascare personalizate fără a dezvolta cod.
- Soluția trebuie să permită mascarea consecventă a datelor.
- Soluția trebuie să păstreze integritatea relațională (PK-FK) definită la nivel de baze de date.
- Soluția trebuie să păstreze relațiile aplicative care nu sunt definite la nivel de baze de date.
- Soluția trebuie să aibă capacitatea de a masca indici unici.
- Soluția trebuie să permită mascarea deterministă pentru coloane complexe.
- Soluția trebuie să permită mascarea condiționată.
- Soluția trebuie să permită mascarea în bloc (permite mascarea similară cu un grup de coloane).
- Soluția trebuie să permită atribuirea automată a metodei de mascare pe categorii.
- Soluția trebuie să permită repornirea operațiunii de mascare în cazul unei erori în procesul de mascare.
- Soluția trebuie să permită previzualizarea rezultatului operațiunii de mascare.

5.8.13. Componenta de service desk

Având în vedere numărul mare de utilizatori și componente ale sistemelor client se impune utilizarea unei soluții de asistență tehnică (help-desk) prin care se vor gestiona toate incidentele înregistrate la nivelul platformei de tip tenant și care totodată să asigure monitorizarea tuturor SLA-urilor stabilite. Soluția va permite preluarea, înregistrarea și urmărirea sesizărilor (incidente/tichete) privind funcționarea anormală a întregului sistem informatic.

Soluția trebuie să asigure managementul incidentelor și al solicitărilor realizate de către utilizatorii fiecărui beneficiar simultan cu separarea datelor (incidente, cereri de suport, SLA etc) astfel încât utilizatorii dintr-o instituție să poată vizualiza datele aferente propriei instituții, dar să nu poată vizualiza datele aferente unei alte instituții.

Implementarea platformei unice de gestionare a incidentelor are ca scop:

- reducerea perioadelor de nefuncționare a diverselor componente /sisteme /aplicații /servicii;
- creșterea vitezei de intervenție a personalului IT;
- suport în prioritizarea corectă a activității de rezolvare a incidentelor;
- monitorizarea timpilor de intervenție și a modului în se respectă contractele de service și suport.

Platforma va permite preluarea incidentelor transmise telefonic, prin email sau prin intermediul interfețelor platformei.

Soluția va permite configurarea următoarelor fluxuri de tratare a incidentelor:

- Flux pentru înregistrare incidente;
- Flux pentru escaladare incidente, preluare și rezolvare incident;
- Flux pentru notificare utilizatori.

Pe parcursul derulării activității de service desk, soluția va permite înregistrarea modalităților de rezolvare a incidentelor frecvent întâlnite sub formă de bază de cunoștințe, astfel încât modalitatea de rezolvare a unui incident similar va fi înregistrată în sistem și va permite un răspuns prompt, prin evitarea pașilor de re-diagnosticare. Componenta bază de cunoștințe va permite cel puțin, dar fără a se limita la, funcții de înregistrare, modificare, căutare, vizualizare.

Componenta bază de cunoștințe trebuie să dispună de facilități de căutare după cele mai frecvente întrebări și să ofere metoda de căutare a informației de tip „arbore de decizie” în baza de cunoștințe.

Soluția de help-desk va avea capabilități integrate de gestionare a cerințelor de SLA ale tuturor componentelor sistemului clientului de cloud.

Caracteristici generale

- Aplicație software pentru gestionarea atât a activităților de Help Desk, cât și a aplicațiilor specifice activității de Management de Proiect bazate pe standardul ITIL.
- Acces bazat pe interfață web.
- Posibilitatea de creare câmpuri de urmărire personalizate.
- ITIL Ready.
- Posibilitatea de configurare bazată pe fluxuri predefinite (“Configuration wizard”).

- Posibilitatea de arhivare date.
- Posibilitatea de implementare teme și afișare bazată pe localizare.

Standarde ITIL Suportate
- Gestionarea incidentelor (“Incident Management”);
- Gestionarea problemelor (“Problem Management”);
- Gestionarea Schimbărilor (“Change Management”);
- Project Management;
- Baza de date integrate (“CMDB – Configuration Management Database”);
- Catalog de servicii (“Service Catalogs”).

Catalog de servicii
- Posibilitatea de afișare a serviciilor disponibile;
- Posibilitatea implementării de template –uri pentru cereri de service;
- Fluxuri de lucru pre-configurate;
- Proces de aprobare în mai multe faze;
- SLA - Service Level Agreement – asumat în timp;
- Posibilitatea de adăugare Categorii de Servicii, Resurse și Servicii;
- Posibilitatea de asociere a multiple activități dependente la un Template.

Modul de Self-Service
- Portal Self-service de tip web-based inclus în aplicație;
- Posibilitatea de creare cereri pentru utilizatorii finali;
- Posibilitatea de verificare și actualizare a stării unei cereri existente;
- Actualizarea detaliilor aferente contactelor;
- Posibilitate de căutare în baza de cunoștințe pentru utilizatori;
- Acces la secțiunea “Frequently Asked Questions (FAQs)”;
- Acțiuni de aprobare.

Gestionarea bazei de cunoștințe (Knowledge base)
- Acces pentru tehnicieni la serviciul de gestionare a bazei de cunoștințe;
- Posibilitatea de adăugare soluții după aprobare;
- Cuvinte cheie pentru găsirea soluțiilor pe baza informațiilor din cerere;
- Indexarea căutărilor de documente pentru obținerea unor rezultate în mod rapid;
- Păstrarea istoricului de căutări ;
- Frequently Asked Questions (FAQs);
- Editor de text integrat.

Gestionarea problemelor
- Detectarea și clasificarea problemelor;
- Posibilitatea de inițiere a unei probleme noi dintr-un incident;
- Posibilitatea de Inițiere/Înregistrare a unei probleme noi;
- Posibilitatea de asociere a unor incidente multiple într-o singurp problemp;
- Posibilitatea de prioritizare a problemelor;
- Posibilitatea de adăugare a informațiilor legate de cauze inițiale, impact, etc.;
- Adăugare de soluții temporare, soluții sau erori cunoscute;
- Posibilitate de închidere a problemelor.

Gestionarea schimbărilor
- Posibilitate de Inițiere/Înregistrare noi cereri de schimbare;
- Inițierea de cereri de schimbare din incidente/probleme;

- Posibilitatea de asociere a unor incidente/probleme multiple la o schimbare;
- Posibilitatea de creare a unui comitet de aprobare a schimbărilor (“Change Advisory Boards (CABs)”);
- Posibilitate de trimitere spre aprobare a cererilor de schimbare către membrii CAB;
- Posibilitate de adăugare informații legate de analiza impactului, cauze, simptome;
- Posibilitate de înregistrare a soluțiilor permanente și temporare;
- Facilitați de coordonare a implementării schimbării;
- Posibilitatea de trimitere spre reverificare a schimbărilor;
- Posibilitate de trimitere anunțuri către tehnicieni și/sau utilizatori finali.

Project Management

- Posibilitate de integrare Proiecte, Milestones –uri și Task –uri;
- Gestionarea și planificare task –urilor;
- Posibilitatea de păstrare a istoricului unui proiect;
- Estimarea efortului;
- Gestionare timpului;
- Harta de privire generală a Proiectului;
- Notificare înainte de expirare SLA.

Rapoarte

- Rapoarte standard pre-definite;
- Posibilitate de realizare rapoarte personificate în format tabelar;
- Unealtă de creare interogări pentru rapoarte (“Query Builder”);
- Posibilitatea de integrare cu aplicații de raportare profesionale;
- Posibilitatea de salvare rapoarte în format .csv,.xls și Pdf;
- Generarea și distribuirea automată a rapoartelor (“Reports Scheduler”);
- Posibilitatea de analiza a evoluției și performanțelor;
- Actualizarea în timp real a rapoartelor;
- Posibilitatea de salvare și programarea rapoartelor customizate.

Integrare

- Integrare cu LDAP;
- Posibilitatea de integrare cu sisteme de email și SMS;
- Aplicații pentru dispozitive iPhone și android;
- Interfață de integrare cu date externe;
- Utilizare a serviciilor web;
- Module API.

Gestionarea apelurilor și a cererilor

- Modalități de generare a cererilor:
- Depozit central pentru stocarea și urmărirea situațiilor;
- Generare automată de tichete;
- Posibilitatea de afișare pe monitor către utilizatori a situațiilor importante;
- Posibilitatea de recepționare și transmitere mesaje email din aplicație;
- Posibilitatea de recepționare și transmitere mesaje SMS din aplicație;
- Creare tichete din mesajele de email primite;
- Email parser;
- Clasificarea și rutarea automată a mesajelor;
- Redirectarea cererilor în mod automat și manual;

- Posibilitatea de personalizare a formei de cereri;
- Editor de text avansat cu posibilitatea adăugării de atașamente;
- Programarea cererilor;
- Calendar pentru tehnicieni;
- Acces bazat pe roluri pentru Tehnicieni;
- Posibilitatea de creare activități multiple pentru o cerere;
- Tratarea activităților dependente;
- Email Spam Filter & Email Notification Filter;
- Clasificarea și rutarea cererilor bazate pe grupuri de lucru;
- Funcționalități de accesare rapidă și istoric de acces la nivel de interfață utilizator;
- Clasificarea cererilor bazată pe categorii;
- Posibilitatea de comunicare a priorităților și a severităților odată cu cererea;
- Escaladarea automată a cererilor bazată pe Reguli de Business;
- Activarea unui mesaj de email în momentul apariției unui eveniment prevăzut într-o regulă de business;
- Posibilitatea de aplicare a unei reguli de business după editarea unei cereri;
- Posibilitatea de continuare cu o sub-regulă de business după ce a fost găsită o regulă;
- Gestionarea eficientă a tehnicienilor bazată pe cozi de suport;
- Posibilitatea de atașare documente la o cerere;
- Posibilitatea de gestionare, editare, asignare și închidere grupuri de tichete;
- Liste de ordine pentru distribuirea tehnicienilor de service și mentenanță;
- Posibilitatea de implementare reguli de închidere a cererilor;
- Posibilitatea de a lega sau uni tichete.

Gestionarea incidentelor

- Clasificarea incidentelor;
- Înregistrarea cererilor de service;
- Posibilitate atașării de informații legate de: Impact, Urgenta, Prioritate, Matrice de prioritate, Stare (ex. Open, On hold, Closed, etc.);
- Posibilitate de a lega un incident de un email (“Mailbox Management”);
- Posibilitate de a crea template –uri de incidente.

Gestionarea SLA

- Posibilitatea de configurare de nivele diferite de escaladare;
- Escaladări automate pe timpul perioadei de escaladare;
- Notificare înainte de expirare SLA.

5.8.14. Componenta de protecție a datelor (salvare / restaurare)

Este solicitată o soluție de protecție a datelor (salvare / restaurare) care să permită salvarea informațiilor din servere, aplicații și baze de date. Produsul trebuie să funcționeze într-un mediu eterogen de sisteme Windows și Linux.

Sistemul propus trebuie să permita realizarea copiilor de siguranță, astfel să asigure creșterea eficienței operaționale, siguranța și agilitatea prin utilizarea noilor politici de backup centralizat.
Se urmareste o soluție enterprise de backup și recuperare a datelor cu urmatoarele caracteristici generale:

- Suport multi-platformă: Windows, Linux, Unix, baze de date și aplicații enterprise
- Automatizare și orchestrare folosind politici centralizate de backup și restaurare automată a datelor.
- Deduplicare avansată cu reducerea volumului de date stocate și a traficului de rețea.
- Restaurare granulară (ex: fișiere individuale, baze de date, mașini virtuale întregi).
- Securitate prin criptare, control de acces și protecție împotriva ransomware.

Solutia va beneficia de mai multe instanțe izolate de backup sub formă de containere, oferind o platformă modulară și flexibilă pentru protecția datelor, cu urmatoarele caracteristici generale:

- Arhitectură containerizată: Fiecare instanță de backup sa ruleze într-un container izolat, similar cu Docker, pentru separare clară și flexibilitate.
- Multi-tenancy: Va permite mai multor echipe/departamente să folosească aceeași infrastructură, dar în medii izolate.
- Scalabilitate: Extinderea capacității va fi simplă, prin adăugarea de instanțe sau noduri.
- Securitate ridicată prin izolarea containerelor, limitand riscul de atacuri interne sau externe.
- Automatizare și orchestrare: Administrarea tuturor instanțelor de backup dintr-o interfață unificată.

Intreaga solutie trebuie sa fie licentiata astfel incat sa asigure backup-ul pentru minim 50TB de date si trebuie sa beneficieze de suport, upgrade si update, precum si dreptul de a deschide cazuri de suport la producator, in perioada de garantie.

Cerinte detaliate:

Soluția furnizată nu trebuie să fie licențiată sau să aibă limitări de configurație în funcție/dependentă de numărul de noduri din arhitectură, numărul de mașini fizice sau virtuale sau numărul de procesoare.
Arhitectura soluției poate fi de tip appliance astfel încât să existe deja configurate bunele practici ale producătorului.
Soluția trebuie să fie organizată în module de aplicații ce vor asigura rularea unor procese automate de salvare și restaurare a datelor, protecția mediilor fizice sau virtuale, protecția directă a aplicațiilor și a sistemelor de operare și monitorizarea politicilor de protecție.
Licențierea soluției de salvare si restaurare date trebuie să includă minim funcționalitățile deduplicare, bare metal restore, replicare, integrare cu medii cloud, integrare cu medii Big Data, integrare cu librării de bandă, integrare cu medii virtuale, independent de platforma utilizată și fără a fi necesară integrarea cu soluții sau componente terțe.
Soluția trebuie să fie flexibilă astfel încât să permită extinderi ulterioare în funcție de dinamica dezvoltării sistemului.
Soluția trebuie să fie flexibilă și scalabilă și să permită instalarea pe două și trei nivele de arhitectură (agent, server de management, echipament de stocare)
Funcționalități licențiate și incluse în configurația oferită:

Soluția trebuie să ofere toate tipurile de backup: full, incremental și diferențial.
Soluția trebuie să identifice segmentele de date unice la nivelul agenților de backup, pentru optimizarea traficului prin rețea.
Soluția trebuie să suporte transferul datelor prin LAN și SAN și să asigure integrarea cu sisteme de tip LDAP pentru autentificarea utilizatorilor.
Soluția trebuie să permită reluarea unui backup nefinalizat cu succes de la ultimul checkpoint și să permită reluarea unei restaurări nefinalizate de la ultimul checkpoint.
Soluția trebuie să permită replicarea automată a imaginilor obținute în procesul de backup la alte appliance-uri din centrul de date principal sau secundar. Replicarea trebuie facută fără rehidratarea imaginilor, în forma lor stocată pe disc (în forma arhivată, deduplicată și criptată).
Soluția trebuie să ofere criptarea datelor replicate, în vederea securizării acestora pe perioada transferului datelor.
Soluția trebuie să permită creare de salvări de date manual și salvări de date prin politici de backup.
Soluția trebuie să permită actualizarea automată a tuturor clienților de backup.
Procesul de deduplicare trebuie să folosească segmente de dimensiuni variabile, pentru eficientizarea factorului de deduplicare. Soluția trebuie să ofere suport pentru aplicarea procesului de deduplicare atât la sursa datelor de protejat cât și la nivelul destinației și să ofere suport pentru deduplicare globală.
Soluția trebuie să permită prevenirea accesului ne-autorizat la aplicația de backup prin mecanisme de control acces bazate pe roluri.

Soluția trebuie să includă mecanisme de protecție informatică, minim:
- împotriva Ransomware, la nivel de client, înainte de backup, la nivelul job-urilor de salvare, în momentul scrierii backup-ului, cat și înainte de executarea unei tentative de restaurare, pentru a determina dacă nu cumva datele au fost deja afectate de ransomware;
- mecanisme de tip „Intrusion Prevention” și „Intrusion Detection” implementate sau integrate de către producătorul soluției;
- Mecanisme de scanare a datelor anti-malware, utilizând un motor anti-malware integrat.
- Mecanisme de prevenire a executiei unor procese, altele decat cele permise pentru activitatea de backup si restaurare

Soluția trebuie să suporte backup și restaurare pentru mediul virtual fără utilizarea unui agent/client. De asemenea trebuie sa suporte restaurare granulară, la nivel de foldere, fișiere sau permisiuni.
Solutia trebuie sa permita restaurarea imediată a unei mașini virtuale (pentru cazuri de urgență maximă)
soluția trebuie să permită expunerea de pe sistemul de backup a unei mașini virtuale direct din fișierele de backup aflate pe sistemul de salvare.
managementul spațiului de stocare din soluție trebuie sa fie gestionat în mod transparent de un sistem de tip software-defined storage, astfel încât orice operație de administrare a sistemului de stocare să fie făcută în timp real, în mediu securizat și controlat, fără întreruperea serviciului de salvare.
soluția trebuie să fie capabilă să creeze zone/volume de salvare a datelor protejate la modificări (de tip WORM).
Soluția trebuie să permită backup de tipul “Incremental Forever”, astfel încât să salveze doar blocurile modificate. Aceste blocuri să poată fi ulterior combinate cu backup-ul anterior pentru a sintetiza un nou full backup, pentru o restaurare mult mai rapidă a datelor.

Soluția trebuie să permită crearea de mount point-uri de tip NFS și CIFS direct din sistemul de deduplicare al datelor, iar datele salvate în mount point-uri trebuie să fie deduplicate și protejate în soluția de backup.
Soluția trebuie să ofere posibilitatea de a efectua Bare Metal Restore (funcționalități de restaurare complet automatizate care includ sistemul de operare, configurația, aplicațiile și datele) pentru Windows, RHEL, SUSE Linux fără a necesita integrarea cu soluții terțe, instrumente native ale sistemului de operare sau instrumente pentru crearea de imagini.
Administrare și monitorizare – funcționalități licențiate și incluse în configurația oferită:
Aplicație pentru management cu acces de la distanță conectare web.
Soluția trebuie să permită administrarea din interfața GUI, CLI și RestfulAPI.
Soluția trebuie să permită monitorizarea activităților într-o interfață web unică, pentru toate locațiile, cum ar fi centrul primar și centrul secundar al beneficiarului.
Interfața unica web trebuie să ofere în timp real detalii cu privire la starea componentelor aplicațiilor, minim avertismente și erori.

Se vor putea gestiona minim următoarele operațiuni:
- stare sistem,
- diagnostice hardware/ software,
- loguri de sistem,
- configurări și setări,
- inventariere,
- software și firmware update.

Componenta de monitorizare a soluției trebuie să identifice în mod automat clienții și seturile de date care nu au o politică de backup asociată.
Pentru a crește gradul de operare și pentru a evita pierderi de date, componenta de monitorizare trebuie să ofere capabilități de a elimina “falsul pozitiv” prin identificarea backup-urilor parțiale sau eșuate dar raportate cu succes de către soluția de backup.
Componenta de monitorizare a trebuie să permită monitorizarea performanței discurilor soluției de backup prin oferirea de rapoarte cu privire la utilizarea discurilor și a capacității scrise pe disc.

Componenta de monitorizare trebuie să ofere vizibilitate asupra sistemelor de stocare, astfel încât să fie cunoscute:
- capacitatea de stocare rămasă disponibilă;
- cine ocupă această capacitate și care este ritmul de creștere;
- unde se află capacitate de stocare ce ar putea fi reutilizată;
- estimarea unui termen în care spațiul de stocare devine indisponibil

Soluția trebuie să conțină o componentă de orchestrare a aplicațiilor și mașinilor virtuale, în scopul automatizării proceselor de disaster/recovery.
Componenta de orchestrare trebuie să permită identificarea mașinilor virtuale și a aplicațiilor și alocarea acestora în diferite grupe de reziliență cu diferite SLA-uri.
Componenta de orchestrare trebuie să ofere în interfața web wizard-uri ajutătoare pentru configurare.
Soluția trebuie să automatizeze complet operațiunile de reziliență care implică mașini virtuale și aplicații complexe multi-nivel.
Soluția trebuie să permită definirea de aplicații multi-nivel ca o singură entitate, pentru ca, în momentul mutării sau a testării, mutării într-o altă locație, toate componentele entității să fie oprite/mutate/pornite în ordinea definită de administrator.

Să permită definirea pașilor pentru pornirea/oprirea componentelor unei aplicații, cum ar fi: baza de date, server de aplicații etc, din interfața web cu posibilitatea de adăugare de scripturi în orice pas al procesului sau oprire automată pentru intervenție manuală.
Aplicațiile multi-nivel tratate ca entități unice să poată fi formate din multiple medii virtuale și fizice (de exemplu serverul web mașina virtuală Hyper-V/serverul de aplicații mașina virtuală VMware și baza de date pe mediu fizic).
Să permită efectuarea de teste pentru recuperare în caz de dezastru în mod de simulare, fără a impacta centrul principal, pentru a valida ca toate procesele sunt funcționale. Testele sub formă de simulare nu trebuie să impacteze sau să modifice parametrii din locația principală.
Să permită în locațiile tip DR (Disaster Recovery) crearea unei rețele dedicate pentru simulările de validare a mutării activității aplicațiilor din locația principală în cea secundară.
Să ofere detalii despre avertismentele și erorile apărute după fiecare exercițiu de simulare.
Soluția trebuie să ofere posibilitatea de a programa acțiunile de simulări de mutare a activității aplicațiilor în altă locație, la momente de timp stabilite de către administratori, iar procesul să se inițieze în mod automat, fără alte intervenții.
Să permită definirea de parametrii de tip RTO și RPO pentru reluarea activității aplicațiilor în locația secundară.
Să permită integrarea cu soluții pentru protecția datelor prin care se pot defini parametrii Service Level Objective, incluzând parametrii RPO de tip Backup/Restore.
Soluția trebuie să ofere propriul mecanism pentru replicarea datelor, posibilitatea de integrare cu mecanismele de replicare ale soluției de backup cât și integrare cu soluții third-party pentru creșterea flexibilității.
Să aibă un mecanism propriu de replicare, care să ofere comprimare, deduplicare și criptare a datelor.
Să permită integrarea cu soluția de backup pentru a iniția în mod automat restaurarea datelor în locația secundară.
Soluția trebuie să ofere roluri pre-definite pentru administrare și integrare cu LDAP pentru identity management.
Soluția trebuie să permită efectuarea de simulări de validare a mutării activității aplicațiilor dintr-o locație în alta la nivel de un singur click în aplicația web, pentru a limita pe cat posibil intervenția umană.
Soluția trebuie să ofere în interfața web detalierea fiecărui pas al execuției proceselor de mutare/migrare/simulare.

5.8.15. Componenta de monitorizare infrastructură

Soluția trebuie să fie de tip enterprise pentru monitorizarea și administrarea infrastructurii IT care este minim compusă din:

- dispozitive de rețea: switch, router, AP, Printer;
- dispozitive/aplicații Securitate: Firewall, Appliance Firewall;
- dispozitive hardware: servere, servere de aplicații;
- gazde de mașini virtuale și mașini virtuale;
- dispozitive și soluții de stocare precum: NAS-uri, soluții stocare pe bandă, RAID-uri;
- Aplicații: SGBD, servere de aplicații.

Soluția propusă trebuie să fie capabilă să monitorizeze și administreze toate dispozitivele ce fac parte din infrastructura sistemului ofertat (switch, router, server, printer, AP, Firewall, Storage, VM's, aplicații etc) folosind un singur panou de comandă

ce conține subpanouri pentru fiecare subcategorie (ex: Server, Network Devices, Storage, Virtualizare, Alarme).

Cerințe Tehnice

Soluția trebuie să analizeze disponibilitatea și performanța dispozitivelor critice de rețea, cum ar fi routerele și switch-uri, monitorizând parametri precum: latența, pierderea pachetelor, bruiajul, timpul de răspuns etc.

Soluția trebuie să analizeze utilizarea lățimii de bandă în rețea utilizând tehnologii avansate de flux precum NetFlow, sFlow, IPFIX, J-flow, Netstream și AppFlow. Soluția trebuie să identifice consumatorii principali de bandă și anomaliile din rețea.

Soluția trebuie sp colecteze informații cheie despre performanța WAN-ului pe mai multe căi, de la sursă la destinație și să analizeze performanța rețelei pentru a vizualiza și deduce unde se află sursa unei întreruperi.

Soluția trebuie:
- să urmărească activitatea utilizatorilor;
- să efectueze gestionarea modificărilor;
- să configureze planificarea backup-urilor;
- să garanteze conformitatea auditurilor;
- să verifice vulnerabilitățile firmware-ului pentru switch-uri, routere și alte dispozitive de rețea.

Soluția trebuie să fie capabilă să aloce adrese IP și să identifice/depaneze problemele comune de rețea cu peste 20 de instrumente, cum ar fi traceroute și PING.
Soluția trebuie să efectueze maparea și monitorizarea porturilor de la switch-uri.
Soluția trebuie să seteze praguri și alerte pentru a avertiza administratorul cu privire la problemele de rețea, erorile de performanță ale serverului, lățimea de bandă și problemele de trafic și alte probleme potențiale care ar putea dăuna infrastructurii.
Soluția trebuie să măsoare/monitorizeze performanța serverelor folosind valori precum: utilizarea procesorului, utilizarea memoriei, spațiul pe disc și temperatura.
Soluția trebuie să stocheze informații istorice pentru referință și depanare.
Soluția trebuie să localizeze de la distanță procesele și serviciile defecte și să le oprească pentru a îmbunătăți performanța.
Soluția trebuie să monitorizeze performanța sistemelor de virtualizare monitorizând valori de performanță complete.
Soluția trebuie să colecteze informații cheie despre performanța dispozitivelor gazdă și a mașinilor virtuale: RAM, HDD, Procesor, temperatura, servicii operaționale etc.
Soluția trebuie să gestioneze eficient activele centrului de date, prevenind timpul de nefuncționare și supra-provizionarea resurselor.
Soluția trebuie să asigure disponibilitatea stațiilor de lucru prin monitorizarea dispozitivelor cheie de rețea, cum ar fi routere, switch-uri, WAPs etc.
Soluția trebuie să fie capabilă să monitorizeze performanța și eficiența a peste 100 de aplicații și tipuri de server. Printre valorile monitorizate trebuie să apară obligatoriu: timpii de răspuns front-end, tranzacțiile sintetice, bazele de date ale aplicațiilor, monitorizarea containerelor.
Soluția trebuie să asigure accesul fără probleme al utilizatorilor la serviciile cloud.
Soluția trebuie să monitorizeze: procesele de la distanță, serviciile, performanța serverului, congestia rețelei, utilizarea lățimii de bandă.

Soluția trebuie să analizeze cauzele problemelor prin existența a peste 20 de monitoare și corelarea datelor furnizate de aceste monitoare pentru deducerea cauzei unei probleme apărute.
Soluția trebuie să permită crearea de fluxuri de lucru dintr-o fereastră interactivă drag-and-drop pentru a automatiza activitățile de rutină și a efectua depanarea de prim nivel, eliberând personalul IT.
Soluția trebuie să permitea efectuarea de planificare avansată a capacității utilizând algoritmi predictivi.
Soluția trebuie să permită setarea de alerte pentru capacitățile estimate pentru a putea fi luate măsuri în timp util pentru a înlocui resursele de rețea care sunt pe cale să fie epuizate.
Soluția trebuie să permită escaladarea alarmelor prin reguli de escaladare ce pot fi configurate pentru a recunoaște alarmele în funcție de nivelul de severitate al alarmei, grupul de dispozitive, timpul scurs și impact.
Soluția trebuie să includă algoritmi de învățare automată și predictivi pentru a determina valorile de prag ideale pentru fiecare valoare.
Soluția trebuie să permită vizualizarea de informații cheie cu privire la rețea dintr-o singură platformă unificată de monitorizare a rețelei.
Soluția trebuie să includă un panou principal de unde se pot vizualiza: rapoarte, hărți și grafice, dispozitive monitorizare, informații despre rețea și alerte.
Soluția trebuie să permită vizualizarea întregii, rețele până la fiecare conexiune individuală.
Soluția trebuie să poată descoperi direct dispozitive necunoscute din rețea.
Soluția trebuie să permită accesarea de informații cheie făcând clic pe fiecare nod și descifrarea de conexiuni complicate.
Soluția trebuie să includă și un panou pentru vizualizarea 3D și interactivă a Rack-urilor de servere și hărților de rețea.
Soluția trebuie să permită descoperirea unei rețele folosind fișiere CSV.
Soluția trebuie să suporte descoperirea unei rețele folosind tehnica de tip “Single Node Discovery”.
Soluția trebuie să permită programarea scanărilor de rețea.
Soluția trebuie să suporte descoperire Layer 2.
Soluția trebuie să includă un motor automat bazat pe reguli pentru descoperirea și analizarea unei rețele.
Soluția trebuie să fie capabilă să descopere și să monitorizeze medii de rețea virtuale.

Soluția trebuie să fie capabilă de următoarele tipuri de monitorizare:

- Monitorizare Disponibilitate
- Monitorizare Interfețe
- Monitorizare SNMP
- Monitorizare VMI
- Monitorizare CLI
- Monitorizare folosind agent
- Monitorizare VMware
- Monitorizare Hyper-V
- Monitorizare XEN
- Monitorizare Nutanix
- Monitorizare UCS
- Monitorizare Procese
- Monitorizare Servicii Windows
- Monitorizare port TCP
- Monitorizare Script

- Monitorizare Eventlog
- Monitorizare Syslog
- Monitorizare File Folder
- Monitorizare Active Directory
- Monitorizare MSSQL
- Monitorizare Hardware
- Monitorizare Vlan
- Monitorizare Cisco ACI
- Monitorizare Meraki
- Monitorizare “Network Patch Analysis.

Soluția trebuie să suporte următoarele tipuri de autentificare pentru utilizatori:
- Local
- AD
- Radius
- Pass Through
- Rest APi.

Soluția trebuie să ofere următoarele tipuri de panouri de comandă interactive :
- Panouri Customizate
- Panouri Speciale pentru fiecare utilizator în functie de rol
- Panou NOC
- Diverse Tipuri de “Widges”.

Soluția trebuie să ofere următoarele capabilități când vine vorba despre hărțile generate pentru rețea și infrastructura IT:
- Business Views
- Harti pentru mediul Virtual
- Integrare Cu Google Maps
- Vizualizarea 3D a centrului de date.

Soluția trebuie să includă următoarele capabilități de escaladare, remediere și escaladare a problemelor:
- Monitorizare Alarme
- Escaladare Alarma
- Monitorizare SNMP Trap
- Automatizare prin WorkFlow
- Integrare cu soluții terțe
- Profiluri de Notificare.

Soluția trebuie să includă un panou de comandă complet structurat în următorul mod:
- Panou Principal
- Subpanou de Inventar
- Subpanou Dispozitive Rețea
- Subpanou Servere
- Subpanou Mediul Virtual
- Subpanou Dispozitive și Mediul De Stocare
- Subpanou Alarme
- Subpanou Hărți 3D și 2D
- Subpanou Aplicații
- Supanou Fluxuri de Lucru

- Subpanou Setări și Configurare Admin
- Subpanou Rapoarte.

Soluția trebuie să furnizeze următoarele informații despre dispozitive precum switch, router, ap, printere, firewalls:

- IP
- DNS
- Model
- Producător
- Categorie
- Credențiale Logare
- Status
- Interfețe
- Analiza a traficului
- Tipuri de monitoare disponibile.

Soluția trebuie să furnizeze următoarele informații despre dispozitive precum servere:

- Status
- IP
- DNS
- Tip (Sistem de Operare:Windows Linux, etc)
- Categorie (Ex: Domain Controler)
- Furnizor
- Credențiale
- Interfețe
- Procese Active
- Software Instalat
- Procese Active
- CPU, HDD, DISK, Operații I/O, Memorie RAM, Latență.

Soluția trebuie să furnizeze următoarele informații despre dispozitive de tip: “Gazde Virtuale”, mașini virtuale:

Gazde Virtuale:

- Status
- IP
- DNS
- Tip (Sistem de Operare: Windows, Linux, etc)
- Categorie (ex: Domain Controler)
- Furnizor
- Credențiale
- interfețe
- Procese Active
- Software Instalat
- Procese Active
- CPU, HDD, DISK, Operații I/O, Memorie RAM, Latență
- Mașini Virtuale Susținute
- Sistem Virtualizare Folosit.

Mașini Virtuale:

- Status

- IP
- DNS
- Tip (Sistem de Operare:Windows Linux, etc)
- Categorie (Ex: Domain Controler)
- Furnizor
- Credențiale
- Interfețe
- Procese Active
- Software Instalat
- Procese Active
- CPU, HDD, DISK, Operații I/O, Memorie RAM, Latență
- Gazda
- Limite RAM
- Limite CPU.

Soluția trebuie să furnizeze următoarele informații despre dispozitive de tip Stocare:
- IP
- DNS
- Model
- Producător
- Categorie
- Credențiale Logare
- Status
- interfețe
- Număr Serie
- Disk-uri Capacitate
- Lun-uri (Pool Stocare, Volume, Mărime, Folosire, Ocupare)
- Valori Precum: RAM, Operațiuni Scriere Citire, RAID.
- interfețe Conexiune la Rețea.

Soluția trebuie să furnizeze următoarele tipuri de alarme și să permită configurarea acestora în funcție de diverși parametri:
- Eventlog
- Syslog
- Trap
- NFA
- Firewall
- Web
- Stocare
- Evenimente
- Analiza Cauză.

Soluția trebuie să fie capabilă să notifice personalul autorizat prin mai multe medii de comunicare:
- Email
- Ticket
- Alarma WEB
- Panou Comanda Notificare.

Subpanoul dedicat Hărților infrastructurii trebuie să includă:
- Hărți Layer 2

- Hărți 3D ale rack-urilor de servere
- Business Views pentru diversele sedii
- Hărți 3D pentru Camele de server și rack-uri.

Subpanoul dedicat monitorizării aplicațiilor și serviciilor trebuie să furnizeze următoarele informații:

- Date despre disponibilitatea și sănătatea Website-urilor
- Date despre disponibilitatea, sănătatea și performanța serviciilor precum: AD, IIS, Oracle, MSSQL
- Servicii Cloud: Azure, AWS, Huawei, Kubernetes
- Monitorizarea Experienței Utilizatorilor de Servicii
- Alarme
- Rapoarte.

Soluția trebuie să furnizeze următoarele tipuri de rapoarte predefinite, dar trebuie să ofere dreptul utilizatorului să își creeze rapoarte customizate:

- Rapoarte Integrate
- Rapoarte Sistem
- Rapoarte Performanță și Sănătate
- Rapoarte Disponibilitate și Răspuns
- Rapoarte Inventar
- Rapoarte Wan RTT
- Rapoarte VOIP
- Rapoarte Servere Virtuale
- Rapoarte Stocare
- Rapoarte Forecast
- Rapoarte WLC
- Rapoarte Avansate
- Programare Rapoarte
- Raport Căutare
- Rapoarte Profiluri
- Rapoarte Anchete
- Rapoarte Consolidate
- Rapoarte Capacitate
- Comparare Rapoarte
- Rapoarte Geolocație
- Rapoarte LAN WAN
- Rapoarte Hardware
- Rapoarte Firmware
- Rapoarte Inventar
- Rapoarte Sănătate Rețea
- Rapoarte Gestionare Dispozitive
- Rapoarte Audit
- Rapoarte Configurații
- Rapoarte Schimbări
- Rapoarte EOL, EOS
- Rapoarte Conformitate
- Rapoarte Configurare
- Rapoarte PCI
- Raport Utilizatori
- Raport Audit Utilizatori

- Raport CVE ID
- Raport Dispozitive expuse
- Raport Vulnerabilități Firmware
- Rapoarte Firewall
- Rapoarte VPN
- Rapoarte Reguli
- Rapoarte IP
- Rapoarte API.

Soluția cerută trebuie să fie de tip COTS și licențiată în mod "Perpetual" sau de tip subscripție valabilă pe toata perioadă de garanție și să funcționeze pe arhitectură de tip "on-premise".

5.8.16. Componenta de instruire în vederea conștientizării securității pentru utilizatori și administratori

Se dorește achiziționarea unei **platforme moderne de managementul riscului de securitate ce are la bază analiza comportamentului uman,** respectiv o platformă de management al riscului uman care oferă cursuri de conștientizare a securității, bazate pe nevoile și nivelul de risc ale angajaților.

Necesitatea acestei achiziții derivă din faptul că este cunoscut că, la nivel de organizații, majoritatea pierderilor de date sunt provenite din lipsa de informare a utilizatorilor asupra diverselor riscuri de securitate și a modalităților de adresare și reducere a acestora.

Aceasta platformă trebuie să fie una modulară, ce trebuie să acopere cel puțin următoarele necesități:

- interfață prietenoasă și intuitivă ce va prezenta situații, rapoarte privind șabloanele de risc comportamental;
- capabilități de integrare cu sisteme de securitate (de exemplu, SIEM, CASB, EDR, Web Filter, Email DLP) deja instalate, pentru a măsura comportamentele de securitate;
- capabilități de monitorizare și analizare a comportamentelor utilizatorilor;
- capabilități de detectare a modalităților de pierdere a datelor și a breșelor comportamentale de securitate;
- mecanisme de măsurare a riscului de securitate uman;
- capabilități de educare / instruire a utilizatorilor privind adresare țintită a acestor comportamente;
- capabilități de intervenție / ghidare țintită privind situațiile de risc;
- capabilități de creare a fluxurilor pentru a preveni / combate comportamente inadecvate;
- capabilități de învățare a comportamentelor utilizatorilor sistemelor informatice în vederea automatizării combaterii / prevenirii riscului uman de securitate;
- oferă utilizatorilor un canal de comunicare bidirecțională și experiență de învățare socială;
- înțelege și gestionează riscul uman, oferind atât acțiuni de îmbunătățire automate (cu un singur clic), cât și manuale, sub forma unor metode de tratare a riscurilor dovedite istoric;

- soluția trebuie să ofere echipelor de securitate vizibilitatea necesară pentru a furniza intervenții direcționate (sesiuni de conștientizare a securității, ateliere de lucru, procese de reinginierie, tehnologie și instrumente) și pentru a gestiona mai eficient riscul de pierdere a datelor cauzate de comportamentul uman;
- simplificarea conștientizării securității;
- furnizarea de formare orientată, bazată pe nevoile și riscurile angajaților;
- livrarea de conținut activ direct către utilizatori - prin Slack și browser web;
- furnizarea de rapoarte de înaltă precizie și tablouri de bord interactive;
- catalogul eLearning trebuie să acopere întregul spectru, așa cum este certificat de GCHQ, NCSC și APMG din Marea Britanie. Acesta trebuie să cuprindă 20 de module interactive scurte (5 minute), cu animație 2D, disponibile în 18 limbi, inclusiv în limba română;
- biblioteca va conține materiale precum videoclipuri scurte, postere, screensavere, imagini de fundal sau buletine informative;
- subiectele de instruire privind conștientizarea securității trebuie să acopere următoarele teme:
    - Introducere în Securitatea Informației,
    - Securitate e-mail și phishing,
    - Securitate Web,
    - Protecție împotriva programelor malware,
    - Medii de stocare (dispozitive portabile),
    - Cloud Computing,
    - Lucru de la distanță (utilizare Wi-Fi publică),
    - BYOD și securitatea dispozitivelor mobile,
    - Criptare,
    - Parole,
    - Inginerie socială,
    - Rețele sociale,
    - Clasificarea informațiilor,
    - GDPR,
    - Răspuns la încălcare procedurilor (raportarea incidentelor);
- soluția trebuie să permită organizațiilor să îndeplinească cerințele de instruire și conștientizare în materie de securitate impuse de standardele de securitate și reglementările specifice sectorului, cum ar fi GDPR UE, NIS, ISO/IEC 27001, PCI DSS, SSAE16/SOC 1/SOC 2, SOX, NIST-SP800-50 , GCC NESA/ISR;
- soluția trebuie să aibă posibilitatea să dețină un nivel suplimentar de insight (inteligență privind riscul uman) - atitudinile utilizatorilor, intenția lor de a se conforma, sentimentul față de securitate și nivelurile de implicare (date subiective). Toate aceste măsurători vor fi efectuate în timp ce personalul își finalizează procesul de conștientizare a securității.
- trebuie să accepte sistemul de management al identității pe mai multe domenii (SCIM v2.0). Acest lucru este necesar pentru a permite să sincronizeze automat grupurile de utilizatori între soluțiile de gestionare a identității conforme (cum ar fi Okta, Azure Active Directory sau OneLogin) și soluția ofertată.
- este necesară și opțiunea tradițională de a integra și actualiza manual cursanții prin importarea fișierelor de tip CSV sau introducerea manuală prin portal;
- să se poată integra în viitor, cu sistemele de securitate precum SIEM, CASB, EDR, soluții de securitate Email/Web, DLP prin care să preia informații precum

jurnalele și evenimentele de la utilizatorul final, rețea și cloud pentru a măsura comportamentul utilizatorilor;
- soluția trebuie să aibă posibilitatea să analizeze aceste date împreună cu datele subiective, utilizând învățarea automată nesupravegheată și pe baza unor modele științifice solide (economie comportamentală și psihologie) pentru a prezice riscul uman. Algoritmii platformei trebuie să recomande noi acțiuni de îmbunătățire.

5.8.17. Componenta de monitorizare evenimente de securitate (SIEM)

Platforma de servicii publice digitale va include o soluție de monitorizare a evenimentelor de securitate bazată pe o aplicație software introdusă deja în circuitul comercial.

Nu se accepta dezvoltări, ci doar configurări sau personalizări, pentru a se putea permite implementarea soluției pentru a răspunde cerințelor tehnice din cadrul proiectului.
Soluția ofertată trebuie să includă în varianta propusă toate cerințele tehnice enumerate în continuare precum și toate costurile asociate.

Soluția va avea în scop monitorizarea întregii infrastructuri IT a proiectului, din punct de vedere al auditului de securitate. Astfel, soluția va colecta evenimente de audit din toate echipamentele, aplicațiile, bazele de date etc. prezente în proiect.

Modul de furnizare în proiect

Soluția va fi furnizata cu licențiere perpetuă și va fi instalată în infrastructura beneficiarului.

Interfața soluției

Interfața soluției va fi de tip WEB. Astfel, soluția va furniza o interfață WEB pentru operarea și administrarea acesteia, compatibilă cu orice browser modern (Chrome, Microsoft Edge etc.).

Depozite de date

Soluția va stoca datele cel puțin în două moduri (depozite):
- Arhiva - datele sunt depozitate pentru păstrare pe termen lung, comprimate:
    - Rata mare de compresie - minim 1 la 20.
    - Va oferi mecanisme anti-repudiere: criptare și semnare digitala a datelor.
- Online - datele sunt depozitate indexat cu accesare rapida pentru nevoi investigaționale, de raportare etc.

Nu se acceptă tehnologii proprietare pentru depozitele de date - datele sunt ale beneficiarului și accesarea/utilizarea acestora nu trebuie să fie dependentă de soluția ofertată (subscripție / mentenanță / suport etc.).

Componentele principale ale soluției

Modul afișare
Soluția va putea afișa în format tabelar toate evenimentele colectate. Interfața va putea fi configurabilă din punctul de vedere al câmpurilor ce pot fi vizualizate și va permite filtrări avansate precum și ordonări ale evenimentelor.

Modul panouri de bord (dashboards)
Soluția va oferi vizualizări grafice pentru evenimentele colectate, sub forma de tablouri de bord (dashboards). Acestea vor putea fi configurabile pentru fiecare utilizator, în funcție de nevoile de business. De asemenea, într-un grup, pot fi asociate tablouri pentru tehnologii diferite și va permite căutarea în toate tablourile relativ la un criteriu sau set de criterii comune.

Modul Raportare
Soluția va furniza un modul de rapoarte. Acesta va conține implicit rapoarte de tip Best practices pentru diverse tehnologii precum și de conformare pentru GDPR și pentru standardele ISO 27001, COBIT, FISMA, SOX, PCI-DSS și, de asemenea, modulul va permite crearea de noi rapoarte, editarea rapoartelor existente, va conține funcții de planificare a rulării și transmiterii rapoartelor și funcții de exportare a rezultatelor rapoartelor.

Modul Alertare
Soluția va dispune de un modul de alertare. Acesta va include implicit alerte de tip Best practices pentru diverse tehnologii. Alertele vor fi definite/editate într-o interfață grafică, intuitivă. Alertele predefinite trebuie să acopere o gamă largă de tehnologii.

Modul tip UEBA
Soluția va furniza un modul de tip UEBA pentru identificarea și alertarea asupra acelor acțiuni care ies dintr-un șablon de comportament considerat normal.

Modul de analizare performanță
Soluția va putea colecta și afișa date referitor la performanța mașinilor de la care colectează evenimente de audit. Astfel, vor fi afișate date referitoare la încărcarea procesoarelor, memoriei, spațiul disponibil pe discuri etc., atât în timp real, cât și istoric.

Modul Scaner de vulnerabilități
Soluția va oferi posibilitatea de a integra nativ (API) un modul de scanare de vulnerabilități. Acesta va detecta vulnerabilități de securitate din sisteme, aplicații web și echipamente de rețea. Odată descoperite, acestea trebuie să poată fi folosite în procesele atât de corelare cât și investigaționale ale organizației.

Modul Case / Incident management
Soluția va avea un modul de tip incident management. Prin intermediul acestui modul, personalul de securitate poate desfășura în mod colaborativ activități de investigare a incidentelor de securitate.
Soluția va oferi un workflow complet pentru analiști și asigură răspunsul la incidente de securitate prin crearea și declanșarea în mod automat de playbook-uri.

Administrare
Administrarea soluției se va face folosind sisteme de permisionare tip RBAC (Role Based Access Control), atât pentru accesul în date cât și pentru configurațiile sistemului. Operatorii soluției nu trebuie să poată modifica datele sistemului.
Soluția se va putea integra cu sisteme de tip LDAP pentru autentificare unitară.

Colectarea datelor
Va fi posibilă colectarea evenimentelor din segmente diferite de rețea.
Soluția va permite colecția datelor prin intermediul agenților sau direct din sistemele sursă. De asemenea, soluția va furniza capacități de colectare fluxuri de evenimente de tip Syslog, NetFlow, sFlow sau direct prin sisteme tip TAP.

Agenții vor transmite datele colectate către serverul de procesare, în format comprimat și criptat
Agenții de colectare vor putea efectua colectare filtrată și vor furniza capacități de procesare / preprocesare / postprocesare a datelor.
Agenții vor asigura mecanisme de protecție împotriva alterării datelor colectate la colecție, în tranzit sau repaos.
Soluția va furniza un modul de management al agenților. Prin intermediul acestui modul va fi posibila instalarea, dezinstalarea, precum și configurarea parametrilor de funcționare a agenților.
Operațiunile de administrare a agenților se vor putea efectua pentru fiecare agent în parte sau pentru mai mulți agenți în același timp.
Soluția va dispune de un modul de management al surselor de date. Astfel, adăugarea surselor de date se va efectua din interfața grafică a soluției și vor fi disponibile capacități de tip autodiscovery. Soluția va identifica automat tipurile de evenimente comune.
Soluția va oferi capacități de tip auto-discovery pentru infrastructura în care este implementată.
Va fi oferit implicit un modul de tip asset management din perspectiva security prin intermediul căruia pot fi populate următoarele informații: nume, nivel de criticitate, adresă/adrese IP, adresă/adrese MAC, zonă de rețea, vulnerabilități identificate.
Soluția va putea genera evenimente pentru interpretarea unor situații sau evenimente specifice.
Evenimente de aplicații generate sub formă de înregistrări text sau tabele de audit în baze de date de tip MS SQL, Oracle, MariaDB, PostgreSQL.
Mesaje syslog generate de echipamente de rețea, echipamente de tipărire, sisteme de control al accesului sau alte echipamente.
Colectarea evenimentelor de securitate la nivel de sistem de fișiere, pentru tehnologii Linux și Windows.
Colectarea de metadate din sisteme terțe (Active Directory, informații WMI, SNMP, sisteme de management al identităților), pentru utilizarea lor în procesul de corelare.
Soluția va oferi funcționalități avansate de configurare a conectorilor, astfel încât să acomodeze fișiere aparent neparsabile:

- Fișiere cu evenimente multiline (număr dinamic de linii, evenimente separate prin newline / datetime),
- Fișiere XML,
- Fișiere free text.

Filtrare evenimente pe fluxul de colectare
Soluția va oferi capacități avansate de filtrare a evenimentelor la destinație. Filtrarea poate fi efectuată astfel:

- Filtrare tip „drop event",
- Filtrare cu trimiterea evenimentelor doar în arhivă,
- Filtrare fără trecerea evenimentelor prin motorul de corelare, cu trimiterea acestora doar în baza de date on-line și arhivă.

Soluția va oferi capacități de filtrare a evenimentelor la sursă.

Depozite de date
Soluția va oferi o funcție de anonimizare sau de pseudonimizare a datelor:

- Cu posibilitate de setare manuală a câmpurilor pe tipuri de surse de date;
- Cu posibilitate de setare automată a anumitor câmpuri - în funcție de forma/conținutul acestora (ex. CNP etc.) pentru toate sau anumite surse de date, precum și posibilitate de excludere.

Importarea datelor din arhivă în depozite online
Evenimentele din arhivă pot fi importate în baze de date on-line pentru activități investigaționale, de raportare etc. Importul se poate face imediat sau programat cu posibilitatea de importare filtrată a evenimentelor.
Activitățile de import vor fi efectuate din interfața grafică a soluției, fără a fi necesară instalarea sau folosirea unor elemente sau aplicații terțe.
Soluția va furniza funcție de tip RTBF (right to be forgotten) pentru toate evenimentele din baza de date on-line și arhivă.
Depozitul on-line trebuie să poată fi scalat în funcție de nevoie, oricând pe durata de utilizare a soluției, fără a implica niciun cost de licențiere pentru baza de date.
Arhiva poate fi scalată în funcție de nevoie, oricând pe durata de utilizare a soluției, fără a implica niciun cost de licențiere pentru baza de date.

Funcții de export evenimente
Soluția va putea fi configurată să redirecționeze evenimente către soluții terțe.
Evenimentele pot fi transmise în format brut sau în format normalizat (syslog, .json, CEF).
Evenimentele pot fi transmise filtrate (doar de la anumite surse, doar de un anumit tip etc.).
Soluția va putea exporta alerte. Exportul se poate face în mod manual, una câte una sau selecție, precum și în mod automat. Se vor putea defini criteriile de export pentru alerte, pentru fiecare alertă în parte sau bulk, în formate și pe medii diferite: Email, call-uri de API-uri, syslog.
Configurările pentru redirecționarea evenimentelor se vor face din interfața grafică a platformei cu granularitate până la nivel de tip de eveniment, alertă etc.

Funcții de monitorizare servicii componente și de alertare / repornire-restaurare
Soluția va include capacități de alertare asupra statusului serviciilor componente, precum și de restaurare automată a acestora în caz de oprire.
Vor fi posibile alerte inclusiv pe praguri de ingestie evenimente/număr de evenimente care așteaptă sa fie ingerate/procesate de soluție.

Funcții de self-audit
Soluția va dispune de funcții de tip self-audit. Astfel, vor fi auditate toate operațiunile efectuate de utilizatorii și de serviciile componente ale soluției.

Funcții de monitorizare resurse
Soluția va furniza funcționalități de monitorizare a resurselor mașinilor de la care colectează evenimente de audit. Astfel, va putea monitoriza gradul de încărcare pentru discuri, memorie, CPU, cu afișarea parametrilor în timp real dar și a istoricului pentru minim 24 ore.

API
Soluția trebuie să pună la dispoziția utilizatorului un API de integrare pentru surse de date noi sau includerea de logică în procesele de colectare, corelare sau alertare a datelor pentru a putea acomoda cele mai exigente cerințe de securitate.

Funcționalități Panouri de bord (dashboards)
Soluția va furniza un modul prin care vor fi afișate grafic agregări de evenimente sub forma de panouri de bord.
Panourile de bord vor putea fi asociate (grupate) în grupe de panouri.
Fiecare utilizator al soluției trebuie să aibă posibilitatea să își configureze propriile panouri din interfață, în conformitate cu permisiunile sale.

Soluția va putea efectua filtrare și afișare în toate panourile relativ la un singur criteriu.

Corelare
Soluția va conține out of the box alerte pe multiple tehnologii, pe scenarii de bune practici.
Toate evenimentele ingerate în soluție trebuie să poată fi incluse în motorul de corelare.
Soluția va oferi posibilitatea de a exclude evenimente din fluxul de corelare. Filtrarea se va face per sursă de date sau per identificator de tip de eveniment.
Procesele de corelare vor putea fi executate în mai mulți pași - corelări din unul sau mai multe evenimente/secvențe de evenimente cu praguri de activare reguli individuale.
În urma alertelor declanșate, soluția trebuie să poată rula acțiuni automate. Acțiunile vor putea fi implicite, pe tehnologii sau vor putea fi personalizate.
În procesul de configurare/personalizare a acțiunilor automate, trebuie să poată fi incluse elemente/câmpuri din evenimentele ce au generat alerta.
Soluția va putea transmite notificări pentru alerte.

Noi reguli de alertare vor putea fi definite în baza unor criterii singulare, corelate sau de excludere, inclusiv:

- Eveniment singular – când un singur eveniment indică situația care necesita remediere,
- Evenimente corelate – când trebuie detectată o situație specifică, definită în termeni de evenimente care survin în aproximativ același timp,
- Cumul de evenimente – când trebuie detectată o situație în care acțiuni similare se derulează într-o succesiune rapidă,
- Lipsa unui eveniment – când se așteaptă evenimente specifice într-un anumit interval de timp sau într-o anumită situație dată, dar acest sau aceste evenimente nu mai au loc,
- Lipsa unui eveniment corelat – când trebuie urmărite situații sau procese în care acțiunile subsecvente nu mai au loc,
- Reguli particularizate – când se dorește detectarea unei situații care nu poate fi definită prin celelalte modele de reguli.

Managementul alertelor va avea minim următoarele caracteristici:

- Posibilitate de marcare a alertelor (acknowledge) de tip one-by-one sau bulk.
- Posibilitate de marcare automată a alertelor – în funcție de scorul de securitate/gravitate.
- Posibilitate notare rezoluție pentru alerte. Notarea se va putea efectua one-by-one sau bulk.

Soluția va oferi un workflow complet pentru analiști și va putea asigura răspunsul la incidente de securitate prin crearea și declanșarea în mod automat de playbook-uri, cu o serie de playbook -uri oferite în mod implicit (out-of-the-box).
Soluția va putea integra în mod nativ feeduri de securitate de tip open source / subscription based. De asemenea, soluția va include un feed propriu de securitate ce trebuie să ofere minim informații tip: IP-uri, domenii și url-uri malițioase.
Soluția va furniza capacități de corelare automată pentru informațiile din evenimente versus informațiile conținute în feedurile de securitate. Astfel, vor fi identificate automat sisteme ce comunică cu IOC-uri provenind din propria infrastructură.
Alertare automată a evenimentelor de trafic de risc (către IP-uri malițioase) din cadrul organizației, atât la nivel de evenimente în curs, cât și (automat) anterioare.
Soluția va oferi posibilitatea de verificare automată/manuală în bazele de date (online și arhivă) pentru identificarea IOC-urilor. Verificarea automată poate fi declanșată la apariția unor vectori noi de risc sau poate fi manuală, efectuată în mod bulk.

Monitorizare tip UEBA

Soluția va monitoriza activitatea utilizatorilor pentru procese de login, cu detecția modificărilor șablonului uzual pentru: Logon-uri interactive, logon-uri automate sau logon-uri de la stații noi.
De asemenea, va monitoriza activitatea de login a utilizatorilor pe VPN, cu detecția locațiilor (tarilor, orașelor) noi de conectare per utilizator în parte.
Soluția va monitoriza și detecta serviciile noi pornite, fie nivel de organizație fie la nivel de server.
Soluția va permite crearea unui scor de risc pentru fiecare tip separat de asset, grup de utilizatori precum și tip de evenimente pentru detecția automată a acțiunilor cu un grad mare de risc.

Afișare evenimente

Soluția va dispune de un modul de afișare tabelară a evenimentelor cu posibilități avansate pentru filtrare și ordonare
Viteza de răspuns pentru filtrări și căutări în baza de date online va oferi o bună experiență de utilizare. Astfel, o căutare simplă, după un singur criteriu, în toată baza de date online va returna rezultate în mai puțin de 10 secunde.
Filtrele aplicate pot fi salvate pentru o utilizare ulterioară. De asemenea, filtrele trebuie să poată fi salvate ca și rapoarte/alerte/dashboard.
Utilizatorii vor putea selecta informațiile (coloanele) ce vor fi vizibile în interfață.
Utilizatorii pot accesa vizualizare detaliată pentru fiecare eveniment.
Interfața de căutare a sistemului de audit va oferi posibilitatea de combinare a operatorilor logici de căutare ("AND", "OR", "NOT") și vor putea fi definite expresii complexe cu operatori paranteză (inclusiv paranteze imbricate).
Va suporta corelarea jurnalelor pentru toate seturile de date, indiferent de sursă și/sau tipul de jurnal.
Va permite detectarea automată a autentificărilor suspecte.
Soluția poate asigura suport pentru rularea unor comenzi direct de la nivelul evenimentelor colectate, astfel încât să fie obținute informații suplimentare (de exemplu: ping, traceroute, whois, nslookup etc.).

Rapoarte

Soluția va furniza, în cadrul modulului de raportare, un set complet de rapoarte pentru standarde conformitate uzuale: SOX, ISO 27001, GDPR.
Vor fi disponibile în mod implicit rapoarte de tip best practices pentru multiple tehnologii.
Toate rapoartele predefinite pot fi personalizate.
Titlurile rapoartelor trebuie să poată fi modificate.
Rapoartele vor include pe prima pagină informații succinte despre perioada evenimentelor din raport/ce evenimente sunt cuprinse etc.
Rapoartele vor conține grafice relativ la informația afișată în acestea.
Rezultatul rapoartelor poate fi exportat ca și fișier în următoarele formate: PDF, HTML, XLSX, XLS, CSV, XML
Definițiile de rapoarte pot fi exportate unul cate unul sau selecție (mai multe).

Scanner de vulnerabilități

Soluția trebuie să poată oferi direct integrare nativă cu un scanner de vulnerabilități. Integrarea trebuie să poată fi făcută direct în interfață, fără a fi nevoie de părăsirea interfeței de administrare.

Soluția trebuie sp ofere rapoarte de vulnerabilități oferite de către scanner pentru analiza în procesul de alertare.

Incident și case management

Soluția trebuie să includă facilitați de incident management/ mecanism integrat de lucru colaborativ în care pot fi definite grupuri de destinatari organizați pe mai multe niveluri.
Se pot face alocări automate sau manuale către analiștii de securitate, precum și escaladarea automată către nivelurile următoare.
Analiștii trebuie să poată deschide cazuri de investigații din alerte și evenimente.
Accesul la cazuri trebuie să se poată face granular.
Soluția va fi instalată în infrastructura beneficiarului.
Soluția va fi furnizată sub forma unui appliance virtual.
Soluția propusă va avea o arhitectură de tip all-în-one - toate serviciile și componentele soluției vor fi instalate pe aceeași mașină.
Soluția va avea posibilitatea de a distribui pe orizontală serviciile și componentele astfel încât, pentru o eventuală nevoie de scalare, să permită utilizarea infrastructurii existente a beneficiarului.
Eventualele servicii ocazionate de scalarea soluției vor fi cotate la un preț similar serviciilor de configurare din prezentul proiect.
Soluția va fi licențiată astfel încât să acomodeze un volum de minim 5.000 EPS (events per second) sau 350 GB data / zi sau minim 1.500 noduri - dacă licențierea este efectuată în funcție de parametrii menționați.
Nu va exista nicio limitare de licență pentru volumul de date întreținut de soluție (volumul bazelor de date online și arhiva), iar acesta va putea fi scalat, pe parcursul sau după încheierea proiectului, în funcție de nevoile beneficiarului, fără niciun cost suplimentar de licențiere pentru dimensiunea depozitelor de date.

Servicii

Soluția va fi instalată și configurată de către furnizor.
Furnizorul va oferi consultanță pentru activarea controalelor de securitate astfel încât să fie generate și colectate evenimente de audit din toate componentele proiectului.
Furnizorul va susține servicii de transfer cunoștințe (training) pentru utilizatorii și operatorii soluției. În acest sens, furnizorul trebuie să dețină o certificare de competențe de la producătorul soluției pentru instalare și configurarea soluției propuse.
Implementarea va fi conformă cu standarde și reglementări obligatorii, precum GDPR și directiva NIS 2 privind asigurarea unui nivel comun ridicat de Securitate a rețelelor și sistemelor informatice utilizate.

5.9. SERVICII

5.9.1. Serviciile de livrare, instalare echipamente hardware

Pentru livrarea și implementarea infrastructurii hardware solicitate vor trebui asigurate următoarele activități:

- Livrarea echipamentelor necesare funcționării soluției informatice;
- Servicii de livrare, instalare și punere în funcțiune echipamente HW;
- Respectarea graficului de livrare a echipamentelor ce urmează a fi recepționate;
- Derularea activităților corespunzătoare recepției cantitative a echipamentelor;
- Livrarea documentației tehnice a echipamentelor recepționate;

1. Realizarea Documentației de instalare

Împreună cu Beneficiarul se va agrea formatul documentului și procedurile de etichetare a echipamentelor în cadrul unor discuții tehnico-procedurale preliminare.
Conform cerințelor inițiale, documentația de instalare asociată site-ului va conține obligatoriu informații privind:

- Numele și codul locației;
- Persoane de contact, atât din partea Beneficiarului, cât și din partea Furnizorului;
- Tipul și codul echipamentelor ce vor fi instalate în site, conform cu propunerea tehnică detaliată anterior;
- Diagrama conexiunilor fizice între echipamente și poziția acestora în rack-ul/urile existent/e la beneficiar;
- Tabele cu informații privind conexiunile dintre echipamente (va conține tipul de cablu folosit, etichetarea, ce echipamente conectează, etc.) ;
- Conexiunile acestora la prizele de electroalimentare în rack-ul/urile ofertat/e sau existent/e la beneficiar.

Procedurile de etichetare vor fi elaborate de comun acord cu Beneficiarul și vor conține obligatoriu informații privind:

- Procedura de etichetare fizică a echipamentelor hardware, a cablurilor de interconectare și a cablurilor de electroalimentare;
- Proceduri de etichetare electronică la conectarea remote pe echipamente pentru administrare (prompt echipamente, bannere de login, descriere interfețe, etc), dacă este cazul.

2. Instalarea echipamentelor în site

Instalarea și punerea în funcțiune a echipamentelor vor respecta cerințele standardului EIA/TIA 568 folosind o echipă de specialiști certificați în instalarea și configurarea echipamentelor ofertate de către producătorii acestor echipamente sau de către centre de training autorizate de către producător în acest sens.

Pentru fiecare site se vor efectua următoarele operații:

- Transportul echipamentelor de către Furnizor la sediul Beneficiarului în vederea instalării și punerii în funcțiune, respectând normele de transport impuse de către producător și de ambalare (în cazul în care echipamentele livrate nu sunt ambalate în ambalajul original);
- Instalarea fizică a fiecărui echipament în rack;
- Interconectarea echipamentelor (folosind cabluri UTP cat. 6, Fibră optică etc.) furnizate de către ofertant;
- Interconectarea noilor echipamente cu sistemul de comunicații existent, daca este cazul;
- Inițializarea echipamentelor;
- Teste de interconectare pentru fiecare legătură;
- Refacerea conexiunilor eronate, în cazul în care unele teste de interconectare dau erori de comunicație;
- Marcarea cu etichete a fiecărui echipament și conexiune conform cu procedura de etichetare agreata.

3. Configurarea echipamentelor

Toate echipamentele vor fi configurate de către Furnizor conform soluției tehnice agreate cu Beneficiarul în urma workshop-urilor comune.
Planul de adresare IP pentru testarea echipamentelor instalate va fi pus la dispoziția Furnizorului de către Beneficiar, iar acesta din urmă va configura adresele IP de producție pe echipamentele respective, după efectuarea tuturor testelor de verificare.
Responsabilitatea Furnizorului se va răsfrânge doar asupra echipamentelor livrate de acesta și va presupune activități legate de integrarea acestor echipamente în sistemul informatic existent.
Toate echipamentele vor fi instalate și configurate în conformitate cu cerințele Beneficiarului, ce vor fi aduse la cunoștința Furnizorului și agreate de acesta în urma discuțiilor tehnice preliminare.
Instalarea și configurarea sistemului informatic de virtualizare se va face conform cerințelor Beneficiarului stabilite în perioada de acceptanță.

5.9.2. Serviciile de livrare, instalare și dezvoltare software

Pentru asigurarea dezvoltării sistemului vor trebui asigurate cel puțin următoarele categorii mari de activități, astfel încât să fie îndeplinite toate cerințele funcționale prevăzute în capitolul 5.1 și funcționarea integrată a tuturor componentelor software prevăzute în capitolul 5.8:

1. Servicii de analiză in vedere proiectarii sistemului informational nou;
2. Servicii de proiectare a sistemului:
    - Proiectarea modelului sistemului de date;
    - Definirea serviciilor aferente noului flux funcțional de sistem;
    - Definirea principalelor funcționalități de sistem folosind modele entitate - asociere sau UML2.0;
    - Proiectarea componentelor și arhitectura de sistem;
    - Arhitectura de deploy în centrul de date și obținerea acordului final din partea administratorului centrului de date.
3. Servicii de instalare și configurare infrastructură de suport;
4. Dezvoltarea softului de aplicație:
    - Instalarea și configurarea produselor COTS;
    - Dezvoltarea componentelor software;
    - Configurarea sistemului software;
    - Integrarea componentelor software;
    - Testarea soluției software.
5. Se vor avea în vedere minim servicii pentru interconectarea sistemului cu:
    - RoeID ca furnizor de identitate acreditat la nivelul UE;
    - portalul Single Digital Gateway – proiectul PDURO;
    - nodul eIDAS al României.
6. Servicii de tip SOC (security operation center)
    - **Prevenirea atacurilor cibernetice și protejarea infrastructurii APIA**. Acest sistem poate reprezenta o țintă atractivă pentru atacatorii cibernetici, deoarece un atac reușit poate cauza pagube semnificative și poate perturba funcționarea întregului sistem critic. Atacurile cibernetice pot varia de la atacuri de tipul malware și phishing până la atacuri sofisticate, cum ar fi atacurile distribuite de tipul DdoS. Prin implementarea unor politici și proceduri de securitate robuste, inclusiv **monitorizarea continuă** și actualizarea sistemelor de securitate, se poate preveni și detecta rapid orice atac cibernetic, asigurând astfel integritatea și disponibilitatea serviciilor APIA.

- **Asigurarea continuității operaționale.** Sistemul este esențial pentru funcționarea fără întreruperi a activităților cheie ale APIA. Asigurarea securității operaționale implică adoptarea unor măsuri precum backup-uri regulate ale datelor, redundanță în infrastructură și planuri de continuitate a afacerii, astfel încât să se poată menține operațiunile critice în caz de incident sau atac.

Asigurarea securității operaționale a unui astfel sistem informatic critic este, deci, de o importanță crucială pentru protejarea informațiilor confidențiale, prevenirea atacurilor cibernetice și asigurarea continuității operaționale. Investirea în măsuri solide de securitate și adoptarea unor politici și proceduri bine definite sunt necesare pentru a răspunde provocărilor tot mai complexe ale securității cibernetice și pentru a proteja sistemele care stau la baza funcționării societății și economiei noastre moderne.

Pentru asigurarea securității operaționale a proiectului, obiectivul serviciilor de monitorizare operațională și de securitate este acela de monitoriza în mod continuu (24/7), pe toata durata perioadei de garanție, evenimentele și incidentele operaționale și de securitate din cadrul infrastructurii informatice a APIA, asigurând o capacitate adecvata de a răspunde la incidentele de performanță și de securitate cibernetică.

Prin monitorizarea continuă a performanței și securității informației, Autoritatea contractantă dorește asigurarea creșterii capacității de reacție la incidentele cibernetice și diminuarea impactului acestora asupra resurselor și serviciilor infrastructurii informatice pe care organizația o operează.
Monitorizarea operațională și de securitate este o activitate importantă în cadrul procesului de Management al Securității Informației prin care trebuie asigurat un grad ridicat de reziliență a infrastructurii informatice.
Astfel, se solicită furnizarea unui serviciu de monitorizare, detecție și răspuns pentru alerte cibernetice cu supervizare pro-activă a evenimentelor de securitate din cadrul Sistemului de Securitate.
Se solicita servicii de monitorizare pentru securitate cibernetică de tip SOC prin care pot fi identificate, analizate și remediate incidentele de securitate informatică.
Autoritatea contractantă are în vedere ca serviciile în scopul achiziției să fie structurate pe trei niveluri de acțiune, fiind reprezentate de o echipă tehnică de specialitate a Prestatorului ce va colabora cu echipa de administrare și de securitate a autorității contractante.
Echipa de răspuns la incidente a autorității contractante este punctul de escaladare pentru implementarea măsurilor de remediere.
Prestatorul va pune la dispoziție o echipă de analiști de securitate ce vor desfășura activitățile descrise mai jos, cu respectarea reglementărilor și a procedurilor Autorității contractante.
Prestatorul trebuie să descrie în propunerea tehnică detalii despre fluxurile de lucru și procesele ciclului de viață ale evenimentelor/incidentelor, inclusiv modul în care un eveniment este descris de un analist SOC, cum este evaluat și triat, ce mecanisme sunt folosite pentru a capta informații relevante pentru a îmbogăți evenimentul, modul în care echipa Autorității contractante va fi alertată cu privire la eveniment și modul în care informațiile capturate vor fi partajate cu echipa Autorității contractante.
Prestatorul trebuie să urmeze o metodologie de management al schimbării care trebuie agreată de Autoritatea contractantă, pentru orice modificare a modelului de operare al SOC-ului sau a sistemelor și serviciilor care susțin modelul de operare. Acestea includ modificări ale soluției SIEM, integrări cu surse de log-uri, dispozitive de rețea, protocoale

de comunicații, cazuri de utilizare, manuale, registre de lucru, notebook-uri sau orice altă modificare care ar putea afecta serviciul.

Prestatorul trebuie să asigure, în timpul procesului de inițializare a serviciilor, managementul proiectului, îndrumări, documentație detaliată și să colaboreze cu personalul Autorității contractante sau cu furnizorii săi pentru a configura procesele necesare care să permită prestarea serviciilor solicitate de Autoritatea contractanta, urmând cel puțin următoarele:

- Ingerarea evenimentelor sau furnizarea accesului pentru sistemele de monitorizare a securității în scopul proiectului
- Configurarea soluțiilor și proceselor de escaladare evenimente/incidente
- Stabilirea proceselor de raportare, conținutul, formatul, frecvența și listele de distribuție
- Prestatorul trebuie să colaboreze cu autoritatea contractantă pentru a prelua inventarul de active și baza de date a configurațiilor, proprietățile sistemelor și nivelul critic al activităților APIA.

Cerințe Specifice

- **Managementul evenimentelor de securitate**

Se va asigura monitorizarea evenimentelor de securitate în cadrul sistemului informatic prin analiza alertelor generate de către soluția SIEM, livrată pentru infrastructura sistemului, pentru colectarea logurilor, agregarea și corelarea evenimentelor de securitate.

În scopul furnizării serviciilor, prestatorul va asigura cel puțin următoarele activități:

- monitorizare continuă a securității infrastructurii autorității contractante,
- triajul evenimentelor de securitate, prin examinarea și analiza evenimentelor potențiale detectate pentru a determina dacă este nevoie de investigații și/sau răspuns suplimentare de către echipele de asistență/răspuns,
- analiștii de securitate ai Prestatorului trebuie să se folosească de cazuri de utilizare, notebook-uri și playbook-uri din cardul SIEM-ul / sistemelor de monitorizare operațională pentru a efectua triajul alertelor și reducerea fals-pozitivelor pentru detectările și alertele generate automat. Triajul ar trebui făcut în corelație cu inventarul activelor autorității pentru a încorpora evaluările de risc ale activităților, ale activelor și vulnerabilitățile reale, împreună cu informații despre amenințările globale.
- gestionarea și prioritizarea evenimentelor, gestionarea răspunsurilor la incidente și escaladarea lor către echipa beneficiarului,
- atribuirea de prioritate recomandată de răspuns la incident fiecărui incident de securitate potențial identificat,
- corelează și documentează evenimente notabile legate într-un singur tichet de incident de securitate, atunci când este posibil,
- crearea tichetelor de incident și documentarea oricărui potențial eveniment de securitate identificate pe baza analizei datelor investigate și tabloului de bord,
- notificarea punctelor de contact desemnate de autoritatea contractantă cu privire la orice incidente de securitate potențiale identificate,
- pentru investigațiile despre evenimente potențiale care necesită investigații suplimentare, analiștii de securitate ai Prestatorului vor crea un tichet și vor include informații suplimentare pentru a ajuta analiști de incident.

Clasificarea evenimentelor de securitate:

- **Evenimentul de securitate potențial** (adevărat pozitiv) este un eveniment care poate încălca politicile, standardele clientului sau amenință confidențialitatea, integritatea sau disponibilitatea sistemelor informatice ale utilizatorilor finali. Pentru a deveni un incident de securitate calificat, este necesară o investigație suplimentară a răspunsului incidentului de securitate din partea echipei SOC.
- **Incident de securitate calificat** este un incident potențial de Securitate, un incident cu impact confirmat asupra confidențialității, integrității sau disponibilității sistemelor informatice ale utilizatorilor finali. Acest lucru necesită o reacție / un răspuns și un plan de remediere din partea echipei SOC.

Evenimentele de securitate semnalate de către Soluția SIEM și celelalte soluții de Securitate vor fi investigate de către echipa SOC a Prestatorului.
In cazul în care se detectează un incident de securitate se va lansa procedura de răspuns la incidente a Autorității contractante.

- **Managementul incidentelor de securitate**

Activitățile în cadrul managementului incidentelor de securitate vor fi documentate și urmărite cu suportul funcționalităților din cadrul soluției SIEM și cuprind:

- analiza operațională zilnică a evenimentelor de securitate din mai multe surse, inclusiv, dar fără a se limita la, evenimente de la instrumente de monitorizare a evenimentelor de informații de securitate (SIEM), rețea și sisteme de detectare a intruziunilor (IPS/IDS), jurnale firewall, jurnale de sistem (Unix și Windows), aplicații și baze de date,
- corelarea, validarea evenimentelor de securitate și identificarea incidentelor de securitate,
- gestionarea, prioritizarea evenimentelor / incidentelor,
- analiza și răspunsul în cazul incidentelor de securitate a informației,
- validarea atacurilor, evaluarea impactului, recomandări de contramăsuri și colaborarea cu echipa beneficiarului în implementarea soluțiilor de remediere,
- suport pentru izolare, eradicare și recuperare în cazul incidentelor de securitate a informației,
- realizarea raportului de incident de securitate după închiderea acestuia.

Clasificarea incidentelor:

Incidentele vor fi clasificate în funcție de potențialul expunerii datelor sau nivelul critic al resurselor folosind o denumire **High - Medium - Low - Info**. Evaluarea inițială a severității poate fi ajustată în timpul executării planului.

- **Incident cu prioritate ridicată (High)**: incident care afectează infrastructura sau aplicația critică, care determină o întrerupere imediată și semnificativă a activității.
- **Incident cu prioritate medie (Mediu):** incident în aplicația critică ce are potențialul de a provoca perturbări ale activității. Împiedică, de asemenea, mulți utilizatori să utilizeze aplicația.
- **Incident cu prioritate scăzută (Low)**: incident care afectează un singur utilizator, împiedicându-l să îndeplinească anumite sarcini, dar NU afectează alte procese ale aplicației.
- **Incident informațional (Info):** Problemă non-critică în care de obicei poate fi furnizată o soluție de rezolvare, cum ar fi împiedicarea utilizatorului să finalizeze o funcție sau o tranzacție.

Impactul sau impactul potențial asupra siguranței, reputației, funcționării activităților și protecției informațiilor constituie unul dintre cei mai importanți factori de luat în considerare la clasificarea unui incident.

- **Analiza avansată de investigații pentru incidente critice**

Activitățile din cadrul analizelor avansate vor presupune efectuarea de investigații tehnice avansate pentru incidentele critice, concentrându-se pe analize de specialitate și pe propuneri de remediere rapidă, cu accent pe îmbunătățirea poziției de securitate a autorității contractante. Activitățile vor consta în furnizarea de rapoarte de investigație end-to-end de înaltă calitate și sumare executive care oferă recomandări cu privire la modul de creștere a eficacității mecanismelor de securitate, informații despre ceea ce s-a întâmplat și determinarea modului de operare al vectorului de infecție.

Activitățile de analiză avansată vor presupune:

- Analiza avansată a log-urilor,
- Analiza avansată a traficului de rețea,
- Analiza avansată a datelor volatile din depozitul de memorie al unui computer,
- Analiza criminalistică (forensic) a disk-urilor de date,
- Analiza comportamentală,
- Coordonarea și raportarea investigațiilor de securitate.

- **Managementul vulnerabilităților**

Se vor detecta și evalua periodic (lunar) vulnerabilitățile existente atât la nivelul infrastructurii hardware cât și la nivelul aplicațiilor software instalate în cadrul infrastructurii informatice.

Pentru automatizarea proceselor de management a vulnerabilităților, Prestatorul trebuie să pună la dispoziția beneficiarului o soluție software, furnizată ca serviciu pe toata durata contractului, serviciu care să includă inclusiv feed-uri pentru organizații de tip enterprise, ce va fi utilizată de echipa de experți ai Prestatorului pentru identificarea, evaluarea și raportarea vulnerabilităților de securitate din cadrul infrastructurii informatice:

- soluția de management a vulnerabilităților trebuie să fie o aplicație pentru testarea și identificarea automată de vulnerabilități ce trebuie să ofere cel puțin următoarele:
  - să poată scana/audita diferite dispozitive din rețea, incluzând mașini UNIX și Windows, servere web, aplicații web, servere de baze de date, routere, imprimante, firewall-uri, switch-uri, pentru a detecta vulnerabilități de securitate.
  - să ofere o bază de date cu exploit-uri/vulnerabilități cunoscute și să ofere o metodă de actualizare automată fără intervenție manuală și cu o actualizare frecventă, cel puțin zilnică, a bazei de date cu vulnerabilități.
  - Baza de date cu vulnerabilități trebuie să includă cel puțin, dar fără a se limita la acestea, verificări pentru OS Security and Patch, CISCO, Firewalls, DNS, FTP, SMTP, SNMP, LDAP, SMB, CGI, Web Servers, SQL Databases, Denial of Service, Default Accounts.
  - Baza de date cu vulnerabilități trebuie să includă o suită mai completă de verificări pentru echipamente de rețea (de exemplu, Cisco), inclusiv cele mai recente modele și configurații.
  - să aibă abilitatea de a stoca rezultatele scanărilor și evaluărilor într-o bază de date pentru raportare și istoric:

- Stocare avansată: o platformă de gestionare a vulnerabilităților (VM) mai robustă, care permite stocarea și analiza unui volum mare de date de scanare.
- Funcționalități complexe: Oferă o gamă largă de funcții pentru căutarea, filtrarea și raportarea rezultatelor scanărilor. Rapoarte personalizate, tendințele în timp și generarea de alerte automate.
- Integrare cu alte sisteme: se integrează cu alte sisteme de gestionare a informațiilor și evenimentelor de securitate (SIEM), permițând corelarea datelor de scanare cu alte informații relevante.
- proiectată pentru a gestiona medii complexe, cu un număr mare de dispozitive și scanări frecvente.

o accesul la aplicație trebuie să se realizeze criptat.
o aplicația trebuie să nu necesite instalarea de agenți pe dispozitivele scanate.
o aplicația trebuie să realizeze scanări în mod neautentificat și/sau autentificat cu credențialele pentru testarea vulnerabilităților și a configurațiilor.
o aplicația trebuie să poată:
  - Detecta servicii care rulează pe porturi non-standard.
  - Testa multiple instanțe ale aceluiași serviciu rulând pe porturi diferite.
  - Scana dispozitivele care nu răspund la ping.
o aplicația trebuie să includă un scor al vulnerabilităților conform standardului în industrie CVSS (Common Vulnerability Scoring System).
o Integrare cu alte sisteme: Poate integra scorurile CVSS cu alte sisteme de gestionare a riscurilor, permițând obținerea unei imagini de ansamblu asupra riscurilor la nivel de entitate.
o Rapoarte detaliate: Oferă rapoarte mai detaliate și personalizate, inclusiv rapoarte bazate pe scorurile CVSS.
o aplicația trebuie să urmărească data descoperirii vulnerabilității și ultima dată la care aceasta a fost observată, pentru filtrare și raportare în funcție de timp.
o aplicația trebuie să poată scana servere web pentru vulnerabilități specifice aplicațiilor web, cum ar fi, dar fără a se limita la acestea, SQL injection, cross-site scripting (XSS), HTTP header injection, directory traversal, remote file inclusion, command execution.
o aplicația trebuie să accepte ținte de scanare în diferite formate, incluzând game de adrese IP (range) și clase IP.
o pentru scanări trebuie să se poată configura cel puțin, dar fără a se limita la acestea, următoarele:
  - Lista porturilor TCP și UDP pe care să le scaneze pentru detecția de vulnerabilități.
  - Lista de vulnerabilități pe care să le verifice.
  - Setări pentru scanări cu sau fără autentificare pe diverse servicii, inclusiv brute force.
o aplicația trebuie să asigure fără a se limita la acestea:
  - Scanarea porturilor cu sau fără credențiale.
  - Scanarea vulnerabilităților în rețea pe echipamente de rețea, servere, stații de lucru
  - Auditul patch-urilor.
  - Auditul cu credențiale al configurațiilor pentru Windows, Unix, echipamente active de rețea.
  - Scanarea cu credențiale a unei largi palete de aplicații software.
  - Modulul de scanare a vulnerabilităților aplicațiilor web trebuie să navigheze automat prin toate paginile site-ului web auditat pentru detecția vulnerabilităților, inclusiv cu evitarea buclelor circulare de link-uri.

        - Scanarea predefinită sau configurabilă a vulnerabilităților bazelor de date.
    - aplicația trebuie să asigure vizibilitatea rapidă a vulnerabilităților prin etichetarea acestora pe grade de risc.
    - pe sistemele Windows, prin scanare autentificată, aplicația trebuie să preia și să raporteze informații despre utilizatori, configurații de rețea, setări de registre, software instalat, dispozitive instalate, vulnerabilități.
    - aplicația trebuie să asigure o bază de date de tip KnowledgeBase cu informații pentru remedierea vulnerabilităților identificate.
    - aplicația trebuie să detecteze și să clasifice riscurile și vulnerabilitățile, oferind informații despre natura riscului și recomandări pentru eliminarea acestuia.
    - aplicația trebuie să exporte rapoarte în formatele: HTML, CSV, XML.
    - prin metoda de licențiere aplicația nu trebuie sa limiteze numărul de adrese IP care pot și scanate.
    - Prestatorul trebuie să facă dovada că deține licență (drept de utilizare) pentru utilizarea acestei aplicații.

Experții Prestatorului vor analiza planul de remediere generat de aplicația de scanare și validează soluția propusă sau aduc recomandări suplimentare, bazat pe experiența / certificările deținute pe partea de evaluare vulnerabilități.
La realizarea recomandărilor se va ține cont de specificitatea fiecărui sistem țintă și de rolul acestuia în cadrul organizației.
Prestatorul va asigura suport de specialitate pentru implementarea contramăsurilor recomandate pentru adresarea vulnerabilităților identificate.
După identificarea vulnerabilităților, Prestatorul trebuie să evalueze riscul pe care acestea îl reprezintă în diferite contexte, astfel încât să poată fi luate decizii cu privire la modalitățile cele mai bune de tratare a acestora.
Modalitatea de furnizare a acestor activități se va face conform unei planificări ce va fi stabilită și agreată de comun acord, între părțile implicate, și prin care se va stabili planul de furnizare și acceptanță a serviciilor.
Planul va cuprinde, fără a se limita, următoarele:

- Stabilire strategie și obiective,
- Planificare activități ,
- Livrabilele (inclusiv rapoartele de activitate),
- Resursele alocate, atât din partea Prestatorului cat și a beneficiarului.

Obligațiile Prestatorului:

- Să prezinte lunar un raport cumulativ al activităților SOC, care va cuprinde cel puțin următoarele:
    - Scor de securitate care să reflecte nivelul de securitate în cadrul infrastructurii, bazat pe vulnerabilitățile descoperite în cadrul procesului de management al vulnerabilităților
    - Evoluția în timp a scorului de securitate
    - Vulnerabilitățile existente în cadrul infrastructurii, vulnerabilitățile eliminate, precum și cele noi apărute în perioada de raportare
    - Metricile de securitate urmărite, precum și evoluția acestora:
    - Evenimentele de securitate analizate, inclusiv cele considerate fals-pozitiv;
    - incidentele de securitate care au avut loc în perioada de raportare
    - Măsurile de securitate recomandate Beneficiarului în perioada de raportare pentru eliminarea vulnerabilităților și reducerea nivelului de risc.

- Pentru cerințele descrise în acest capitol, Prestatorul trebuie să respecte indicatorii Acordului privind nivelul serviciilor (SLA) descriși mai jos:

Tip de serviciu	Mean Time to Acknowledge (MTTA)		Mean Time to Respond (MTTR)	
	Mediu	**High**	**Mediu**	**High**
Managementul incidentelor de securitate	4 ore	2 ore	8 ore	4 ore

- **Timpul mediu de confirmare (MTTA)** este timpul mediu pe parcursul unei luni, pentru un nou Incident de Securitate calificat, să primească un responsabil în echipa SOC, pentru procesare ulterioară (anchetă).
- **Timpul mediu pentru a răspunde (MTTR)** este timpul mediu pe parcursul unei luni, pentru un nou Incident de Securitate calificat, pentru a primi un răspuns inițial din partea echipei SOC.

Toate activitățile prevăzute vor fi documentate conform metodologiilor propuse de Prestator și bunelor practici în domeniu.

Toate documentațiile vor fi supuse aprobării Beneficiarului.

Lista minimă de documentații de livrat pentru dezvoltare software:

1. ***Raport de analiză;***
2. ***Raport de proiectare;***
3. ***Raport de instalare și configurare a produselor software COTS;***
4. ***Plan(uri) de testare;***
5. ***Raport de livrare echipamente TIC si alte dispozitive eferente;***
6. ***Raport de instalare si configurare a echipamentor TIC si altor dispozitive eferente, livrate;***
7. ***Raport/rapoarte de testare;***
8. ***Documentația de administrare a sistemului;***
9. ***Documentația de utilizare a sistemului;***
10. ***Codul sursa documentat, fișiere de configurare;***
11. ***Metodologia de contorizare a numărului de utilizatori;***
12. ***Plan de instruire;***
13. ***Raport de instruire;***
14. ***Plan de punere în producție;***
15. ***Raport de punere în producție;***
16. ***Documentația as-built a Sistemului Informatic Integrat;***
17. ***Procedura de suport tehnic.***

5.9.3. Testarea și asigurarea calității sistemului

Este necesar ca furnizorul să planifice în detaliu, să pregătească și să efectueze o serie de teste care să confirme că sunt asigurate cerințele funcționale și nonfuncționale ale sistemului, compatibilitatea sistemului cu specificațiile de interfațare ale acestuia cu sistemele externe.

5.9.3.1 Testarea

Pentru nodul central, Beneficiarul se va asigura că furnizorul a efectuat cu succes următoarele activități cu rezultatele lor respectiv:

- toate componentele software de bază necesare au fost livrate și instalate corespunzător;
- toate elementele din nodul central sunt pe deplin funcționale;
- aplicația a fost livrată și instalată;
- sistemul funcționează fără incidente majore pentru o durată de 4 săptămâni;
- sesiunile de instruire au fost livrate;
- toate documentele necesare, manuale, CD-uri de instalare și licențele solicitate în acest proiect au fost livrate;
- s-a realizat cu succes testarea proceselor interne: jurnalizare, arhivare, auditare, raportare ștergeri, managementul notificărilor;
- s-a realizat generarea de raportări statistice care au fost identificate în procesul de implementare a sistemului.

Testele non-funcționale trebuie să acopere cerințele de disponibilitate, scalabilitate, fiabilitate, robustețe, salvare și restaurare, recuperare în caz de dezastru, estimări capacitate și planificare, performanța, management configurații, extensibilitate/flexibilitate, siguranță în funcționare, securitate, management și monitorizare sistem, management căderi în sistem, contingența, operare, conectivitate și calitate servicii.

Testare de securitate

Aplicația va fi supusă unor verificări riguroase de securitate (auditare de securitate și test de penetrare) pentru a se identifica și elimina orice vulnerabilități înainte de a se utiliza în producție, precum și regulat, la intervale definite de timp. Testele vor respecta cel puțin metodologiile OSSTM (Open Source Security Testing Methodology) sau OWASP (Open Web Applications Security Project). Raportul final de testare de securitate va cuprinde vulnerabilitățile existente în cadrul sistemului și componentelor acestuia, și va fi structurat astfel:

- Sumar Executiv;
- Obiectivele și scopul evaluării;
- Prezentare succintă a metodologiei utilizate;
- Descrierea contextului în care s-a desfășurat evaluarea;
- Lista testelor de securitate efectuate.

Prezentarea individuală a vulnerabilităților descoperite după cum urmează:

- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnică;
- Analiza severității și probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere;
- Alte detalii și recomandări.

Scanarea de vulnerabilități informatice se va realiza prin utilizarea de aplicații dedicate și actualizate la momentul realizării scanărilor. În acest sens se vor utiliza aplicații care să conțină baze de date de vulnerabilități la nivel de rețea, sisteme de operare, aplicații/servicii, care, pe de-o parte, trebuie să permită auditarea activităților realizate astfel încât să poată fi demonstrată efectuarea acestor activități și, pe de altă parte, să conțină baze de date actualizate cu exploit-uri (coduri care demonstrează că o vulnerabilitate poate fi exploatată însă fără ca sistemul să fie propriu-zis compromis).

Planurile de testare trebuie să includă cel puțin următoarele elemente:

- descrierea componentei de sistem testat,
- obiectivele de testare,
- descrierea mediului de testare,
- rezultatele așteptate ale testului,
- test de abordare,
- datele de test,
- descrierea procedurilor de test,
- cazuri de testare,
- instrumente folosite de testare,
- persoanele responsabile,
- cerințe de intrare/ieșire.

Instrumente de testare

Furnizorul trebuie să precizeze toate instrumentele de testare (aplicații, scripturi, etc.), destinate a fi utilizate în timpul procedurilor de testare. Furnizorul trebuie să pună la dispoziție instrumentele de testare. Toate rezultatele testelor trebuie înregistrate și furnizate Beneficiarului după fiecare test.
Toate componentele necesare testării vor fi descrise de furnizor și vor fi disponibile pentru toată perioada întregului contract (inclusiv pentru actualizări/testare pentru modificări). Același mediu de testare se va utiliza pentru a testa toate modificările cerute și derivate din modificări legislative.
Mediul de testare nu trebuie să fie reutilizat sau integrat în alt mod în mediul de producție.

Dezvoltarea și punerea în aplicare de teste

Toate testele se vor efectua/supraveghea de către Beneficiar. Pentru cazurile de testare care necesită resurse externe sau acces la sisteme, Beneficiarul va asigura accesul la aceste resurse. Furnizorul va oferi toate instrumentele de testare, în cazul utilizării instrumentelor automate pentru testele de acceptanță operațională.

Coordonarea testelor

Testele vor fi coordonate de către Beneficiar, care va revizui și aproba planul și specificațiile de testare înainte de execuția efectivă a testelor, va controla că mediul de testare e conform cu cerințele, va monitoriza efectuarea testelor și se va asigura de aplicarea procedurilor de management al testării.

5.9.3.2 Asigurarea Calității

- Furnizorul trebuie să prezinte un plan pentru Asigurarea Calității acceptabil pentru Beneficiar, ca parte a planului de proiect;
- Furnizorul trebuie să aloce timp suficient, în cadrul planului de proiect, pentru verificare și validare în termeni de calitate, pentru serviciile prestate în cadrul contractului și pentru livrabilele/documentele/rapoartele rezultate;
- Furnizorul va elabora procedurile standard de operare pentru toate aplicațiile livrate, cu instrucțiuni detaliate pentru sprijinirea angajaților în diferite procese de lucru;
- Furnizorul va pune la dispoziție manuale, documentații, proceduri complete privind concepția, implementarea și administrarea în integralitate a sistemului informatic;

- Furnizorul va oferi, pe durata proiectului, trimestrial, un raport intermediar de audit intern privind modul în care au avut loc activitățile în cursul perioadei de raportare, calitatea rezultatelor obținute în cursul perioadei de raportare și propunerile de acțiuni corective și preventive menite să îmbunătățească calitatea rezultatelor. Rapoartele trimestriale vor prezenta valorile măsurate pentru o serie de indicatori de performanță.

6. INSTRUIRE UTILIZATORI - INCLUSIV CONȘTIENTIZARE SECURITATE INFORMATICĂ

Pentru utilizarea în bune condiții a sistemului informatic, este foarte important ca personalul care va opera sistemul să fie instruit corespunzător. Furnizorul trebuie să organizeze sesiuni de instruire și să realizeze activități de instruire a personalului care va utiliza noul sistem informatic în vederea familiarizării corespunzătoare cu elementele de noutate și cu modul de operare ale acestuia.

Sistemul va fi operat, administrat și gestionat de către următoarele categorii de utilizatori, având rolurile menționate mai jos, pentru care va fi asigurat formare **diferențiată**:

Administratori sistem integrat
Cursuri specifice soluției integrate oferite:

- cursul va avea o durată de minim 5 zile (8 ore /zi), cu prezență fizică;
- cursul va fi dimensionat pentru 10 utilizatori;
- cursul va fi susținut în limba română;
- curriculum va acoperi toate aspectele necesare utilizării în bune condiții a sistemului;
- curriculum va acoperi toate aspectele relevante privind securitatea cibernetica
- curriculum va acoperi toate aspectele de securitate cibernetică a sistemului informatic;
- participanții la curs vor primi de la furnizor certificate de instruire individuale.

Training utilizatori

Utilizatori avansați
Utilizatori cu rol de configurare avansată a funcționalităților software. Realizează, fără a se limita la: asigurare suport nivel 1 gestionarea utilizatorilor sistemului, gestionarea bunei funcționari a fluxurilor, emiterea de rapoarte, etc.

- cursul va avea o durată de minim 5 zile (8 ore /zi), cu prezență fizică;
- cursul va fi dimensionat pentru 10 de utilizatori;
- curriculum va acoperi toate aspectele relevante privind securitatea cibernetica
- cursul va fi susținut în limba română;
- curriculum va acoperi toate aspectele necesare utilizării în bune condiții a sistemului;
- participanții la curs vor primi de la furnizor certificate de instruire individuale.

Personalul operațional
Această categorie de utilizatori este responsabilă de operaționalizarea sistemului. Va fi format personal selectat, care vor acționa ulterior ca formatori la nivelul structurilor teritoriale din care provin.

- cursul va avea o durată de minim 4 zile (8 ore /zi), cu prezență fizică, organizat în București;
- cursul va fi dimensionat pentru 200 utilizatori (10 sesiuni a 20 de utilizatori),
- cursul va fi susținut în limba română;
- curriculum va acoperi toate aspectele necesare utilizării în bune condiții a sistemului;

- curriculum va acoperi toate aspectele relevante privind securitatea cibernetica

- participanții la curs vor primi diplome de participare care sa ateste statutul de formator la nivelul APIA pentru utilizarea aplicației.

Prin instruire se va asigura transferul de competențe necesare fiecăreia dintre cele 3 categorii pentru a-și îndeplini atribuțiile de serviciu prin utilizarea sistemului informatic.

Prin instruire se va asigura realizarea cel puțin a următoarelor obiective:
- cunoașterea sistemului integrat în ansamblul său;
- învățarea modului de operare a funcționalităților sistemului propus;
- învățarea modului de rezolvare a problemelor curente de folosire a componentelor sistemului;
- înțelegerea implicațiilor sistemului propus și a avantajelor acestuia;
- cursuri de conștientizare a securității;
- cursuri de securitate pentru administratori.

Pentru activitatea de instruire, furnizorul va trebui să asigure materiale de curs în format .pdf dar și materiale împachetate minim SCORM 2004 (dacă este cazul) - **Sharable Content Object Reference Model (SCORM**) este o colecție de standarde și specificații pentru instruirea asistată de calculator (e-learning).

Pentru cursurile în format fizic, furnizorul sistemului informatic va asigura toate resursele necesare desfășurării serviciilor de instruire (sala de training cu dotările necesare, servicii de catering), va elabora și susține cursurile și va tipări, dacă este cazul, materiale de curs pentru toți participanții.

La sfârșitul cursurilor, toți participanții vor completa formulare pentru evaluarea serviciilor de training.

7. GARANȚIA

Pentru toate echipamentele și pentru produsele software de bază se va acorda suport tehnic până la finalizarea proiectului, conform contractului încheiat de instituția beneficiară cu furnizorul soluției informatice.

Prin garanție în acest context se înțelege:

a. **Asigurarea funcționării echipamentelor furnizate**, în următoarele condiții:
- Contractantul va realiza corectarea gratuită, pentru echipamentele livrate, a oricăror erori, defecte și neconformități constatate, cu excepția cazurilor în care defectele se datorează în mod exclusiv utilizării inadecvate / necorespunzătoare de către personalul Achizitorului;
- În cazul în care echipamentele și accesoriile necesită înlocuire ca urmare a defectării sau funcționării neconforme cu cerințele specificate în prezentul caiet de sarcini, aceasta se va realiza în timpul programului de lucru al Achizitorului, transportul de la și înapoi la Achizitor intrând în sarcina Contractantului.
- Toate costurile legate de înlocuirea sau repararea bunurilor, precum și de remedierea defecțiunilor cad în sarcina Contractantului (diagnosticare, transport, costuri de asigurare, taxe în vamă, manoperă pentru reparare etc.) și vor fi incluse în prețul echipamentelor.

b. **Asigurarea suportului tehnic pentru produsele software furnizate** (actualizări și patch-uri de securitate). Costurile cu suportul tehnic vor fi incluse în prețul componentelor software ofertate.

c. **Asigurarea funcționalităților realizate în baza serviciilor prestate** (analiză, proiectare, implementare), în următoarele condiții:
- Contractantul va asigura utilizatorilor finali un Punct Unic de Contact pentru toate solicitările de intervenții pentru semnalările unor disfuncționalități ale soluției furnizate.
- Remedierea defecțiunilor se va realiza la sediul beneficiarului sau prin intervenție de la distanță (remote maintenance).
- Fiecare intervenție va fi documentată cu ajutorul unei fișe de intervenție care va conține minimum următoarele informații: defectul semnalat, data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției, durata de intervenție și confirmarea remedierii defectului prin semnăturile furnizorului și beneficiarului.
- Intervențiile se vor realiza în următoarele cazuri:
  - În condițiile apariției unei defecțiuni a soluției software instalate și configurate - se vor asigura verificări tehnico-metodologice, pentru a determina dacă problemele apărute sunt de natură hardware sau software.
  - În condițiile apariției unei erori în funcționarea soluției software instalate și configurate - se vor asigura verificări pentru a determina natura problemelor apărute și se va decide, de comun acord, care este cel mai potrivit mod de intervenție pentru soluționarea defecțiunii. Modalitățile de intervenție sunt: help-desk online, asistenta telefonică, realizarea, in caz de necesitate, a actualizărilor de software, remedierea in locația beneficiarului.
  - Actualizări de software - pot face referire, dar nu limitativ, la: compilarea sau descărcarea unor patch-uri care conțin corecții ale unor erori sau îmbunătățirea software-ului cu scopul de a crește ușurința în exploatare sau performanțele acestuia. Actualizările vor fi însoțite, daca este cazul, de actualizări ale manualelor/ghidurilor de utilizare destinate utilizatorilor.

Toate soluțiile software vor trebui să fie de tip comercial (COTS), drept de utilizare perpetuă sau sub formă de subscripție valabilă pentru perioada de implementare a contractului și cel puțin pentru întreaga perioadă de garanție în functie de soluția propusă.

Pentru întregul sistem integrat se va acorda o garanție de 5 ani. Prin garanție, în acest context, se înțelege asigurarea funcționalităților existente la data acceptanței finale a sistemului informatic.

Pentru componentele licențiate ale software-ului de aplicații se va asigura suport tehnic pe perioada garanției de 5 ani, începând cu data acceptanței finale pentru sistemul informatic.

Pe întreaga perioadă de garanție, furnizorul soluției informatice va asigura funcționarea conform specificațiilor tehnice și funcționale agreate în documentele de analiză de business, de arhitectură, de specificații funcționale elaborate pentru dezvoltarea și implementarea sistemului, va presta servicii de suport pentru toate sistemele software furnizate, iar această activitate va fi monitorizată de către managerul de proiect.

Activitățile de mentenanță și suport din perioada de garanție vor realiza prevenirea și remedierea defecțiunilor și anomaliilor apărute la produsele software livrate în cadrul soluției informatice.

Serviciul de suport tehnic va avea scopul de a oferi utilizatorilor finali un Punct Unic de Contact pentru toate solicitările de intervenții asupra componentelor software, pentru suport operativ și pentru semnalările unor disfuncționalități ale soluției furnizate.

Remedierea defecțiunilor pe perioada garanției se va realiza la sediul beneficiarului proiectului sau prin intervenție de la distanță (*remote maintenance*). Iar, în cazul unor defecte care nu pot fi rezolvate prin modalitățile menționate mai sus, echipamentele se vor transporta, de către beneficiar, la sediul furnizorului. Pe durata remedierii defectelor, furnizorul va asigura, la schimb, echipamente cel puțin echivalente (ca și parametrii tehnici/funcționali) cu cele înlocuite.

Fiecare intervenție în perioada de garanție va fi documentată cu ajutorul unei fișe de intervenție care vor conține, minimum, următoarele informații: defectul semnalat, data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției, durata de intervenție și confirmarea remedierii defectului prin semnăturile furnizorului și beneficiarului.

În perioada de garanție pentru componentele sistemului propus se vor presta următoarele servicii de garanție:

- Consiliere și suport telefonic 24 de ore pe zi, 7 zile pe săptămână prin serviciu Help-desk, atât pentru produsele software, cât și pentru cele hardware.
- Remediere software de la distanță cu acordul beneficiarului.
- Actualizări software la locația de instalare a beneficiarului sau de la distanță.
- Reconfigurări software la nivelul inițial solicitat în cazul în care erorile apărute nu sunt datorate beneficiarului.
- Mentenanța preventivă periodică.
- Consiliere și suport tehnic pentru posibilități de extindere a soluției existente.

Pe timpul derulării garanției, se vor presta următoarele intervenții:

- În condițiile apariției unei defecțiuni ale produselor software instalate și configurate, se vor asigura verificări tehnico-metodologice pentru a determina dacă problemele apărute sunt de natură hardware sau software.
- În condițiile apariției unei erori în funcționarea produselor software instalate și configurate, se vor asigura verificări pentru a determina natura problemelor apărute și se va decide, de comun acord, care este cel mai potrivit mod de intervenție pentru soluționarea defecțiunii. Modalitățile de intervenție sunt: help-desk online, asistență telefonică, realizarea, în caz de necesitate, a actualizărilor de software, remedierea în locația beneficiarului.
- Actualizările de software pot face referire, dar nu limitativ, la: compilarea sau descărcarea unor patch-uri care conțin corecții ale unor erori sau îmbunătățirea software-ului cu scopul de a crește ușurința în exploatare sau performanțele acestuia. Actualizările vor fi însoțite, dacă este cazul, de actualizări ale manualelor/ghidurilor de utilizare destinate utilizatorilor.

Controlul intervențiilor

Pentru înregistrarea tuturor tipurilor de intervenții (preventive, corective, actualizări etc) și pentru asigurarea bunei funcționări a produselor ofertate, se va propune, dacă este cazul, un model de registru pentru controlul intervențiilor, care va fi validat de comun acord în urma workshop-urilor comune avute cu beneficiarul. Beneficiarul va actualiza acest registru, pe baza documentelor elaborate de către furnizor, cu toate informațiile care descriu intervențiile respective.

În cadrul perioadei de garanție se vor asigura:
- rezolvarea bug-urilor care nu au fost identificate în timpul implementării și testării 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;
- actualizarea manualelor de utilizare și altor documente în urma efectuării corecțiilor.

Toate incidentele vor fi gestionate prin intermediul aplicației software de gestionare a tichetelor.

Nivele de Prioritate

Nivel Prioritate	Descriere
Urgent	**Impact Major** asupra funcționării sistemului Problema împiedică desfășurarea activității instituției, procesul de activitate este serios afectat şi nu mai poate continua, pierderea funcționalităților devenind critică.
Critic	**Impact Semnificativ** asupra funcționării sistemului Problema împiedică desfășurarea în condiții normale a activității utilizatorilor. Nicio soluție alternativă nu este disponibilă iar activitatea utilizatorilor poate totuși continua, însă într-un mod restrictiv.
Major	**Impact Mediu** asupra funcționării sistemului Problema afectează minor funcționalitățile sistemului. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.
Minor	**Impact Minim** asupra funcționării sistemului Problema nu afectează funcționalitățile sistemului. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiţii a activităţii utilizatorilor.

Asistența este de tipul on site (numai la sediul central al beneficiarului).

În cazul incidentelor cu nivel de prioritate ”urgent”, asistența va fi asigurată 24x7, fiind disponibilă până când problema va fi rezolvată. Pentru aceasta, beneficiarul va furniza o persoană de contact, disponibilă 24x7, care să furnizeze informații, să testeze soluții şi să aplice soluțiile furnizate.

Timpi de răspuns şi rezoluții

Furnizorul va respecta următorii timpi de răspuns, în corelație cu nivelul de prioritate:

Nivel prioritate	Timp de răspuns	Timp soluție provizorie / temporară	Timp de remediere
Urgent	4 ore	1 zi	1 zi
Critic	4 ore	1 zi	1 zi
Major	4 ore	2 zile	3 zile
Minor	4 ore	2 zile	5 zile

Timpii de mai sus sunt calculați din momentul în care Contractantul a fost înștiințat de apariția problemelor.

La sfârșitul fiecărui caz deschis, Contractantul va efectua o analiză a cauzelor care au dus la producerea deranjamentului şi o va fi include în recomandarea finală.

Furnizorul va garanta că SLA-ul mai sus menționat se bazează pe servicii de suport pentru soluția software furnizată în cadrul acestui contract.

Definițiile, descrise mai jos, se vor aplica la Service Level Agreement:

- **Timp de Răspuns:** Timpul scurs de la contactul inițial dintre beneficiar şi HELPDESK şi răspunsul primit de la echipa de suport tehnic a Furnizorului către beneficiar; Această acțiune se va desfășura prin intermediul telefonului;
- **Timp de Remediere:** Durata de timp până la oferirea soluției finale;
- **Remediere Temporară:** O modificare în cadrul procedurilor sau datelor care să evite erorile fără folosirea defectuoasă a produselor;

- **SLA**: Service Level Agreement identifică funcționalitățile și definește procesele care implică livrarea de către Furnizor a diferitelor servicii de suport către Beneficiar;
- **Suport**: Telefonul de suport tehnic, asistență web și e-mail oferite de Furnizor pentru a ajuta Beneficiarul în rezolvarea problemelor apărute;
- **HELPDESK**: Un centru de asistență tehnică ce oferă serviciul de preluare a cererilor prin telefon, web și e-mail operat de către personalul care face parte din echipa Furnizorului care oferă asistență pentru componentele soluției informatice integrate furnizate.

8. ATRIBUȚII ȘI RESPONSABILITĂȚI ALE PĂRȚILOR

Atribuțiile și responsabilitățile Părților vor fi guvernate de prevederile prezentului Caiet de Sarcini și ale contractului care va fi semnat între contractant și operatorul economic desemnat câștigător, în conformitate cu prevederile documentației de atribuire.

Contractantul va avea obligația ca pentru componentele livrate, să obțină din timp în numele Achizitorului, sau să transfere acestuia, prin documente cu caracter juridic, documentele necesare pentru utilizarea acestora conform contractului. Aceasta prevedere se aplică tuturor componentelor/resurselor licențiate și/sau sub licențiate, componentelor software comercializate de Contractant, componentelor software ale unor terți, componentelor pre-existente, uneltelor software necesare livrării, monitorizării și mentenanței, ș.a.m.d.

Contractantul va prezenta documente care dovedesc faptul că software-ul în ansamblul său este supus sau nu unor politici de licențiere (inclusiv se vor avea în vedere utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată).
Documentele justificative trebuie să fie clare, să permită identificarea tipului de licențiere, metodele de calcul (fie virtual, fizic, grad de încărcare, număr de utilizatori etc.), condițiile de utilizare, perioada de timp precum și orice altă informație valabilă la momentul contractării). Orice diferend juridic ulterior cu un terț pe subiectul drepturilor de proprietate intelectuală va cădea în sarcina și responsabilitatea Contractantului.

Contractantul va avea obligația să despăgubească Achizitorul împotriva oricăror: a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.) și b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea caietului de sarcini întocmit de către Achizitor.

Contractantul va avea obligația ca, la transferul documentelor privind licențele, ca drepturi de folosință, să facă transferul către Achizitor a unor documente în original, atât pentru propriile produse cât și pentru toate cele ale unor terți pe care le-a înglobat, adaptat, modificat, îmbunătățit, ș.a.m.d. și simultan să aibă în vedere că orice reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), în legătură cu produsele achiziționate, montate și puse în funcțiune, vor fi în sarcina și responsabilitatea sa.

Toate documentele și informațiile primite de la Ofertant precum și rezultatele tuturor activităților Contractantului din contract (cum ar fi: documente de analiză, arhitecturi de sisteme, adrese, etc., fără a se limita la acestea) reprezintă informații confidențiale, iar Ofertantul câștigător va asigura respectarea confidențialității lor.

Contractantul și personalul său au obligația de a respecta confidențialitatea documentelor și informațiilor menționate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia și după încetarea contractului.

Toate documentele, rapoartele și datele, inclusiv diagrame, scheme tehnice, specificații tehnice, planuri și orice alte materiale realizate de către Contractant în cadrul contractului, trec în proprietatea /proprietatea intelectuală a Achizitorului,

aceasta având dreptul să le utilizeze, modifice, transfere fără acceptul Contractantului sau al unei terțe părți. Contractantul le va furniza Achizitorului, la finalizarea contractului, fără a le utiliza în alte scopuri care nu au legătura cu contractul.

Contractantul nu va publica articole sau informații legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terți și nu va divulga informațiile obținute de la Achizitor, fără acordul scris al acesteia.

Achizitorul va asigura accesul reprezentanților Contractantului în locațiile în care se vor efectua activitățile de livrare, instalare, punere în funcțiune și testare a produselor, precum și condițiile necesare efectuării acestora, astfel cum vor fi stabilite prin Contract.

În raport cu serviciile solicitate și cu cerințele stipulate în prezentul Caiet de Sarcini, responsabilitățile și atribuțiile părților sunt:

8.1. OBLIGAȚIILE AUTORITĂȚII CONTRACTANTE:

a) punerea la dispoziție a tuturor informațiilor de care dispune pentru obținerea rezultatelor așteptate în limita competențelor pe care le deține;
b) desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit contractantului;
c) asigurarea accesului în spațiile în care urmează a se realiza prestarea serviciilor;
d) mobilizarea tuturor resurselor care sunt în sarcina sa, pentru buna derulare a contractului;
e) colaborarea cu Contractantul pentru a identifica în timp util orice eventuale probleme care ar putea apărea pe parcursul derulării contractului;
f) asigurarea acurateței oricăror informații puse la dispoziția Contractantului pe durata derulării contractului;
g) monitorizarea îndeplinirii tuturor cerințelor din Caietul de Sarcini și a oricăror elemente ale Propunerii Tehnice și Financiare pe durata derulării contractului, efectuarea și păstrarea unei arhive cu înregistrări pentru documentarea nivelului de performanță a Contractantului;
h) notificarea Contractantului prin canalele de comunicare puse la dispoziție de acesta privind orice incidente sau disfuncționalități care intervin pe perioada de derulare a contractului;
i) verificarea tuturor documentelor asociate recepției serviciilor care fac obiectul contractului, respectiv care confirmă prestarea serviciilor potrivit condițiilor de calitate stabilite în Caietul de sarcini;

8.2. OBLIGAȚIILE OFERTANTULUI DEVENIT CONTRACTANT

8.2.1. Obligațiile generale ale Ofertantului devenit Contractant

a) asigurarea planificării resurselor în raport cu graficul de prestare și mobilizarea de resurse suficiente și cu expertiză adecvată pentru a asigura gestionarea contractului, astfel cum este solicitat la nivelul Caietului de Sarcini;
b) îndeplinirea obligațiilor contractuale, cu respectarea bunelor practici din domeniu, a prevederilor legale și contractuale relevante, astfel încât să se asigure că obligațiile sunt îndeplinite la parametrii solicitați;
c) asigurarea unui grad de flexibilitate în planificarea modalității de gestionare a contractului, pe toată durata de derulare a contractului; Prin gradul de flexibilitate în prestarea serviciilor, în funcție de necesitățile obiective ale Autorității

Contractante, se înțelege faptul că activitățile descrise în cadrul Caietului de Sarcini reprezintă o exemplificare a fluxului de lucru, dar nu sunt limitate la cele expuse, acestea vor fi adaptate în funcție de nevoile Autorității Contractante și de necesitățile apărute în cadrul analizei realizate împreună cu prestatorul în perioada de adaptare a fluxurilor de lucru, *fără costuri suplimentare* pentru punerea în aplicare a regulamentelor europene și a documentelor de lucru menționate, dar și eventualele modificări ulterioare ale documentelor de lucru/legislației comunitare sau solicitări suplimentare ale Comisiei Europene pe perioada de implementare a proiectului.

d) transmiterea datelor de identificare și de contact ale personalului alocat pentru executarea contractului;
e) colaborarea cu personalul autorității contractante alocat pentru verificarea produselor si serviciilor livrate și realizarea recepțiilor;
f) reducerea, în măsura posibilă, la minim, a situațiilor de întârzieri în efectuarea livrărilor, minimizând astfel impactul negativ asupra activității autorității contractante;
g) asigurarea că orice documente, documentații și/sau instrucțiuni furnizate către personalul autorității contractante sunt exacte și elaborate în conformitate cu bunele practici specifice în domeniu;
h) prezentarea rapoartelor solicitate de personalul autorității contractante, potrivit cerințelor de raportare stabilite prin Contract;
i) completarea unor Declarații de imparțialitate, confidențialitate și privind conflictul de interese de către Personalul desemnat de Contractant, înainte de implicarea în implementarea contractului;
j) asigurarea că pentru toate activitățile cuprinse în propunerea tehnică, dispune de toate resursele necesare pentru îndeplinirea contractului.

Obligațiile principale ale Ofertantului devenit Contractant se completează cu obligațiile prevăzute în Contract.

8.2.2. Obligațiile specifice ale Ofertantului devenit Contractant

a) Toate documentele și informațiile primite de la Autoritatea contractantă precum și rezultatele tuturor activităților din cadrul acestui contract reprezintă informații confidențiale iar Contractantul va asigura respectarea confidențialității lor, urmând să semneze o declarație în acest sens. Această obligație va fi respectată inclusiv de Personalul Contractantului;
b) Contractantul și personalul său au obligația de a respecta confidențialitatea documentelor și informațiilor menționate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia și după încetarea contractului. În acest sens, Contractantul precum și personalul acestuia implicat în activitățile contractului, sunt obligați să semneze Acorduri de Confidențialitate cu Autoritatea contractantă;
c) Contractantul nu va publica articole sau informații legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terți și nu va divulga informațiile obținute de la Autoritatea contractantă, fără acordul scris al acesteia;
d) Contractantul are obligația de a asigura disponibilitatea Personalului, pe toată durata Contractului. Contractantul are obligația de a asigura desfășurarea activităților stipulate în Contract prin acoperirea cu Personal specializat pe toată durata implementării Contractului. Contractantul trebuie să se asigure că, pentru toată perioada Contractului, persoanele alocate fiecărei activități vor îndeplini obligațiile stabilite în sarcina acestora;

e) Contractantul nu va efectua schimbări în cadrul Personalului stabilit, fără aprobarea prealabilă scrisă a Autorității contractante. Autoritatea contractantă va transmite aprobarea/respingerea schimbărilor de Personal în termen de maximum 15 zile, calculat de la primirea documentelor justificative în formă completă și corectă. Aprobarea înlocuirii personalului/de personal produce efecte cu data emiterii acesteia de către Autoritatea contractantă;
f) În situația în care Contractantul sau Autoritatea contractantă solicită înlocuirea Personalului, Contractantul va transmite Autorității contractante, pentru verificare și aprobare, documente justificative privind calificarea educațională și/sau profesională, abilitățile, experiența profesională generală și specifică a Personalului propus. În cazul în care Personalul înlocuit a generat Contractantului un avantaj pe perioada derulării procedurii, la momentul aplicării criteriului de atribuire, Autoritatea contractantă are dreptul de a aproba înlocuirea Personalului numai în situația în care noul Personal nominalizat pentru îndeplinirea Contractului obține cel puțin același punctaj ca Personalul propus la momentul aplicării factorilor de evaluare, chiar și în cazul în care caracteristicile Personalului propus sunt inferioare celor ale Personalului înlocuit. În cazul respingerii Personalului propus, Autoritatea contractantă va notifica, în scris, motivele respingerii și termenul de prezentare a unei noi propuneri;
g) În cazul în care Contractantul nu este în măsură să furnizeze un înlocuitor în condițiile de mai sus, care să nu diminueze avantajul obținut de Contractant ca urmare a aplicării criteriului de atribuire din prezentul Contract, Autoritatea contractantă va decide rezoluțiunea/rezilierea Contractului;
h) Costurile suplimentare generate de înlocuirea Personalului incumbă Contractantului;
i) Executarea contractului nu va genera sub nicio formă cheltuieli comerciale neuzuale. Dacă apar totuși astfel de cheltuieli, contractul poate înceta. Sunt considerate cheltuieli comerciale neuzuale:
   - comisioanele care nu sunt menționate în contract sau care nu rezultă dintr-un contract valabil încheiat referitor la prezentul contract,
   - comisioanele care nu corespund serviciilor prestate și legitime,
   - comisioanele plătite unui destinatar care nu este în mod clar identificat sau
   - comisioanele plătite unei persoane care potrivit tuturor aparențelor este o persoană interpusă.
j) Contractantul va furniza Autorității contractante, la cerere, documente justificative cu privire la condițiile în care se execută contractul. Autoritatea contractantă va efectua orice documentare sau cercetare la fața locului pe care o consideră necesară pentru strângerea de probe în cazul oricărei suspiciuni cu privire la existența unor cheltuieli comerciale neuzuale.
k) Contractantul va avea obligația ca pentru componentele livrate, să obțină din timp în numele Achizitorului, sau să transfere acestuia, prin documente cu caracter juridic, licențele necesare pentru utilizarea acestora conform contractului. Aceasta prevedere se aplică tuturor componentelor/resurselor licențiate și/sau sub licențiate, componentelor software comercializate de Contractant, componentelor software ale unor terți, componentelor pre-existente, uneltelor software necesare livrării, monitorizării și mentenanței ș.a.m.d.
l) Contractantul va prezenta documente care dovedesc faptul că software-ul în ansamblul său este supus sau nu unor politici de licențiere (inclusiv se vor avea în vedere utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată). Documentele justificative trebuie să fie clare, să permită identificarea tipului de licențiere, metodele de calcul (fie virtual, fizic, grad de încărcare, număr de utilizatori etc.), condițiile de

utilizare, perioada de timp precum și orice altă informație valabilă la momentul contractării). Orice diferend juridic ulterior cu un terț pe subiectul drepturilor de proprietate intelectuală va cădea în sarcina și responsabilitatea Contractantului.

m) Ofertantul va include în oferta sa licențe (drepturi de utilizare pentru Autoritatea Contractantă) pentru toate componentele software livrate. Licențierea poate fi perpetuă sau de tip abonament, fiind incluse și costurile suportului tehnic în condițiile stipulate în prezentul caiet de sarcini.

n) Contractantul va avea obligația să despăgubească Achizitorul împotriva oricăror: a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.) și b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea caietului de sarcini întocmit de către Achizitor.

o) Contractantul va avea obligația ca, la transferul documentelor privind licențele, ca drepturi de folosință, să facă transferul către Achizitor a unor documente în original, atât pentru propriile produse cât și pentru toate cele ale unor terți pe care le-a înglobat, adaptat, modificat, îmbunătățit, ș.a.m.d. și simultan să aibă în vedere că orice reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), în legătură cu produsele achiziționate, montate și puse în funcțiune, vor fi în sarcina și responsabilitatea sa.

p) Toate documentele și informațiile primite de la Contractant precum și rezultatele tuturor activităților Contractantului (cum ar fi: documente de analiză, arhitecturi de sisteme, adrese, etc., fără a se limita la acestea) reprezintă informații confidențiale, iar Ofertantul câștigător va asigura respectarea confidențialității lor.

r) Contractantul și personalul său au obligația de a respecta confidențialitatea documentelor și informațiilor menționate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia și după încetarea contractului.

q) Toate documentele, rapoartele și datele, inclusiv diagrame, scheme tehnice, specificații tehnice, planuri și orice alte materiale realizate de către Contractant în cadrul contractului, trec în proprietatea /proprietatea intelectuală a Achizitorului, aceasta având dreptul să le utilizeze, modifice, transfere fără acceptul Contractantului sau al unei terțe părți. Contractantul le va furniza Achizitorului, la finalizarea contractului, fără a le utiliza în alte scopuri care nu au legătura cu contractul.

s) Contractantul nu va publica articole sau informații legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terți și nu va divulga informațiile obținute de la Achizitor, fără acordul scris al acesteia.

9. IPOTEZE ȘI RISCURI

La elaborarea ofertei, ofertanții trebuie să aibă în vedere cel puțin ipotezele și riscurile descrise în continuare, să estimeze posibilele efecte ale acestora precum și modalitatea de reducere/remediere a riscului. În acest sens, la elaborarea ofertei, ofertantul trebuie să ia în considerare resursele necesare (financiare, de timp, umane și de orice altă natură), pentru implementarea strategiilor de risc propuse.

9.1. IPOTEZE

Ipotezele avute în vedere sunt:
- buna cooperare între contractant și autoritate contractantă, în special între persoanele desemnate în derularea contractului;
- contractantul va furniza servicii la un înalt nivel de calitate, cel puțin egal cu cel solicitat în prezentul caietul de sarcini;
- conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
- nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major executarea și desfășurarea în bune condiții a acordului cadru, respectiv a contractelor subsecvente;
- corelarea dintre resursele necesare și rezultatele așteptate este realistă;
- toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Contractantului.

9.2. RISCURI

Pentru a identifica și combate efectele adverse pe care contractul ar putea să le întâmpine, au fost identificate o serie de riscuri și măsuri de atenuare a acestora.

Autoritatea contractantă își asumă responsabilitatea pentru urmărirea și aplicarea strategiei de răspuns pentru fiecare dintre riscurile identificate pentru implementarea contractului, în sfera sa de responsabilitate.

Contractantul își asumă responsabilitatea pentru urmărirea și aplicarea strategiei de răspuns pentru fiecare dintre riscurile aferente implementării contractului ce cad în sfera sa de responsabilitate.

Riscurile și măsurile de combatere a acestora, care vor fi luate în considerare pe durata implementării serviciilor, sunt:

Nr. crt.	Risc identificat	Măsuri de răspuns / atenuare ale riscului
1	Prelungirea termenelor procedurii de achiziție publică Riscul de anulare și repetare a procedurilor de achiziție publică	- realizarea și actualizarea permanentă a unui plan de achiziții; - analiza permanentă a legislației referitoare la achizițiile publice; - desemnarea unui membru al echipei de proiect cu rol de a coordona și realiza derularea achizițiilor publice Manifestarea acestui risc având în vedere impactul mare pe care îl poate avea precum și

		probabilitatea mare de manifestare îl califică ca fiind critic. Medoda de tratare a acestui risc este prin diminuare (minimizarea manifestării), astfel: - elaborarea documentațiilor de atribuire într-un mod clar și concis, astfel încât sa fie ușor de înțeles de către potențialii ofertanți, reducându-se astfel riscul de a primi doar oferte neconforme care ar conduce la anularea procedurilor
2	Începerea activităților cu întârziere	- realizarea și actualizarea permanentă a unui plan de management; - monitorizarea permanentă a respectării termenelor
3	Adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților	- contractantul va avea o abordare caracterizată de agilitate; - autoritatea contractantă va avea în vedere o abordare pro-activă ce vizează identificarea potențialelor schimbări / modificări cât mai curând posibil și informarea adecvată a Contractantului
4	Obiectul contractului / obligațiile contractuale să fie neîndeplinite / îndeplinite necorespunzător, ori cu întârziere	- autoritatea contractantă introduce în caietul de sarcini cerințe minime privind personalul responsabil de implementarea Contractului, extinse la nivelul factorilor tehnici de evaluare; - stabilirea unor indicatori de performanță ce vor fi avuți în vedere la etapa de recepție și în etapa de întocmire a certificatului constatator; - autoritatea contractantă va solicita constituirea de către Contractant a unei garanții de bună execuție, în cuantum de 10% din valoarea contractului ce va putea fi reținută în condițiile descrise în Contract; - autoritatea contractantă a prevăzut în Contract sancțiunile și penalitățile aplicabile
5	Solicitări de modificare a Personalului desemnat de Contractant pentru implementarea contractului sau modificări în structura organizatorică a Contractantului	- asigurarea flexibilității în planificarea și utilizarea resurselor umane incluse în implementarea contractului și posibilitatea suplimentării resurselor alocate în cazul în care riscul se materializează; - la nivel contractual sunt introduse reguli clare referitoare la modalitățile de înlocuire a personalului Contractantului
6	Regulile privind evitarea conflictului de interese sunt încălcate	- sunt prevăzute reguli clare și precise pentru prevenția conflictului de interese, atât în etapa de ofertare, cât și în etapa de implementare a Contractului; - sunt prevăzute sancțiuni pentru încălcarea regulilor referitoare la conflictul de interese
7	Dificultăți de colaborare și comunicare între factorii	- se va urmări în mod continuu fluxul de comunicare între personalul Autorității

	interesați implicați (inclusiv personal insuficient sau diferențe de înțelegere ale noțiunilor din caietul de sarcini)	Contractante și al Contractantului; - atât Autoritatea Contractantă cât și Contractantul vor avea permanent în vedere o listă de rezervă a personalului responsabil cu implementarea proiectului
8	Datele și informațiile necesare în vederea desfășurării serviciilor comunicate de către autoritatea contractantă nu sunt suficiente pentru îndeplinirea cerințelor solicitate prin caietul de sarcini	- atât Autoritatea Contractantă cât și Contractantul vor monitoriza continuu fluxul de lucru, cu scopul de a remedia deficientele, iar, după caz autoritatea contractanta va pune la dispoziție toate informațiile disponibile pentru îndeplinirea cerințelor solicitate la nivelul de calitate așteptat, conform graficului de prestare a activităților asumat de Contractant

Ofertantul trebuie să prezinte în cadrul propunerii tehnice un **PLAN DE MANAGEMENT AL RISCURILOR**, iar această secțiune să conțină cel puțin:
- descrierea unor riscuri suplimentare relevante, identificate de Ofertant, care pot afecta execuția contractului, precum și măsurile asociate de răspuns/atenuare a riscurilor astfel identificate;
- recomandări suplimentare de reducere/atenuare/eliminare pentru riscurile identificate de Autoritatea Contractantă, fără afectarea cerințelor Caietului de Sarcini.

10. ABORDAREA, METODOLOGIA ȘI PLANUL DE LUCRU ÎN CADRUL CONTRACTULUI

În această secțiune se va prezenta modul în care Ofertantul înțelege contextul, scopul, obiectivele contractului și sarcinile stabilite de autoritatea contractantă.

Astfel, vor fi descrise soluțiile pe care le propune autorității contractante pentru atingerea obiectivelor contractului și modul de abordare ce va fi urmat pentru atingerea rezultatului.

Se vor avea în vederea respectarea cerințelor minimale prevăzute în prezentul caiet de sarcini al achiziției.

În cazul în care, oferta este depusă de o asociere, se va descrie implicarea fiecărui asociat în prestarea serviciilor solicitate, a modului de colaborare între asociați în vederea executării contractului, inclusiv prin delimitarea sarcinilor și responsabilităților individuale în prestarea serviciilor, descrierea oricăror aranjamente de subcontractare a unei părți a serviciilor solicitate, a interacțiunii dintre ofertant și subcontractor/i, precum și o descriere detaliată a serviciilor ce vor fi subcontractate.

Ținând cont de informațiile detaliate în prezentul caiet de sarcini, ofertanții vor detalia în anexe distincte (Oferta tehnică trebuie conțină aceste capitole):
- ***METODOLOGIA PENTRU REALIZAREA SERVICIILOR;***
- ***PLANUL DE LUCRU PENTRU REALIZAREA SERVICIILOR;***
- ***PERSONALUL UTILIZAT PENTRU REALIZAREA SERVICIILOR ȘI ORGANIZAREA ACESTUIA.***

Metodologia propusă va detalia cel puțin modul de organizare a resurselor propuse de Ofertant pentru obținerea rezultatelor la nivelul cantitativ și calitativ așteptat.

Ofertantul are libertatea de a alege metodologia de planificare și realizare a activităților din Contract fără să se înregistreze abateri de la cerințele minime sau condiționări de orice fel.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea metodologiei proprii de management de proiect pe care o va utiliza în cadrul Contractului, din care va reieși cel puțin modul de organizare a resurselor pentru obținerea rezultatelor așteptate.

Metodologia și planul de lucru sunt componente-cheie și obligatorii ale ofertei tehnice.

Ofertantul va trebui să prezinte în cadrul ofertei modul de organizare a activității sale pentru a finaliza fazele de execuție. De asemenea, va descrie detaliat metodele folosite în cadrul contractului, principalele activități legate de organizarea contractului, experții cheie, programul și livrabilele. Descrierea trebuie sa fie suficient de clară și concretă astfel încât să se poată identifica rezultatele pentru fiecare activitate.

Propunerea tehnică va conține cel puțin următoarele:

a. **Viziunea proprie** asupra realizării contractului, din care sa reiasă modul în care a înțeles contextul și scopul acestuia;
b. **Identificarea aspectelor principale** legate de îndeplinirea obiectivelor contractului și a rezultatelor așteptate și o scurtă descriere a acestora;
c. Ofertantul va prezenta detaliat **metodologia de management de proiect** utilizată.

10.1. METODOLOGIA PENTRU REALIZAREA SERVICIILOR

Metodologia de prestare a serviciilor constituie fundamentul conceptual al propunerii tehnice și trebuie să prezinte strategia propusă de ofertant pentru prestarea serviciilor solicitate prin specificațiile tehnice incluse în documentația de atribuire. Ofertantul va demonstra înțelegerea profundă a cerințelor prin prezentarea viziunii sale asupra modului de realizare a contractului, identificând și analizând contextul specific în care se va desfășura contractul, particularitățile sarcinilor stabilite în caietul de sarcini, factorii critici de succes și potențialele riscuri specifice care pot afecta implementarea.

Autoritatea contractantă permite ofertanților să propună o abordare proprie de răspuns la cerințele caietului de sarcini, fără să se înregistreze abateri de la cerințele minime sau condiționări de orice fel.

În această secțiune trebuie prezentate cel puțin următoarele informații:
- obiectivele contractului și sarcinile stabilite prin caietul de sarcini;
- modul de abordare ce va fi urmat în prestarea serviciilor, inclusiv descrierea conceptului utilizat pentru atingerea obiectivelor contractului;
- metodologia de realizare a activităților în scopul obținerii rezultatelor așteptate.
- prevederile legale în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit, ce pot avea incidență asupra derulării/implementării acestuia;
- identificarea și explicitarea aspectelor-cheie privind îndeplinirea obiectivelor contractului și atingerea rezultatelor așteptate;
- modalitatea de abordare a activităților ce corespund rezultatului final al contractului și a rezultatelor intermediare aferente, în raport cu serviciile și responsabilitățile stabilite prin caietul de sarcini.

Toate materialele elaborate trebuie să fie:
- complete, respectiv să conțină toate informațiile și argumentele pentru susținerea îndeplinirii obiectivelor;
- accesibile, fapt ce implică utilizarea unui limbaj cât mai clar și mai simplu, pentru a fi înțeles cu ușurință; acestea trebuie să fie logice și să nu ofere posibilitatea unor interpretări eronate; în cazul utilizării unor termeni tehnici, de specialitate sau abrevieri, aceștia vor fi descriși în mod distinct, într-un glosar de termeni;
- obiective, ceea ce presupune ca acestea să fie echilibrate, fără distorsiuni, pentru a nu crea suspiciuni privind credibilitatea și independența;
- concise, ceea ce presupune redactarea numai a acelor aspecte ce reies din obiective, evitându-se detaliile, formulările și constatările inutile;
- constructive, respectiv să prezinte clar și echilibrat toate aspectele constatate, astfel încât să se evite repetarea unor probleme deja evidențiate;
- oportune și competente, prin respectarea termenelor de elaborare, fără întârzieri, în așa fel încât să reflecte competență și profesionalism;
- convingătoare, ceea ce presupune prezentarea concludentă și exactă a rezultatelor, iar concluziile și recomandările din raport trebuie să fie susținute cu probe suficiente și adecvate;
- Limba oficială de pregătire a tuturor documentelor este limba română.

Pentru a demonstra o foarte bună înțelegere a caietului de sarcini, abordarea și metodologia trebuie să fie adaptate cerințelor specifice ale contractului, fiind descurajate abordările de tip copy-paste.
În această secțiune se va prezenta modul în care Ofertantul înțelege contextul, scopul, obiectivele contractului și sarcinile stabilite de autoritatea contractantă.

Astfel, vor fi descrise soluțiile pe care le propune autorității contractante pentru atingerea obiectivelor contractului și modul de abordare ce va fi urmat pentru atingerea rezultatului.

Activitățile descrise la acest capitol trebuie reprezentate ca durată, la capitolul aferent din planul de lucru.

10.2. PLANUL DE LUCRU

Planul de lucru reprezintă transpunerea operațională a abordării și metodologiei propuse și va prezenta structura detaliată de defalcare a lucrărilor (WBS - Work Breakdown Structure) pentru întregul contract.

Acesta va demonstra alinierea atât cu cerințele caietului de sarcini, cât și cu abordarea și metodologia propuse. Cu titlu exemplificativ, non-limitativ, se vor reflecta concret aspectele de management al calității / management al riscurilor detaliate în etapa anterioară prin transpunerea în planul de lucru a acelor activități/sub-activități necesare pentru transpunerea lor în practică.

Structura WBS va prezenta fazele și etapele contractului, defalcate în activități principale și sub-activități, organizate într-o structură logică și ierarhică.

Pentru fiecare activitate principală, se vor detalia sub-activitățile componente cu un nivel de granularitate care să permită monitorizarea eficientă a progresului, dar fără a genera complexitate excesivă. Nivelul de detaliere va fi de maximum o lună pentru sub-activități, permițând astfel un control al execuției.

Pentru fiecare activitate și sub-activitate, planul de lucru va specifica în mod explicit rezultatele/livrabilele concrete asociate, criteriile clare de acceptare a livrabilelor, durata estimată și justificarea acesteia prin raportare la efortul estimat în zile-om* și resursele alocate.

Se va prezenta matricea de alocare a responsabilităților (RACI) pentru toate activitățile principale, clarificând rolurile fiecărui membru al echipei.

Ofertantul va prezenta structura organizatorică propusă pentru managementul și implementarea contractului, detaliind procesele de coordonare, comunicare și raportare. Se va clarifica procesul de luare a deciziilor, diferențiind între deciziile operaționale și cele strategice care necesită aprobarea autorității contractante. Vor fi prezentate procedurile de escaladare pentru situațiile care necesită intervenție la nivel superior.

Alocarea resurselor umane pentru implementarea contractului va fi prezentată de Ofertant, demonstrând corelația între competențele experților propuși, activitățile necesar a fi realizate și efortul estimat pentru realizarea acestora.

În cazul ofertelor depuse de asocieri, această secțiune va detalia modul în care expertiza și experiența fiecărui membru al asocierii contribuie la implementarea contractului, demonstrând sinergia și complementaritatea competențelor. Similar, pentru serviciile subcontractate, se va prezenta modul în care intervenția subcontractanților se integrează în abordarea generală și mecanismele de coordonare și control avute în vedere.

*NOTĂ: Estimarea efortului este necesară în această etapă pentru a putea evalua planificarea realizată de Ofertant. În etapa de implementare, aceste estimări au caracter orientativ, iar monitorizarea se va realiza EXCLUSIV prin raportare la rezultate/livrabile.

10.3. GRAFIC DE PRESTARE

Graficul de prestare reprezintă planificarea temporală detaliată a tuturor activităților și subactivităților identificate în planul de lucru și constituie instrumentul principal pentru monitorizarea cronologică a progresului contractului. Acesta va fi elaborat utilizând un software profesional de management de proiect care permite calculul automat al drumului critic, nivelarea resurselor și replanificarea dinamică în cazul modificărilor.

Graficul va prezenta toate activitățile și sub-activitățile într-o reprezentare de tip GANTT, cu respectarea structurii WBS, precum și a cerințelor formulate, în care se face referire la termene. Reprezentarea vizuală va permite identificarea rapidă a fazelor, etapelor, activităților principale și subactivităților. Pentru fiecare element vor fi specificate data de început planificată, durata estimată în zile lucrătoare, data de finalizare planificată și resursele umane alocate, demonstrând că planificarea propusă este realistă și fezabilă.

Dependențele dintre activități vor fi modelate folosind tipurile de relații logice necesare, cu specificarea eventualelor decalaje sau constrângeri. Nu este permisă utilizarea constrângerilor temporale fixe de tip “must start on” sau “must finish on”, toate activitățile fiind planificate exclusiv pe baza dependențelor logice. Singura excepție o constituie prima activitate a contractului care marchează data de început. Termenele de implementare și modalitatea de calcul a lunilor proiectului trebuie să fie calculate începând de la data semnării contractului de către părți.

Pentru fiecare fază/etapă/activitate majoră, se vor defini jaloane (milestones) intermediare/finale, avându-se în vedere încadrarea activităților în timp de așa manieră încât să se asigure finalizarea serviciilor în termenul specificat în caietul de sarcini.

Drumul critic al proiectului va fi calculat automat de software și va evidenția secvențele critice care determină durata totală a contractului. Ofertantul va detalia scenarii posibile de optimizare.

Graficul de prestare al proiectului va fi obligatoriu prezentat într-un format electronic care să permită identificarea și vizualizarea automată a Drumului Critic, a relațiilor de dependență dintre activități/sub-activități și replanificarea dinamică în cazul modificărilor. Fișierul transmis de ofertant va putea fi vizualizat de autoritatea contractantă fără costuri suplimentare.

În elaborarea graficului de prestare, Ofertantul va ține cont că serviciile ce trebuie prestate în cadrul contractului, se vor desfășura conform următorului calendar de implementare orientativ, cu încadrare în durata maximă de 24 de luni:

nr.crt	activitati/luna	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	Analiza cerințelor																								
2	Proiectarea solutiei informatice																								
3	Servicii de livrare, instalare si punere in functiune infrastructura software																								
4	Dezvoltarea, configurarea si instalarea aplicatiei informatice																								
5	Testarea aplicatiei și operaționalizarea sistemului IT																								
6	Instruire utilizatori																								
7	Recepții finale																								

Ofertanții pot opta justificat pentru durate diferite pentru fazele proiectului, cu condiția încadrării în termenul contractual maxim. Se va ține cont și de faptul că ultima lună contractuală este dedicată formalităților legate de plată.
Termenii utilizați în calendarul de implementare au următoarele definiții:
- ”Fază” reprezintă un element bine definit și delimitat de acțiune în cadrul contractului ce urmează să fie atribuit, a cărei realizare presupune un timp estimat de realizare rezultat din etapele, respectiv activitățile în care este descompusă;
- ”Etapă” reprezintă un element bine definit și delimitat de acțiune în cadrul unei faze a contractului ce urmează să fie atribuit, a cărei realizare presupune un timp estimat de realizare rezultat din activitățile în care este descompusă;
- ”Jalon” reprezintă un element prin care se marchează finalizarea uneia sau mai multor etape sau faze în cadrul execuției contractului.

În termen de maximum cinci zile lucrătoare de la semnarea contractului, contractantul va actualiza graficul de prestare în consultare cu autoritatea contractantă, pentru a reflecta data efectivă de începere și orice ajustări necesare rezultate din clarificări/constrângeri suplimentare identificate, dacă este cazul. Această versiune actualizată va deveni anexă la contract și va constitui referința oficială pentru monitorizarea execuției și aplicarea eventualelor penalități pentru întârziere.

În cazul în care, din motive obiective, neimputabile Contractantului, pe parcursul implementării, autoritatea contractantă solicită modificarea Graficului de prestare, atunci versiunea astfel actualizată va constitui referința pentru monitorizarea execuției contractului precum si în cazul în care se va impune aplicarea unor penalități de întârziere.

11. LOCUL ȘI DURATA DESFĂȘURĂRII ACTIVITĂȚILOR

11.1. LOCUL DESFĂȘURĂRII ACTIVITĂȚILOR

Activitățile necesare în vederea prestării serviciilor se pot desfășura la sediul Prestatorului, la sediul autorității contractante și în locațiile de implementare a proiectului.

Având în vedere natura activităților, o parte din activitățile ce fac obiectul contractului se pot desfășura și de la distanță, dar Autoritatea Contractantă își rezervă dreptul de a solicita oricând prezența experților Contractantului la sediul ei, atunci când consideră că este necesar.

Pentru activitățile ce vor fi realizate la sediile Autorității contractante, Contractantul trebuie să transmită datele de identificare a persoanelor care își vor desfășura activitatea la acestea și are obligația de a asigura instruirea lucrătorilor proprii cu privire la riscurile specifice activității pe care o vor desfășura la alt sediu decât cel propriu.

Întâlnirea de demarare a activităților din contract (kick-off meeting) între echipa propusă de Contractant și reprezentanții Beneficiarului se realizează la sediul Beneficiarului sau sediul Contractantului (prin stabilire de comun acord).

Întâlnirile de lucru, de monitorizare a progresului activităților și a rezultatelor intermediare, corespunzătoare fiecărei etape din contract sau ori de câte ori sunt necesare se realizează la sediul Beneficiarului (pentru fiecare întâlnire, se stabilește de comun acord). În funcție de subiectele abordate, părțile pot agrea ca aceste întâlniri de lucru să se desfășoare și online.

11.2. DURATA CONTRACTULUI

Durata contractului va fi de cel mult **24 de luni** de la data semnării acestuia de către ambele părți, cu posibilitatea de prelungire în condițiile modificării duratei contractului de finanțare.
Autoritatea contractantă își rezervă opțiunea de a prelungi contractul, în cazul în care proiectul se prelungește. Pentru a exercita această opțiune, Autoritatea contractantă va notifica Contractantului intenția cu 30 de zile înainte de finalizarea contractului sau până la sfârșitul oricărei prelungiri.

12. RESURSE NECESARE / EXPERTIZA NECESARĂ

Pentru prestarea serviciilor solicitate prin Caietul de sarcini, Contractantul trebuie să pună la dispoziția autorității contractante o echipă de experți principali (experți cheie) și secundari (experți non-cheie), care să dețină competențele necesare fiecărui tip de serviciu solicitat, la calitatea și la momentele de timp relevante.

Toate costurile aferente personalului Contractantului (experți cheie, experți non-cheie, personal administrativ) vor fi suportate de Contractant și nu vor fi reflectate distinct în propunerea financiara, ci incluse în prețurile unitare ale produselor și soluțiilor ofertate.

Resursele necesare / expertiza necesară pentru realizarea activităților în contract și obținerea rezultatelor:

Ofertanții vor nominaliza specialiștii care vor asigura pe parcursul contractului serviciile prevăzute.

Ofertanții trebuie să aibă capacitatea de a oferi servicii de calitate, sens în care trebuie să dispună de personal calificat pentru prestarea serviciilor raportat la sarcinile fiecărui specialist solicitat, experții fiind un factor important în execuția și finalizarea cu succes a contractului. Este important ca experții propuși să aibă competențe și experiență dovedite, capabili să ducă la bun sfârșit cu succes sarcinile definite prin prezentul caiet de sarcini, astfel ca, în final, să contribuire la îndeplinirea obiectivului general și a obiectivelor specifice ale contractului, în condițiile respectării cerințelor de calitate și a termenelor stabilite și încadrarea în bugetul prevăzut.

În vederea prestării cu succes a serviciilor prevăzute în caietul de sarcini al achiziției, Contractantul va organiza și va pune la dispoziția Beneficiarului o echipă de experți care, prin atribuțiile și pregătirea lor, vor realiza toate activitățile prevăzute în cadrul contractului.

Contractantul va fi responsabil în exclusivitate și integral pentru stabilirea componenței echipei, pentru organizarea tuturor experților propuși, precum și pentru depunerea efortului necesar desfășurării în bune condiții a tuturor activităților solicitate prin prezentul caiet de sarcină.

În cazul necesității de implicare a unor asemenea experți, este în răspunderea Contractantului:
- să furnizeze suportul necesar, pentru asigurarea îndeplinirii corespunzătoare a obligațiilor contractuale pe toată durata de execuție a contractului;
- să prezinte în cadrul propunerii tehnice rolul și responsabilitățile deținute în vederea execuției contractului, precum și orice alte informații relevante din cadrul cărora să rezulte pregătirea și experiență/competențele profesionale ale acestora.

Pentru prestarea serviciilor solicitate prin Caietul de sarcini, Contractantul trebuie să pună la dispoziția autorității contractante o echipă de **experți principali (experți cheie) și secundari (experți non-cheie)**, care să dețină competențele necesare fiecărui tip de serviciu solicitat, la calitatea și la momentele de timp relevante.

Experții propuși vor fi, de preferat, vorbitori de limba română. În cazul experților propuși care nu sunt vorbitori de limba română, Contractantul va pune la dispoziție interpreți/traducători autorizați în vederea comunicării cu personalul Autorității contractante și în vederea traducerii livrabilelor ce trebuie predate Autorității contractante în limba română. Ofertantul declarat câștigător este responsabil de acoperirea tuturor cheltuielilor referitoare la interpreți/traducători/traduceri.

În conformitate cu principiul recunoașterii reciproce, beneficiarul acceptă documente echivalente celor solicitate la nivelul documentației de atribuire, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Operatorul economic străin trebuie să întreprindă, acolo unde legislația națională impune, demersurile necesare pentru a putea prezenta pe parcursul derulării contractului autorizațiile recunoscute de autoritățile române.

Nu se acceptă îndeplinirea cerințelor minime aferente unui expert-cheie prin cumul de către mai multe persoane.

Prin aceste cerințe se urmărește obținerea unor servicii de calitate și a unei garanții minime că obiectivul general și obiectivele specifice ale achiziției vor fi îndeplinite.

12.1. NUMĂRUL DE EXPERȚI PE CATEGORIE DE EXPERTIZĂ

Cerințe minime pentru personalul de specialitate / Experți

Ofertantul trebuie să demonstreze accesul la personalul de specialitate de care dispune, sau al cărui angajament a fost obținut de către ofertant pentru îndeplinirea corespunzătoare a contractului care urmează a fi atribuit. În acest sens, ofertantul va face dovada că dispune de cel puțin următorii experți care au obligația de a îndeplini anumite cerințe minime și obligatorii:

Nr.	TIP EXPERT CHEIE	Număr experți
1	Expert cheie nr. 1: Manager de proiect	1
2	Expert cheie nr. 2: Expert Analist business	1
3	Expert cheie nr. 3: Expert Arhitect de sistem	1
4	Expert cheie nr. 4: Expert coordonator testare	1
5	Expert cheie nr. 5: Expert implementare Portal	1
6	Expert cheie nr. 6: Expert soluție management documente	
7	Expert cheie nr. 7: Expert implementare soluție de gestiune a utilizatorilor	1
8	Expert cheie nr. 8: Expert software monitorizare date, sisteme și aplicații	1
9	Expert cheie nr. 9: Expert implementare soluție de Asistență Tehnică / Service Desk	1
10	Expert cheie nr. 10: Expert implementare soluție de virtualizare	1
11	Expert cheie nr. 11: Expert hardware și rețele	1
12	Expert cheie nr. 12: Expert securitate informatică	1

Experții cheie au fost solicitați cu respectarea art. 3 din Instrucțiunea președintelui ANAP nr. 1/2017, deoarece activitatea acestora va fi reflectată direct în rezultatul contractului.

12.2. EXPERȚII PRINCIPALI (EXPERȚII CHEIE)

Ofertanții vor prezenta la nivelul ofertei tehnice, lista cu experții propuși care vor realiza efectiv serviciile din cadrul contractului, în care va enumera persoanele nominalizate și în care va descrie modalitatea prin care experții propuși îndeplinesc cerințele.
Fiecare dintre persoanele propuse pentru rolurile de expert-cheie detaliate mai jos trebuie să îndeplinească integral toate cerințele minime aferente rolului pentru care au fost nominalizate.
Toți experții cheie trebuie să dețină o diplomă de absolvire studii superioare indifereent de domeniu cu excepția celor pentru care este mentionat explicit mai jos domeniu.

Pentru demonstrarea îndeplinirii cerințelor minime și, după caz, pentru obținerea punctajului tehnic, ofertanții trebuie să prezinte, pentru fiecare expert-cheie solicitat prin Caietul de sarcini, următoarele informații/documente:

a) în Propunerea tehnică, conform formularului pus la dispoziție de autoritatea contractantă, se va indica numele persoanei propuse pentru fiecare poziție, studiile absolvite, denumirea contractelor / proiectelor similare în care a mai fost implicat și indicații clare privind paginile unde pot fi regăsite documentele suport anexate aferente fiecărui expert;
b) anexate la Formularul de Propunere tehnică, pentru fiecare expert cheie se vor prezenta:
   (i) **Curriculum Vitae (CV)**, semnat de către fiecare titular în parte și datat;
   (ii) Documente referitoare la disponibilitatea expertului cheie - Pentru persoanele propuse care au calitatea de salariați ai ofertantului, se va prezenta în mod obligatoriu orice document prin care să se demonstreze relația contractuală dintre expertul-cheie nominalizat și Ofertant (extras Revisal / Contract de muncă etc.). În cazul în care se propune personal care nu este salariat al Ofertantului, pentru îndeplinirea cerinței de disponibilitate se va anexa o **Declarație de disponibilitate** semnată de titular, cu referire strictă la obiectul contractului ce face obiectul prezentei proceduri;
   (iii) Pentru cerințele privind competențele/calificările profesionale solicitate: copii după documente justificative relevante care demonstrează îndeplinirea cerințelor referitoare la studiile și specializările prezentate în CV: Diplome de studii, certificări în specializarea solicitată, autorizații/atestate profesionale (aflate, acolo unde este cazul, în termen de valabilitate la termenul stabilit pentru depunerea ofertelor), alte documente relevante(recomandări din partea beneficiarilor produselor și serviciilor în care au acumulat experiență similară);
   (iv) Copii după documente justificative relevante care demonstrează îndeplinirea cerințelor referitoare la expertiza și experiența specifică relevantă solicitată și prezentate în CV: Contracte de muncă / Contracte de colaborare / Fișe de post / Adeverințe sau alte documente edificatoare de la beneficiari sau de la angajatori, din care să reiasă în mod clar denumirea, beneficiarul și perioada de realizare a proiectelor / contractelor în care expertul propus a acumulat experiența solicitată și activitățile prestate de către persoana propusă precum și rolul deținut în proiect, care să evidențieze experiența profesională specifică similară;

(v) **<u>Recomandări / Declarații</u>** pe proprie răspundere în ceea ce privește experiența expertului în domeniu. Implicarea și rolul experților în contracte / proiecte care sunt de interes pentru evaluare, poate fi demonstrată și prin recomandări / declarații pe propria răspundere emise de ofertant, cu condiția ca acestea sa fie însoțite de documente care să demonstreze relația contractuală dintre expertul propus și emitentul recomandării, la data derulării proiectului referit și orice documente relevante care să demonstreze participarea expertului propus în implementarea contractului/proiectului prezentat drept experiență specifică. În cazul în care se prezintă declarație pe proprie răspundere/recomandare emisă de ofertant, aceasta va cuprinde în mod obligatoriu, pe lângă celelalte informații necesare, următoarea mențiune: *„Cunosc prevederile art. 57 din Regulamentul financiar UE nr.966/2012 și legislația națională în vigoare cu privire la conflictul de interese, precum și prevederile art.292 „Falsul în declarații" din Codul penal potrivit căruia „Declararea necorespunzătoare a adevărului, făcută unui organ sau instituții de stat ori unei alte unități în vederea producerii unei consecințe juridice, pentru sine sau pentru altul, atunci când, potrivit legii ori împrejurărilor, declarația făcută servește pentru producerea acelei consecințe, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă."*

Prin depunerea ofertei, Ofertantul își asumă răspunderea cu privire la conformitatea cu originalul a oricăror documente depuse în copie.

Se acceptă prezentarea de documente echivalente în conformitate cu prevederile art. 202 alin. (4) din Legea nr. 98/2016, prin intermediul cărora se probează în mod concludent, îndeplinirea respectivelor cerințe. Sarcina probei incumbă ofertantului, autoritatea contractantă rezervând-si dreptul de a solicita, dacă se consideră necesar, clarificări privind documentele prezentate.

Certificatele/diplomele/documentele justificative emise în altă limbă decât limba română vor fi prezentate în limba de origine, însoțite de traducerea autorizată în limba română.

În urma verificării exactității informațiilor și a dovezilor furnizate de către ofertanți, autoritatea contractantă poate solicita și alte documente/informații care să clarifice experiența similară solicitată atât ofertantului, cât și experților-cheie. De asemenea, autoritatea contractantă își rezervă dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experiența profesională, în vederea confirmării celor prezentate de către ofertanți.

Autoritatea contractantă își rezervă dreptul de a verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți și de a solicita și alte documente/ informații care să clarifice experiența profesională respectivă.

Ofertanții vor transmite documentele solicitate în caietul de sarcini care certifică îndeplinirea cerințelor minime de calificare, pentru experții cheie.

Înlocuirea experților cheie

Pe parcursul derulării Contractului, modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează conform prevederilor art. 162 din HG nr. 395/2016 și în condițiile clauzelor prevăzute în Contract.

Un membru al echipei de proiect poate fi înlocuit pe parcursul derulării contractului doar cu notificarea prealabilă a beneficiarului cu minim 10 zile calendaristice înainte de data propusă pentru înlocuire. Notificarea va fi în mod obligatoriu însoțită de documentele justificative asociate noului expert, așa cum au fost acestea solicitate prin documentația de atribuire a contractului. Contractantul are obligația de a se asigura că expertul nou propus îndeplinește toate cerințele minime solicitate de beneficiar pentru expertul înlocuit (precum și toate calificările sau experiența suplimentară care a făcut obiectul evaluării ofertelor), inclusiv condițiile și cerințele cu privire la inexistența unui conflict de interese.

Astfel, înlocuirea experților nominalizați se realizează numai cu acceptul Autorității contractante, această modificare nereprezentând o modificare substanțială, așa cum este aceasta definită în art. 221 din Legea nr. 98/2016, decât în situația în care noul expert nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin criteriile de calificare solicitate pentru expertul care este înlocuit, așa cum au fost prevăzute în cadrul documentației de atribuire.

În situațiile prezentate anterior, Contractantul are obligația de a transmite pentru noul personal, documentele solicitate prin caietul de sarcini, în vederea demonstrării îndeplinirii cerințelor stabilite prin prezentul caiet de sarcini.

Autoritatea contractantă are dreptul de a respinge motivat noul expert propus, în situația în care constată că acesta nu îndeplinește cerințele minime prevăzute în documentația de atribuire sau constată existența unui conflict de interese.

În cazul în care un membru al personalului Contractantului implicat în implementarea contractului (inclusiv experți cheie) trebuie înlocuit, înlocuirea se va face prin raportare la cerințele solicitate prin prezentul caiet de sarcini și oferta depusă, iar dacă experiența/calificarea expertului înlocuit au făcut obiectul aplicării vreunui factor de evaluare și a fost acordat un anumit punctaj, înlocuitorul acestuia trebuie să dețină cel puțin experiența și calificarea corespunzătoare astfel încât după aplicarea algoritmului de calcul al punctajului, expertul înlocuitor să obțină minim punctajul obținut de expertul înlocuit la faza de atribuire a contractului.

Îndeplinirea acestui criteriu (obținerea cel puțin a aceluiași punctaj) este suficientă pentru considerarea ca acceptabil a expertului înlocuitor, din punct de vedere al experienței/calificării. Autoritatea contractantă va putea respinge experții propuși pentru înlocuire sau solicita argumentat înlocuirea experților în situația în care aceștia nu îndeplinesc cerințele/sarcinile precizate în prezentul caiet de sarcini și în ofertă.

Costurile suplimentare generate de înlocuirea personalului incumbă Contractantului. În cazul în care expertul nu este înlocuit imediat şi funcțiile acestuia urmează să fie preluate după o anumită perioadă de timp de către noul expert, Autoritatea contractantă poate solicita Contractantului să desemneze un expert temporar pentru Proiect, până la sosirea noului expert, sau să ia alte măsuri pentru a compensa absența temporară a expertului absent.

Experiența specifică a experților, necesară pentru a îndeplini sarcinile din cadrul contractului de achiziție publică poate fi demonstrată prin îndeplinirea unor activități/responsabilități similare cu cele pe care urmează să le îndeplinească în prezentul contract.

Echipa ce va fi prezentată de ofertant va trebui sa aibă o vastă experiența în implementarea de sisteme informatice integrate. În acest sens, ofertantul trebuie să asigure pe întreaga perioada de derulare a contractului personalul necesar în funcție de obiectivele, rezultatele și activitățile/ livrabilele solicitate în prezentul document, garantând cel puțin personalul având calificarea și experiența profesională descrisă mai jos.

Ofertantul va prezenta componența echipei, instrumentele/ metodele de coordonare a activității acesteia și va detalia rolurile, atribuțiile și responsabilitățile experților și modalitatea concretă în care echipa prezentată interacționează cu personalul de suport/ back-stopping pentru îndeplinirea contractului.

Profilul, cerințele minime și obligatorii ale experților pe fiecare categorie în parte, se regăsește mai jos:

12.3. PROFILUL EXPERȚILOR CHEIE

12.3.1. Expert cheie nr. 1: Manager de proiect

Responsabilități:

- Organizează și asigură bunul mers al activităților desfășurate de către echipa Furnizorului în cadrul proiectului;
- Asigură interfața cu structurile care participă la execuția contractului, respectiv cu persoanele responsabile nominalizate de către acesta, cu care va colabora pe întreaga durată a contractul (punct principal de contact în comunicarea cu beneficiarul);
- Răspunde de managementul contractului conform metodologiei agreate cu beneficiarul, respectiv de activitățile de planificare, organizare a execuției, monitorizare, control și încheiere a proiectului;
- Asigură coordonarea echipei de implementare a proiectului;
- Alocă resursele în cadrul proiectului astfel încât Furnizorul să aibă capacitatea de a răspunde în mod optim necesităților, constrângerilor și obiectivelor beneficiarului;
- Analiza gradului în care livrabilele proiectului corespund cerințelor de business;
- Asigură elaborarea proceselor-verbale de recepție/rapoartelor de activitate și alte documente de raportare a progresului către beneficiar.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar în care serviciile au fost duse la bun sfârșit, la nivelul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Competențe profesionale	- Studii de specializare în **managementul proiectelor** dovedite prin prezentarea unei diplome/ a unui certificat de absolvire în domeniul managementului de proiect, eliberat(ă) de un organism de formare,

	pentru ocupația manager de proiect (**COR 242101/241919**) sau echivalent, sau prin prezentarea de diplome de studii superioare care au inclus în curriculumul educațional cursuri de management de proiect

12.3.2. Expert cheie nr. 2: Expert Analist business

Responsabilități:

- Analiza cerințelor și specificațiilor tehnico-funcționale ale sistemului;
- Participare la modelarea datelor și la definirea funcțională a aplicației;
- Identificarea proceselor interne ale beneficiarului;
- Colectarea și validarea datelor documentate de la beneficiar;
- Furnizarea informațiilor, restricțiilor precum și recomandărilor privind implementarea sistemului;
- Elaborarea fluxurilor de informație și a specificațiilor de interconectare;
- Participă la elaborarea manualelor de utilizare;
- Acordă suport utilizatorilor cheie pentru testarea de acceptanță a sistemului;
- Colaborarea cu echipele tehnice (Realizarea de interviuri cu persoanele implicate).

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Calificare educațională	Studii universitare absolvite cu diploma de licență (sau echivalent) într-unul din domeniile detaliate **ISCED F-2013 ”Matematică”, ”Dezvoltarea și analiza soft și aplicații”, ”Electronică și automatică”, ”Programe și calificări interdisciplinare legate de tehnologia informației și comunicațiilor (TIC)”**. Sunt acceptate și studiile universitare de masterat absolvite în aceleași domenii detaliate ISCED F-2013
Competențe profesionale	Deținerea de competențe privind analiza de business în contextul sistemelor informatice și/sau privind modelarea proceselor de business în contextul sistemelor informatice, dovedite prin certificare recunoscută la nivel național sau internațional. a. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.3. Expert cheie nr. 3: Expert Arhitect de sistem

Responsabilități:

- Proiectarea arhitecturii la nivel hardware, software și funcțională a sistemului;
- Proiectarea și documentarea arhitecturii, a specificațiilor funcționale, respectiv a specificațiilor de integrare;
- Elaborarea documentației de proiectare;
- Definire cerințe funcționale, non-funcționale și de integrare, proiectare model de date și procese;
- Este responsabil de implementarea sistemului integrat în conformitate cu cerințele Beneficiarului și documentația de proiectare;
- Verificarea documentelor de natură tehnică elaborate de către echipa Contractantului pe durata derulării proiectului;
- Urmărirea respectării caracteristicilor proiectate pe parcursul implementării sistemului.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Calificare educațională	Studii universitare absolvite cu diploma de licență (sau echivalent) într-unul din domeniile detaliate **ISCED F-2013 ”Matematică”, ”Dezvoltarea și analiza soft și aplicații”, ”Electronică și automatică”, ”Programe și calificări interdisciplinare legate de tehnologia informației și comunicațiilor (TIC)”**. Sunt acceptate și studiile universitare de masterat absolvite în aceleași domenii detaliate **ISCED F-2013**
Competențe profesionale	Deținerea de competențe în dezvoltarea arhitecturii de sistem, dovedite prin prezentarea unei certificări în domeniu recunoscute la nivel național sau internațional. a. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.4. Expert cheie nr. 5: Expert coordonator testare

Responsabilități:
- coordonarea tuturor activităților de testare și a echipei de testare:
- Testarea aplicațiilor software din punct de vedere tehnic, funcțional, performanță și identificarea posibilelor erori;
- Testarea tuturor cerințelor din caietul de sarcini, și a celor identificate/detaliate în urma desfășurării etapei de analiză și proiectare;
- Analiza problemelor și recomandarea de soluții;
- Identificarea, specificarea și implementarea îmbunătățirilor în ceea ce privește funcționarea soluțiilor software;
- Crearea de scenarii de utilizare și scripturi de testare dacă e cazul;
- Va conlucra îndeaproape cu ceilalți experți și cu echipa de implementare, fiind responsabil de testarea tehnică, funcțională și de performanță a întregii platforme;
- Acesta va fi responsabil de elaborarea documentației de testare. De asemenea, are ca responsabilitate finală întocmirea Raportului de Testare a soluției;

- Avizează documentațiile de proiectare și testare elaborate de către echipa Contractantului pe durata derulării proiectului.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Calificare educațională	Deținerea de **competente privind stabilirea activităților optime de testare pe baza efectuării analizei sistemelor informatice și realizarea testelor în funcție de metodologia specifica de dezvoltare a software-ului suspus respectivelor teste** (dovedite prin participarea la cel puțin un program de perfecționare în acest domeniu și prezentarea diplomei / certificării aferente recunoscuta la nivel național / internațional, cum ar fi cele echivalente cu **ISTQB**). Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.5. Expert cheie nr. 5: Expert implementare Portal

Responsabilități:

- transpunerea în funcționalități a cerințelor documentate în etapele de analiză și proiectare;
- participarea la activitățile de instalare și dezvoltare/configurare a Portalului;
- testarea funcționării soluției instalate și configurate, la nivelul sistemului, cu setul de date de test agreat cu Beneficiarul astfel încât să fie acoperite cerințele specifice de sistem;
- asigurarea expertizei în domeniul tehnic cu privire la Portal, precum și participarea la activitățile de testare;
- colaborarea cu ceilalți membrii ai echipei cu scopul de a asigura implementarea corectă a cerințelor Beneficiarului;
- documentarea configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Beneficiarului;
- Stabilirea și elaborarea curriculei pentru instruirea utilizatorilor standard privind funcționalitățile sistemului implementate;
- Participarea la elaborarea documentației de instruire atât pentru utilizatorii cât și pentru administratorii sistemului;
- Participarea la elaborarea documentațiilor de utilizare și administrare pentru soluția implementată.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare

Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Calificare educațională	Studii universitare absolvite cu diploma de licență (sau echivalent) într-unul din domeniile detaliate **ISCED F-2013 "Matematică", "Dezvoltarea și analiza soft și aplicații", "Electronică și automatică", "Programe și calificări interdisciplinare legate de tehnologia informației și comunicațiilor (TIC)"**. Sunt acceptate și studiile universitare de masterat absolvite în aceleași domenii detaliate ISCED F-2013
Competențe profesionale	Certificare profesională eliberată sau atestată /recunoscută național/ internațional care să demonstreze **specializarea în platforma de Portal ofertată**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.6. Expert cheie nr. 6: Expert implementare soluție management documente

Responsabilități:

- Transpunerea în funcționalități a cerințelor documentate în etapele de analiză și proiectare;
- Participarea la activitățile de instalare, dezvoltare/configurare a soluției EIP ofertate;
- Documentarea aplicațiilor dezvoltate și a configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Beneficiarului;
- Testarea funcționării soluției instalate și configurate, la nivelul sistemului, cu setul de date de test agreat cu Beneficiarul astfel încât să fie acoperite cerințele specifice de sistem;
- Colaborează cu managerul de proiect, cu arhitectul și ceilalți membrii ai echipei pentru înțelegerea și implementarea specificațiilor funcționale ale soluției;
- Asigurarea expertizei în domeniul tehnic cu privire la soluția EIP ofertată, precum și participarea la activitățile de testare internă, înainte de testarea acesteia de către Beneficiar;
- Documentarea aplicațiilor dezvoltate și a configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Beneficiarului;
- Participarea la elaborarea documentației de instruire atât pentru utilizatorii finali cât și pentru administratorii sistemului;
- Stabilirea și elaborarea curriculei pentru instruirea utilizatorilor finali privind funcționalitățile sistemului implementate.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract

Competențe profesionale	Certificare profesională atestată /recunoscută național/ internațional care să demonstreze **specializarea în soluția DMS propusă**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor / autorizațiilor în cauză

12.3.7. Expert cheie nr. 7: Expert implementare soluție de gestiune a utilizatorilor

Responsabilități:

- Activități specifice de implementare și configurare a componentelor oferite pentru gestiunea utilizatorilor;
- Activități specifice de implementare și configurare a componentei oferite pentru control access – single sign-on;
- Activități specifice de implementare și configurare a componentei oferite pentru stocare profil utilizatori;
- Activități specifice de configurare din punct de vedere securitate a soluției pentru gestiunea utilizatorilor;
- Instruirea utilizatorilor și administratorilor Autorității Contractante privind funcționalitățile implementate;
- Asigurarea suportului tehnic pentru echipa Autorității Contractante.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Competențe profesionale	Certificare profesională atestată /recunoscută național/ internațional care să demonstreze **specializarea în soluția propusă pentru gestiunea utilizatorilor**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.8. Expert cheie nr. 8: Expert software monitorizare date, sisteme și aplicații

Responsabilități:

- transpunerea în funcționalități a cerințelor documentate în etapele de analiză și proiectare;
- participarea la activitățile de instalare și dezvoltare/configurare a soluției software monitorizare date, sisteme și aplicații;
- testarea funcționării soluției instalate și configurate, la nivelul sistemului, cu setul de date de test agreat cu Beneficiarul astfel încât să fie acoperite cerințele specifice de sistem;
- asigurarea expertizei în domeniul tehnic cu privire la soluția software monitorizare date, sisteme și aplicații, precum și participarea la activitățile de testare;

- colaborarea cu ceilalți membrii ai echipei cu scopul de a asigura implementarea corectă a cerințelor Beneficiarului;
- documentarea configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Beneficiarului;
- Stabilirea și elaborarea curriculei pentru instruirea utilizatorilor privind exploatarea soluției implementate;
- Participarea la elaborarea documentației de utilizare și administrare pentru soluția implementată.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrula cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Competențe profesionale	Certificare profesională eliberată sau atestată /recunoscută național/ internațional care să demonstreze **specializarea în domeniul de monitorizare date, sisteme și aplicații ofertată**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor / autorizațiilor în cauză

12.3.9. Expert cheie nr. 9: Expert implementare soluție de Asistență Tehnică / Service Desk

Responsabilități:
- Activități de consultanță tehnică de specialitate cu echipa de proiect pentru definirea activităților și pașilor de integrare cu Componenta de Asistență Tehnică;
- Activități specifice de implementare și configurare a Componentei de Asistență Tehnică;
- Activități specifice de configurare din punctul de vedere al securității accesului și utilizării a Componentei de Asistență Tehnică;
- Instruirea utilizatorilor și administratorilor Autorității Contractante privind funcționalitățile implementate;
- Asigurarea suportului tehnic pentru echipa Autorității Contractante;.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Competențe profesionale	Certificare profesională atestată /recunoscută național/ internațional care să demonstreze **specializarea în soluția de Asistență Tehnică propusă**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii

	Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.10. Expert cheie nr. 10: Expert implementare soluție de virtualizare

Responsabilități:
- Activități de consultanță tehnică de specialitate cu echipa de proiect pentru definirea activităților și pașilor de implementare a soluției de virtualizare;
- Activități specifice de implementare și configurare a soluției de virtualizare;
- Activități specifice de configurare din punctul de vedere al securității accesului și utilizării soluției de virtualizare;
- Instruirea administratorilor Autorității Contractante privind funcționalitățile implementate;
- Asigurarea suportului tehnic pentru echipa Autorității Contractante;.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul cel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Competențe profesionale	Certificare profesională atestată /recunoscută național/ internațional care să demonstreze **specializarea în soluția de virtualizare propusă**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză

12.3.11. Expert cheie nr. 11: Expert hardware și rețele

Responsabilități:
- Activități de consultanță tehnică de specialitate cu echipa de proiect pentru definirea activităților și pașilor de configurare a infrastructurii hardware și de rețea;
- Activități specifice de instalare și configurare a infrastructurii hardware și de rețea;
- Instruirea administratorilor Autorității Contractante privind funcționalitățile implementate;
- Asigurarea suportului tehnic pentru echipa Autorității Contractante.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul acel puțin un proiect/contract similar, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Competențe profesionale	Certificări profesionale atestate /recunoscute național/ internațional care să demonstreze **specializarea în instalarea și configurare echipamentelor hardware și de rețea ofertate**. Sunt acceptate și

	documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/ autorizațiilor în cauză

12.3.12. Expert cheie nr. 12: Expert securitate informatică

Responsabilități:
- Identificarea și analiza riscurilor de securitate ale soluției;
- Definirea controalelor de securitate pentru asigurarea îndeplinirii cerințelor specifice solicitate;
- Acordarea de suport pentru înțelegerea deplină a problemelor identificate și alegerea măsurilor/metodelor aplicabile pentru remedierea acestora, în scopul minimizării riscurilor de securitate informatică;
- Implementarea controalelor de securitate în cadrul soluției implementate.

Cerințe:

Experiență generală: minim 5 ani de la absolvirea studiilor superioare	
Experiența specifică	Experiență specifică dovedita prin participarea in cadrul a cel puțin un **proiect/contract similar**, în care serviciile au fost duse la bun sfârșit, în cadrul căruia expertul a avut responsabilități și atribuții similare poziției pentru care este propus în prezentul contract
Calificare educațională	Certificare profesională eliberată sau atestată /recunoscută național/ internațional care să demonstreze **specializarea în evaluarea securității sistemelor informatice**. Sunt acceptate și documente echivalente celor solicitate, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/ autorizațiilor în cauză

NOTĂ 1:
Referitor la experiența specifică solicitată experților cheie, prin „proiect/contract similar" se înțelege un contract / proiect de dezvoltare software si/sau implementarea unei soluții și/sau sistem informatic integrat.

NOTĂ 2:
Prin „servicii duse la bun sfârșit" se înțeleg serviciile finalizate, care au fost recepționate. Dovada se va face prin depunerea documentelor justificative, cum ar fi: documente constatatoare, procese-verbale de recepție, recomandări sau alte documente de la Beneficiar/Beneficiarii produselor și/sau serviciilor în care au acumulat experiență similară. Precizăm că factura fiscala nu reprezintă document care probează livrarea produselor. Aceasta poate fi luată în considerare doar daca este însoțită de documente de recepție care să ateste livrarea produselor.

12.4. ALTE CONDIȚII REFERITOARE LA CALIFICAREA EXPERȚILOR

Eventualele diplome/certificări/autorizații/atestate prezentate trebuie să fie emise de o autoritate publică competentă sau de către un organism de drept public/privat care

respectă standardele europene de certificare - ISO IEC 17024 (înțelegând prin aceasta organisme al căror obiect de activitate este formarea/perfecționarea profesională, indiferent de forma de organizare a respectivelor entități publice/private ca ONG-uri, universități/academii/companii de profil ce emit astfel de certificări). Se acceptă prezentarea de documente echivalente în conformitate cu prevederile art. 202 alin. (4) din Legea nr. 98/2016, prin intermediul cărora se probează în mod concludent, îndeplinirea respectivelor cerințe. Sarcina probei incumbă ofertantului, autoritatea contractantă rezervând-si dreptul de a solicita, dacă se consideră necesar, clarificări privind documentele prezentate.

În cazul în care experții prezentați din cadrul echipei de proiect nu sunt vorbitori de limba română, ofertantul va asigura pe costul sau servicii de traducere și interpretariat de specialitate în limba româna, pe toata durata contractului. Ofertantul va lua toate măsurile pentru asigurarea unor traduceri de calitate.

Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.

Autoritatea contractantă își rezervă dreptul:
- de a verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți și de a solicita și alte documente/ informații care să clarifice experiența echipei de proiect propusă;
- de a contacta beneficiarii proiectelor/ contractelor prezentate la experiență profesionala, în vedere confirmării celor prezentate de către ofertanți.

Pentru fiecare persoană nominalizată în echipă ca expert, se va prezenta **Declarația de confidențialitate**, semnată de către persoana respectivă (olograf sau semnată cu semnătură electronică extinsă bazat pe un certificat calificat, valabil, eliberat de un furnizor de servicii de certificare acreditat în condițiile legii), din care se rezulte că persoana respectivă:
- va păstra confidențialitatea în legătură cu faptele, informațiile sau documentele de care ia la cunoștință pe perioada derulării Contractului;
- nu va face cunoscut Contractul sau orice prevedere a acestuia unei terțe părți, în afara persoanelor implicate în îndeplinirea Contractului;
- se angajează ca dezvăluirea oricărei informații față de persoanele implicate în îndeplinirea Contractului să se facă în mod confidențial și să se extindă doar asupra acelor informații necesare în vederea îndeplinirii Contractului;
- se angajează să ia toate măsurile necesare pentru a asigura ca toate informațiile confidențiale sunt tratate ca și confidențiale și că nu sunt divulgate sau folosite în alte scopuri decât în relație strictă cu Contractul.

12.5. EXPERȚI SECUNDARI (EXPERȚI NON-CHEIE)

Ofertanții au dreptul de a include în oferte și alți experți în afara celor indicați în caietul de sarcini al achiziției, în cazul în care consideră că aceștia sunt necesari în vederea bunei derulări a contractului și a atingerii obiectivului acestuia.

Ofertantul poate propune experți non-cheie în afara celor solicitați, **fără a-i nominaliza**, însă cuprinzând în Propunerea tehnică activitățile lor, făcând dovada unei planificări realiste menite să asigure realizarea livrabilelor contractului.

Experții non-cheie vor lucra în permanență sub coordonarea experților cheie nominalizați.

Pentru experții non-cheie, Ofertantul va prezenta numai informații privind modul de implicare a acestora în activitățile proiectului, responsabilitățile și momentul implicării în echipa de proiect în momentele necesare.

Pentru experții non-cheie NU este necesară prezentarea în cadrul Propunerii Tehnice nici a identității exacte a acestora și nici a vreunui document suport.

Contractantul va prezenta, pe parcursul implementării contractului, pentru fiecare expert non cheie propus, următoarele informații/documente:
- numele persoanei propuse pentru fiecare poziție;
- curriculum Vitae (CV), semnat de către titular și datat;
- declarația privind disponibilitatea, semnată în original;
- copii ale documentelor justificative relevante care demonstrează îndeplinirea cerințelor referitoare la studiile, expertiza și experiența specifică relevantă solicitată și prezentată în CV, cum ar fi:
    - diplome de studii, certificări, alte diplome relevante;
    - recomandări sau alte documente edificatoare din care să reiasă activitățile desfășurate și care să evidențieze experiența profesională specifică relevantă.

Toate costurile aferente personalului Contractantului (experți cheie, experți non-cheie, personal administrativ) vor fi suportate de Contractant și nu vor fi reflectate distinct în propunerea să financiara, ci incluse în prețurile unitare ale produselor și soluțiilor ofertate.

12.6. PERSONALUL ADMINISTRATIV ȘI PERSONALUL SUPORT / BACKSTOPPING PENTRU ACTIVITATEA EXPERȚILOR PRINCIPALI ÎN CADRUL CONTRACTULUI

Contractantul va asigura personalul administrativ/suport care este necesar pentru desfășurarea activității echipei sale.

În plus, Contractantul va asigura pentru serviciile din contract, personal de backstopping pentru prestarea serviciilor.

Prin personal de backstopping se înțelege personal de înaltă calificare al Contractantului care acordă sprijin echipei de experți implicați în derularea activităților în Contract. Sprijin înseamnă orice activitate care contribuie la îndeplinirea serviciilor conform Contractului.

De asemenea, dacă Ofertantul consideră că pe lângă experții solicitați de autoritatea contractantă, sunt necesari și alți experți pentru îndeplinirea corespunzătoare și la timp a activităților prevăzute în Caietul de sarcini, acesta are obligația să prevadă aceste resurse și să includă în propunerea financiară costurile aferente.

12.7. RESURSELE CONTRACTANTULUI, NECESARE PENTRU DESFĂȘURAREA ACTIVITĂȚILOR CONTRACTULUI

Ofertantul devenit Contractant trebuie să se asigure că personalul care își desfășoară activitatea în cadrul Contractului dispune de sprijinul material și de infrastructura necesară pentru a permite acestuia să se concentreze asupra realizării activităților din cadrul Contractului. Toate costurile vor fi incluse în costurile unitare ofertate, nefiind decontate separat.

Ofertantul va prezenta în propunerea tehnică o listă cu dotările existente sau a aranjamentelor întreprinse pentru a avea acces la dotările necesare pentru o bună implementare a contractului.

În consecință, se consideră necesara alocarea de către furnizorul Sistemului Informatic a unor resurse umane specializate.

12.8. INFRASTRUCTURA CONTRACTANTULUI NECESARĂ PENTRU DESFĂȘURAREA ACTIVITĂȚILOR CONTRACTULUI

Ofertantul, devenit Contractant, trebuie să se asigure că personalul care își desfășoară activitatea în cadrul Contractului, dispune de sprijinul material și de infrastructura necesară pentru a permite acestuia să se concentreze asupra realizării activităților din cadrul Contractului.

Pentru îndeplinirea cu succes a activităților descrise, Contractantul va pune la dispoziția echipei de proiect proprii toate resursele materiale necesare. În mod minimal, fiecare expert va avea la dispoziție un echipament de calcul portabil, pe care va exista instalat software tip office (editor de text, program de calcul tabelar, instrument de realizare prezentări grafice etc.).

De asemenea, Contractantul va pune la dispoziție următoarele:
- Hardware necesar pentru prestarea serviciilor;
- Instrumente software pentru prestarea serviciilor.

Contractantul are obligația ca toate instrumentele software utilizate pentru îndeplinirea contractului (producerea livrabilelor necesare) să fie licențiate conform prevederilor legale în vigoare și în funcție de tipul de instrument folosit, modul de licențiere recomandat de producător, număr de utilizatori, etc.

În calitate de solicitant al investiției, **APIA** înțelege că pentru bunul mers al proiectului ce face obiectul investiției trebuie să pună la dispoziție toate resursele necesare îndeplinirii cu succes a proiectului.

Întregul proiect se va realiza și implementa la sediul **APIA** sau într-o locație desemnată de **APIA**.

În cadrul proiectului se va asigura dotarea hardware necesară pentru realizarea, testarea și operarea curentă a sistemului propus. Astfel, vor fi achiziționate de furnizorul soluției informatice și vor rămâne în proprietatea **APIA** resursele materiale descrise în secțiunea de componente din cadrul arhitecturii funcționale a sistemului.

În același timp, beneficiarul va pune la dispoziție pentru buna desfășurare a fazelor proiectului, dar și pentru exploatarea curentă a acestuia după implementare, dotări și resurse materiale existente.

Dintre aceste resurse disponibile, enumeram:

Instituția	Adresa de implementare	Resurse materiale puse la dispoziție de către instituție
APIA	Bd. Carol I, București	Spațiu în centrul de date

12.9. INFRASTRUCTURA ȘI RESURSELE DISPONIBILE LA NIVEL DE AUTORITATE CONTRACTANTĂ PENTRU ÎNDEPLINIREA CONTRACTULUI

În situația în care va fi necesar, pentru derularea proiectului în bune condiții, autoritatea contractantă va pune la dispoziție Contractantului următoarele:

- Sediul propriu;
- Dotările permanente: mobilier, linii de comunicații, etc.;
- **Activitățile desfăsurate la sediul APIA,** repectiv, cheltuielile administrative (energie electrică, termică, comunicații, etc.) vor fi suportate de către **APIA**.

13. MANAGEMENTUL/GESTIONAREA CONTRACTULUI ȘI ACTIVITĂȚI DE RAPORTARE

Managementul contractului include o **componentă de management** și o **componentă administrativă** (de administrare efectivă a contractului) și presupune coordonarea continuă, monitorizarea și controlul tuturor activităților și rezultatelor realizate de Contractant.

Contractantul este pe deplin responsabil de managementul contractului din punct de vedere administrativ, financiar, orientat spre obținerea rezultatelor. Acesta trebuie să respecte toate condițiile formulate în prezentul caiet de sarcini.

- Coordonarea implică:
  - organizarea întâlnirilor de analiză a modalității de executare a contractului;
  - coordonarea resurselor implicate și a activităților realizate în executarea contractului.

- Monitorizarea implică:
  - Analiza/măsurarea și evaluarea modalității de executare a obligațiilor contractuale prin raportare la prevederile contractuale. Pentru activitățile de monitorizare se utilizează cel puțin următoarele elemente:
    - Informațiile din propunerea tehnică, pe baza cerințelor din caietul de Sarcini;
    - Informațiile din propunerea financiară și clauzele contractuale privind modalitatea de plată.
  - Constatarea conformității prin acceptarea serviciilor prestate, pe baza procedurii și criteriilor de recepție incluse în caietul de sarcini, condițiile contractuale;

- Controlul implică:
  - identificarea acțiunilor corective pentru abordarea abaterilor de la condițiile contractuale, constatate în cadrul întâlnirilor dintre contractant și autoritatea contractantă.

13.1. GESTIONAREA RELAȚIEI DINTRE CONTRACTANT ȘI AUTORITATEA CONTRACTANTĂ

Contractantul va adopta o atitudine constructivă (pro-activă), caracterizată de agilitate, în îndeplinirea obiectivelor contractului, demonstrând capacitatea de a se adapta modificărilor din proiectul în care este implicat. Contractantul trebuie să consulte Autoritatea contractantă cu privire la orice aspect / problemă, evitând implicarea acesteia în aspecte de micro management al Contractului.

Fiecare parte contractantă are obligația coordonării propriilor resurse și a activităților pentru derularea contractului, în conformitate cu atribuțiile precizate în prezentul caiet de sarcini.

Achizitorul și Furnizorul identifică acțiunile corective pentru abordarea abaterilor constatate față de prevederile contractului.

Pe parcursul derulării contractului, Achizitorul verifică dacă toate activitățile planificate au fost realizate conform clauzelor contractuale. Achizitorul se asigură pe toată perioada derulării contractului și nu doar la finalizarea / terminarea acestuia că

activitățile planificate au fost realizate, cerințele stabilite au fost îndeplinite, serviciile au fost prestate, soluția informatică implementată a fost admisă la recepție și instruirea personalului a fost finalizată.

Furnizorul este responsabil în totalitate de asigurarea managementului contractului din punct de vedere administrativ și financiar, sens în care va fi orientat spre obținerea rezultatelor stabilite pentru îndeplinirea obiectivelor. Acesta trebuie să respecte condițiile formulate în contract.

13.1.1. Ședințe / întâlniri

Un instrument în derularea activității de monitorizare vor fi ședințele/întâlnirile dintre echipa Contractantului și echipa Autorității contractante, ședințe care au drept scop și urmărirea progresului Contractului.

Pentru buna desfășurare a activităților și atingerea rezultatelor proiectului, Contractantul va colabora permanent cu echipa de implementare a proiectului.

În termen de **5 zile lucrătoare de la data semnării contractului**, va fi organizată o **întâlnire de lucru** la care vor participa reprezentanți ai Autorității contractante (membrii echipei de implementare a proiectului), pentru obținerea asigurării că Autoritatea Contractantă și Contractantul au aceeași perspectivă asupra activităților și rezultatelor din Contract.

Autoritatea contractantă va organiza prima întâlnire de lucru la care vor participa reprezentanți ai Autorității contractante și ai Contractantului (cel puțin expertul cheie desemnat ca responsabil de contract). În cadrul acestei întâlniri se vor pune la dispoziția contractantului datele de care dispune Autoritatea contractantă necesare prestării serviciilor.
Responsabilă de organizarea întâlnirii este Autoritatea contractantă.
În cadrul acestei întâlniri vor fi stabilite următoarele:
(a) principiile de comunicare reciprocă;
(b) planul de lucru;
(c) detaliile privind colaborarea;
(d) frecvența reuniunilor;
(e) modelele de procese-verbale;
(f) modelele de rapoarte privind progresele înregistrate;
(g) planurile de acțiune în cazul apariției unor probleme;
(h) alte detalii logistice și organizaționale.
La finalul reuniunii se va întocmi o minută, ce va cuprinde toate aspectele stabilite în această întâlnire.

Alte întâlniri / ședințe care ar putea fi desfășurate pe parcursul derulării contractului:
(a) **ședințe periodice de monitorizare și control al progresului** în cadrul contractului și evaluarea stadiului contractului, la un interval de o lună, pe perioada desfășurării contractului. Frecvența acestora poate fi modificată în funcție de situațiile specifice ce ar putea apărea;
(b) **întâlniri ad-hoc** de rezolvare a unor probleme specifice care pot fi stabilite /planificare într-un termen scurt, ceea ce înseamnă că trebuie să existe disponibilitatea contractantului în termen de 1 zi lucrătoare de la solicitare pentru întâlnirile online și 3 (trei) zile lucrătoare de la solicitare pentru întâlnirile în format fizic.

Rezultatele ședințelor vor fi documentate în minute de ședință întocmite de Contractant și validate de autoritatea contractantă. Ședințele se vor desfășura, în funcție de context, fie virtual (teleconferințe/videoconferințe) atunci când nu este necesară prezența fizică a Contractantului la fiecare întâlnire/ședință, fie fizic, prin prezența Contractantului la sediul autorității contractante.

Participarea reprezentanților Contractantului la ședințe / reuniuni / întâlniri nu va genera costuri suplimentare pentru Autoritatea contractantă, față de cele indicate în propunerea financiară.

13.1.2. Modalitatea de abordare a eventualelor cereri de schimbare / modificări nesubstanțiale

Contractantul are obligația de a informa Autoritatea contractantă permanent și în mod corect despre evoluția contractului. Pe baza informațiilor furnizate de Contractant și în baza analizei actorilor implicați în gestionarea proiectului, autoritatea contractantă poate decide modificarea/completarea anumitor detalii legate de implementarea Contractului, în situația în care acest lucru se impune.

Părțile contractante au dreptul, pe durata valabilității Contractului, de a conveni modificarea și/sau completarea clauzelor acestuia, fără organizarea unei noi proceduri de atribuire, cu acordul părților, fără a afecta caracterul general al contractului, în limitele dispozițiilor prevăzute de art. 221 și art. 222 din Legea nr. 98/2016.
Modificările nesubstanțiale sunt singurele modificări ale Contractului care pot fi făcute fără organizarea unei noi proceduri de atribuire.

Modificările contractuale nu trebuie să afecteze, în niciun caz și în niciun fel, rezultatul procedurii de atribuire, prin anularea sau diminuarea avantajului competitiv pe baza căruia Ofertantul a fost declarat câștigător în cadrul procedurii de atribuire.

Ofertantul va prezenta în cadrul propunerii tehnice modalitatea de tratare a schimbărilor în cadrul Contractului.

13.1.3. Opțiuni de suplimentare fără a se depăși valoarea maximă aprobată a proiectului

În baza prevederilor art. 221 alin. (1) lit. a), autoritatea contractantă își rezervă dreptul de a achiziționa cantități suplimentare de servicii/produse dacă sunt îndeplinite cumulativ condițiile enumerate mai jos:
a) autoritatea contractantă înregistrează economii la atribuirea contractului sau în etapa de implementare a proiectului;
b) se constată necesitatea unor cantități suplimentare de servicii/produse, în limita maximă a economiilor înregistrate;
c) cantitățile suplimentare de servicii/produse, vor fi a achiziționate la prețurile unitare din propunerea financiară detaliată.

În această ipoteză, autoritatea contractantă va notifica Contractorului intenția de a exercita această opțiune cu minimum 30 de zile înainte, urmând ca modificarea să se reflecte la nivel contractual prin încheierea unui act adițional.

13.2. RAPORTAREA ÎN CADRUL CONTRACTULUI

Contractantul este responsabil de elaborarea și transmiterea rapoartelor către Autoritatea Contractantă.

Anterior convocării oricărei recepții și, implicit anterior emiterii oricărei facturi, Contractantul va elabora **raportul de progres**, în care va preciza cel puțin:

a) detalii tehnice cu privire la activități derulate și rezultate obținute în termeni cantitativi și calitativi;
b) detalii financiare referitoare la toate cheltuielile efectuate, cu respectarea categoriilor de cheltuieli și a prețurilor unitare conform propunerii financiare;
c) detalii referitoare la măsurile întreprinse pentru prevenirea/evitarea conflictului de interese;
d) dificultățile întâmpinate în cursul implementării activităților și soluțiile propuse pentru a depăși respectivele dificultăți, dacă este cazul;
e) întârzieri înregistrate, dacă este cazul;
f) recomandări/propuneri de planificare a activităților pentru perioada următoare, dacă este cazul;
g) alte informații solicitate de către autoritatea contractantă/organismul intermediar.

Furnizorul va elabora **rapoarte trimestriale** prin care să prezinte evoluția activităților și întârzierile, dacă acestea sunt semnificative. Rapoartele trimestriale vor detalia:

a) progresele înregistrate;
b) activități aflate în derulare cu data estimativă a finalizării acestora și cu rezultatele anticipate;
c) dificultățile întâmpinate în cursul implementării proiectului și soluțiile propuse pentru a depăși respectivele dificultăți;
d) rezultatele realizate în cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente, și planificarea activităților pentru perioada următoare.

Furnizorul trebuie să consulte Achizitorul cu privire la oricare aspect/problemă care apare în procesul de implementare. Furnizorului i se poate cere să participe la întâlniri periodice, pentru a comunica problemele identificate și pentru a găsi soluții optime. De asemenea, acesta va lua toate măsurile pentru a comunica în timp util, toate problemele identificate, în vederea evitării riscurilor rezultate din activitatea prestată.

Achizitorul (prin echipa de management a proiectului condusă de Managerul de Proiect) va fi responsabil de monitorizarea activităților desfășurate de Furnizor, de punerea în aplicare a rezultatelor acestui contract și de monitorizarea activităților derulate.

Furnizorul va avea nevoie de aprobarea prealabilă a Achizitorului pentru livrabile, precum și pentru materialele elaborate în cadrul contractului.

Toate comunicatele/raportările și documentele vor fi transmise către Achizitor, care analizează activitatea Furnizorului și formulează eventuale recomandări în legătură cu implementarea contractului în vederea avizării/aprobării documentelor respective.

Transmiterea și aprobarea rapoartelor

Rapoartele trebuie transmise la datele de contact din Contract în atenția Managerului de Contract desemnat din partea Autorității contractante.

Variantele intermediare, de lucru, vor fi transmise Autorității Contractante în format electronic editabil.

Variantele finale vor fi transmise atât în format editabil, cât și în format .pdf semnate cu semnătură electronică, dar și format tipărit, semnate ograf.

Aprobarea rapoartelor se face de către Comisia de recepție desemnată de Autoritatea Contractantă.

13.3. EVALUAREA PERFORMANȚEI FURNIZORULUI

Pentru activitățile și rezultatele relevante pentru îndeplinirea obiectului contractului autoritatea contractantă definește nivelurile de performanță, prezentate în continuare.

Este important ca performanța să fie monitorizată în mod regulat atât de către Contractant, cât și de către Autoritatea contractantă, iar acțiunile corective să fie implementate în cazul în care rezultatele nu ating nivelul așteptat. În acest sens, Contractantul va ține evidența valorilor asociate indicatorilor de performanță și va include informații referitoare la nivelul de performanță înregistrat în toate rapoartele și documentele întocmite pentru realizarea întâlnirilor de pe durata derulării contractului, așa cum sunt acestea descrise în caietul de sarcini.

Autoritatea Contractantă utilizează indicatorii de performanță de mai jos:

13.3.1. Termenele de prestare

Indicator	Descrierea indicatorului
Categorie indicator	Tehnic - nivel de calitate
Denumire indicator de performanță	Termenele de predare a livrabilelor proiectului
Nivelul de performanță așteptat	Livrabil/rezultat final predat în termenul agreat
Formula de calcul	Se compară termenul efectiv de prestare cu termenul/termenele convenite contractual
Modalitatea de evaluare	**Calificativele vor fi acordate** după cum urmează: **Foarte satisfăcător (5 puncte)** - Livrabil/rezultat final predat în termenele convenite în contract. Nu au fost necesare modificări majore ale livrabilelor transmise de către Furnizor ca urmare a observațiilor formulate de Autoritatea Contractantă. **Satisfăcător (4 puncte)** - Livrabil/rezultat final predat imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului. Au fost necesare ajustări nemateriale ca urmare a observațiilor formulate de Autoritatea Contractantă pentru livrabilele transmise de către Furnizor. S-a răspuns în timp util și adecvat la toate observațiile adresate de Autoritatea Contractantă. Nu au existat solicitări majore ale Furnizorului pentru prelungirea termenelor din cauza lipsei de claritate sau a existentei neconcordantelor sau erorilor în livrabile.

	Acceptabil (3 puncte) - Livrabil/rezultat final predat după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Au fost necesare câteva ajustări/corecturi ca urmare a observațiilor formulate de Autoritatea Contractantă. Cu toate acestea observațiile au fost abordate adecvat. Nu au existat solicitări ale Furnizorului pentru prelungiri semnificative ale termenelor din cauza lipsei de claritate sau a existentei neconcordanțelor sau erorilor în livrabile. **Nesatisfăcător (2 puncte)** – Livrabil/rezultat final predat cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului pentru mai mult de 60 de zile. Conținutul livrabilului a fost semnificativ modificat și corectat de Furnizor ca urmare a observațiilor adresate de Autoritatea Contractantă ceea ce a condus la întârzieri ale activităților din calendarului general al proiectului (ex. proiectul nu a putut fi finalizat la timp). Implementarea a fost finalizata cu întârzieri majore din cauza lipsei de claritate sau a existentei neconcordantelor în livrabile. **Foarte nesatisfăcător (1 punct)** – Livrabil/rezultat final predat cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului pentru mai mult de 90 de zile. Conținutul livrabilului a fost modificat în totalitate și corectat de Furnizor ca urmare a observațiilor adresate de Autoritatea Contractantă ceea ce a condus la întârzieri ale activităților din calendarului general al proiectului (ex. proiectul nu a putut fi finalizat la timp). Implementarea a fost finalizata cu întârzieri majore din cauza lipsei de claritate sau a existentei neconcordantelor în livrabile.

13.3.2. Nivelul de calitate a livrabilelor

Indicator	Descrierea indicatorului
Categorie indicator	Tehnic - nivel de calitate
Denumire indicator de performanță	Nivelul de calitate a livrabilelor
Nivelul de performanță așteptat	Livrabilele includ îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini.
Formula de calcul	N/A
Modalitatea de evaluare	**Calificativele aferente livrabilelor vor fi acordate după o evaluare**, după cum urmează: **Foarte satisfăcător (5 puncte)** – Livrabilele includ îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini.

	Satisfăcător (4 puncte) – Livrabilele includ unele îmbunătățiri și nu includ neconformități/inexactități față de nivelul agreat. Au fost necesare doar ajustări minore. **Acceptabil (3 puncte)** – Livrabilele nu includ neconformități/inexactități față de nivelul agreat însă nu includ nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului. Nu au existat întârzieri semnificative ca urmare a efectuării eventualelor remedieri. **Nesatisfăcător (2 puncte)** – Livrabilele prezintă neconformități / inexactități față de nivelul agreat, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost remediate de către Contractant. **Foarte nesatisfăcător (1 punct)** – Livrabilele prezintă neconformități / inexactități majore față de nivelul agreat, iar aceste aspecte nu au putut fi corectate de către Contractant. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului.

În cazul în care calificativul obținut se încadrează în categoria nesatisfăcător sau foarte nesatisfăcător, autoritatea contractantă respinge recepția, Contractantul nefiind în drept să primească plată pentru serviciile prestate.
Performanța Furnizorului va fi evaluată pe baza livrabilelor contractului, luându-se în considerare caracterul corect și complet al livrabilelor aferente prestării serviciilor din cadrul contractului.
Furnizorul va ține evidența valorilor asociate indicatorilor de performanță și va include informații referitoare la nivelul de performanță înregistrat în toate rapoartele și documentele întocmite pentru realizarea întâlnirilor de pe durata derulării contractului, așa cum sunt acestea descrise în Caietul de sarcini.

14. RECEPȚIA PRODUSELOR ȘI SERVICIILOR

Recepția produselor și serviciilor se va realiza conform „Planului de lucru / Graficului de prestare" întocmit de ofertant conform prevederilor din prezentul document.

Recepția produselor și serviciilor se face în baza Procesului verbal de recepție întocmit Beneficiar, în urma transmiterii de către Contractant a rapoartelor.

Recepția livrabilelor trimise de către Contractant va consta în:
- identificarea produselor furnizate și a serviciilor prestate;
- verificarea respectării condițiilor de furnizare și prestare conform specificațiilor din caietul de sarcini;
- constatarea eventualelor neconcordanțe.

Acceptarea rezultatelor/livrabilelor obținute din derularea Contractului se finalizează prin semnarea, după caz, a proceselor-verbale de recepție parțială / finală.

Dreptul achizitorului de a verifica, dacă este necesar, de a respinge serviciile, nu va fi limitat sau amânat din cauza faptului că serviciile au fost verificate de Contractant.

Procesul verbal de recepție parțială atestă îndeplinirea parțială de către Contractor a obligațiilor prevăzute în Caietul de sarcini, respectiv faptul că produsele au fost furnizate, respectiv serviciile au fost prestate corespunzător. Documentul „proces verbal de recepție parțială" nu va fi emis dacă un serviciu a fost respins de către Autoritatea Contractantă și ulterior nu a mai fost acceptat/aprobat printr-un nou proces verbal de recepție.

Procesul verbal de recepție finală se emite de regulă în baza proceselor verbale de recepție parțială și reprezintă acordul final al Autorității contractante cu privire la întregul Contract.

Procesul verbal de recepție va include unul din următoarele rezultate:
- **admiterea** recepției cu sau fără obiecții;
- **suspendarea** recepției;
- **respingerea** recepției (dacă se constată vicii care nu pot fi remediate și care, prin natura lor, împiedică realizarea uneia sau a mai multor exigențe esențiale).

Autoritatea Contractantă, în urma recepției, va aproba rapoartele/livrabilele sau va prezenta observațiile sale în termen de maximum 10 zile lucrătoare de la primirea lor.

În cazul unor modificări, Contractantul are obligația de a răspunde pozitiv solicitărilor Autorității Contractante de modificare/completare a rapoartelor/livrabilelor, corespunzător cu observațiile Autorității Contractante, în termen de maximum 5 zile lucrătoare de la data primirii acestora. Autoritatea Contractantă, prin recepție, va proceda la aprobarea sau respingerea rapoartelor, după caz, în termen de 5 zile lucrătoare de la data primirii acestora în forma revizuită, termen care poate fi prelungit în funcție de situațiile specifice.

Comisia de recepție recomandă suspendarea recepției când:

a) se constată existența unor neconformități, neconcordanțe ori deficiențe care sunt de natură să afecteze calitatea serviciului conform scopului, dar care pot fi remediate;
b) se constată existența unor servicii realizate necorespunzător sau nefinalizate, care pot afecta cerințele fundamentale aplicabile, dar care pot fi remediate/finalizate;
c) se constată existența, în mod justificat, a unor suspiciuni rezonabile cu privire la calitatea serviciilor și este necesară realizarea unor verificări aprofundate pentru a le clarifica;
d) contractantul nu pune la dispoziția comisiei de recepție documentele prevăzute în contract și caietul de sarcini.

În cazul în care comisia de recepție decide suspendarea procesului de recepție, aceasta încheie un proces-verbal de suspendare a procesului de recepție în care consemnează decizia de suspendare, măsurile recomandate în scopul remedierii aspectelor constatate, precum și termenul de remediere, iar autoritatea contractantă comunică Contractantului decizia comisiei în maximum 3 zile lucrătoare de la luarea la cunoștință a procesului-verbal de suspendare a procesului de recepție, împreună cu un exemplar al acestuia.

Termenul de remediere acordat de comisia de recepție va fi stabilit în funcție de neconformitatea constatată, fiind cuprins între min. 1 (una) și max. 15 zile lucrătoare, calculate de la momentul aducerii la cunoștință a procesului-verbal de suspendare a procesului de recepție. În cazul în care Contractantul nu remediază aspectele constatate și nu adoptă măsurile recomandate în cadrul procesului-verbal de suspendare a procesului de recepție în termenul stabilit, comisia de recepție va decide respingerea recepției.

Pentru evaluarea livrabilelor/rezultatelor intermediare/finale Autoritatea Contractantă utilizează ca date de intrare informații din:
a) cerințele din Caietul de Sarcini;
b) informațiile furnizate în Propunerea tehnică;
c) contract;
d) documentele /rapoartele/ puse la dispoziție de Contractant;
e) orice alte evidențe considerate relevante pentru analiza livrabilelor/ rezultatelor intermediare/finale.

În cazul în care calificativul obținut se încadrează în categoria nesatisfăcător sau foarte nesatisfăcător, autoritatea contractantă respinge recepția, Contractantul nefiind în drept să primească plată pentru serviciile prestate.

14.1. RECEPȚIA PRODUSELOR

Dreptul Achizitorului de a inspecta, testa și, dacă este necesar, de a respinge produsele, nu va fi limitat sau amânat din cauza faptului că produsele au fost inspectate și testate de Contractant, anterior furnizării acestora la locația de livrare/instalare.

Transferul drepturilor de proprietate și/ sau folosința, și al oricăror drepturi conexe către Achizitor va avea loc de la data recepției calitative.

Recepția produselor se va efectua pe baza de proces verbal semnat de Contractant și Achizitor și va consta în recepție cantitativă, recepție calitativă respectiv proces verbal de punere in funcțiune după cum urmează:

A. **Recepția cantitativă** a produselor se va realiza după livrarea produselor în cantitatea solicitată la locația indicată de Achizitor și va consta în efectuarea următoarelor operațiuni:
- numărare bucată cu bucată a echipamentelor, componentelor și a accesoriilor acestora;
- verificarea aspectului exterior, a integrității fizice și a caracteristicilor constructive;
- verificarea existenței tuturor componentelor și accesoriilor;
- verificarea existenței documentelor de însoțire a mărfii (aviz de însoțire a mărfii/ aviz de expediție etc.);
- verificarea existenței documentației tehnice aferente fiecărui tip de echipament;
- verificarea existenței certificatelor de garanție
- verificarea existenței documentelor de licențiere pentru software-ul livrat;
- verificarea suporților optici/USB (sau alte tipuri de suporți care permit Autorității contractante arhivarea și păstrarea produselor achiziționate) pe care sunt inscripționate produsele software;
- întocmirea unui Proces verbal de recepție cantitativă (PVRcant.) între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus;
- Achizitorul își rezervă un termen de maxim 5 zile lucrătoare pentru realizarea recepției cantitative.

B. **Recepția calitativă** se va realiza după finalizarea activităților aferente și va consta în efectuarea următoarelor operațiuni:
- verificarea semnării procesului verbal de recepție cantitativă;
- verificarea instalării și electroalimentării echipamentelor livrate;
- verificarea configurării hardware-software a echipamentelor livrate;
- verificare conexiuni fizice în rack: etichetare, documentare și cosmetizare;
- verificarea funcționalităților de disponibilitate prin realizare teste de redundanță (alimentare, conectivitate, calcul/stocare, HA failover, replicare/restaurare date);
- verificarea conformității produselor livrate cu specificațiile tehnice din Caietul de sarcini și din Propunerea tehnică, prin efectuarea de inspecții și teste funcționale. Inspecțiile și testele funcționale din cadrul recepției vizează respectarea cerințelor Caietului de sarcini și a specificațiilor Producătorului (caracteristici tehnice, constructive, electrice, cerințele funcționale etc.);
- testările funcționale din cadrul recepției se vor efectua pe baza unui set de teste, teste care vor fi propuse de către contractant și agreate de Autoritatea contractantă;
- verificarea versiunii codurilor software instalate, a licențelor corespunzătoare acestora, astfel încât la finalizarea recepției calitative Autoritatea contractantă să se asigure că va deține toate documentele juridice privind licențele proprii sau cele din partea terților;
- verificarea Raportului de instalare.
- întocmirea unui Proces Verbal de Recepție Calitativă (PVRcal.) între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus;
- Achizitorul își rezervă un termen de maxim 5 zile lucrătoare pentru realizarea recepției calitative a produselor.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:
- acceptat;
- refuzat.

În cazul procesului verbal de recepție calitativă refuzat, Contractantul va analiza observațiile primite și va efectua modificările solicitate în termen maxim de 5 zile lucrătoare, după care se va relua procedura de recepție a acestora.

14.2. RECEPȚIA SERVICIILOR

Recepția serviciilor solicitate se va realiza conform fazelor definite în „Planul de lucru / Graficul de prestare". Fiecare fază sau etapă, după caz, se va finaliza cu întocmirea unui Proces verbal de recepție cantitativă și calitativă fază sau etapă, după caz, se va verifica existența, conformitatea și completitudinea livrabilelor aferente prestării serviciilor cu specificațiile contractuale și specificațiile tehnice minimale ale caietului de sarcini și ale ofertei câștigătoare.

Achizitorul va stabili dacă documentele/livrabilele sunt complete și respectă cerințele minime din documentele contractuale și condițiile/cerințele detaliate rezultate ca urmare a evaluărilor/analizelor efectuate de Achizitor.

Achizitorul are dreptul de a verifica modul de prestare a serviciilor pentru a stabili conformitatea cu prevederile documentelor contractuale și din cele rezultate ca urmare a evaluării, în termen de 5 (cinci) zile lucrătoare de la primirea livrabilelor.

Recepția livrabilelor se va realiza de către o comisie formată din reprezentanți ai Achizitorului.

În situația în care comisia de recepție constată că sunt îndeplinite cerințele solicitate prin documentele contractuale și din cele rezultate ca urmare a evaluărilor, se va întocmi proces-verbal de recepție cantitativă și calitativă, care va fi semnat de către membrii din comisia de recepție și de către reprezentanții Contractantului.

Contractantul are obligația de a depune livrabilele, în vederea recepției, înainte de termenul limită de prestare a fiecărei faze sau etape, după caz, astfel încât să includă perioada de verificare de către Achizitor (5 zile lucrătoare), precum și cea necesară remedierii eventualelor deficiențe (3 zile lucrătoare).

După semnarea de către membrii din comisia de recepție și de către reprezentanții Contractantului a proceselor-verbale de recepție cantitativă și calitativă, aferente tuturor fazelor definite în „Planul de livrare produse și prestări servicii", în termen de cel mult 5 zile lucrătoare de la semnarea ultimului proces verbal de recepție cantitativă și calitativă, se va întocmi un Proces verbal de recepție finală (PVRfin.) între reprezentanții părților, în care se va consemna obținerea tuturor rezultatelor contractului.

14.3. LIVRABILE PENTRU PRODUSELE FURNIZATE ȘI SERVICIILE PRESTATE

Principalele activități și livrabile ce trebuie avute în vedere de Contractant în cadrul acestui contract, dar fără a se limita la acestea, sunt:

Nr. livrabil	LIVRABILE (Servicii și Produse solicitate)	UM	CANT.
1	**ECHIPAMENTE TIC ŞI ALTE DISPOZITIVE AFERENTE**		

1.1	Platforma de interconectare – Switch Data Center	buc.	2
1.2	Sistem de calcul modular	buc.	1
1.3	Platforma unificată de securitate	buc.	2
1.4	Platforma de balansare a traficului de aplicatie	buc.	2
1.5	Rack echipat (inclusiv cu ups)	buc.	3
1.6	Scanner	buc.	330
2	**Servicii IT inclusiv achiziționarea și/sau dezvoltarea aplicațiilor software/licențelor necesare implementării proiectului, configurarea produselor software de bază**		
2.1	DMS	licențe	1
2.2	BPM	licențe	1
2.3	Portal	licențe	1
2.4	Gestiune si analiza a datelor	licențe	1
2.5	Componenta interoperabilitate	licențe	1
2.6	Componenta monitorizare performate app	licențe	1
2.7	ETL	licențe	1
2.8	Componenta de analiza avansata si statistica	licențe	1
2.9	Componenta pentru optimizarea resurselor	licențe	1
2.10	Service desk	licențe	1
2.11	Platforma de virtualizare	licențe	1
2.12	Componenta software pentru instruire	licențe	1
3	**SERVICII DE DEZVOLTARE ȘI IMPLEMENTARE**		
3.1	Servicii de dezvoltare	servicii / pachet	1
3.2	Servicii de instalare și configurare software de bază	servicii / pachet	1
4	**SERVICII DE INSTRUIRE / FORMARE PROFESIONALĂ SPECIFICĂ**		
4.1	Servicii de pregătire a personalului care va utiliza echipamentele şi aplicația / serviciul software (Training utilizatori)	servicii / pachet	1
4.2	Servicii de pregătire a personalului care va asigura administrarea şi mentenanța echipamentelor şi aplicației / serviciului software (Training administratori sistem)	servicii / pachet	1
5	**Servicii IT inclusiv achiziționarea și/sau dezvoltarea aplicațiilor software/licențelor necesare implementării proiectului, configurarea produselor, pentru asigurarea securității cibernetice a rețelei și sistemelor informatice dezvoltate**		
5.1	Componenta de administrare identității utilizatorilor	licențe	1
5.2	Componenta de monitorizare a evenimentelor de securitate	licențe	1
5.3	Componenta de monitorizare infrastructură	licențe	1
5.4	Componenta de mascare a datelor	licențe	1
5.5	Backup	licențe	1
5.6	Componenta de securizare acces privilegiat	licențe	1

14.4. FINALIZAREA SERVICIILOR ÎN CADRUL CONTRACTULUI

Autoritatea Contractantă va considera serviciile din cadrul Contractului finalizate în momentul în care:
a) toate cerințele cuprinse în Caietul de Sarcini au fost îndeplinite;
b) rezultatele/rapoartele au fost aprobate de Autoritatea Contractantă, pe baza cerințelor incluse în Contract;
c) procesul verbal de recepție finală a fost aprobat fără obiecțiuni de către Autoritatea Contractantă.

În cazul în care calificativul final obținut se încadrează în categoria nesatisfăcător sau foarte nesatisfăcător, autoritatea contractantă emite documentul constatator cu selectarea opțiunii de neîndeplinire a obligațiilor contractuale.

14.5. MONITORIZAREA REALIZĂRII ACTIVITĂȚILOR ȘI A REZULTATELOR PE PERIOADA DERULĂRII CONTRACTULUI

În sensul prezentului caiet de sarcini următorii termeni au sensul definit mai jos:
- monitorizarea este activitatea de colectare de date și informații cu privire la modul de implementare a activităților contractului, vizând atât aspecte cantitative, cât și calitative;
- controlul implică identificarea acțiunilor preventive și corective pentru abordarea abaterilor de la condițiile contractuale.

Ofertantul va include în Propunerea tehnică detalii referitoare la modul concret prin care acesta va asigura monitorizarea și controlul activităților și rezultatelor prevăzute de Contract.

Pentru monitorizarea activității Contractantului, autoritatea contractantă va avea în vedere următoarele aspecte:
a) Contractantul și-a îndeplinit atribuțiile, așa cum reies acestea din cadrul prezentului caiet de sarcini, iar rezultatele contractului au fost atinse;
b) Contractantul a respectat termenele de realizare a activităților contractului și a predat la timp livrabile;
c) Contractantul a respectat cerințele minime ale caietului de sarcini și asumate prin propunerea tehnică cu privire la forma și calitatea livrabilelor contractului;
d) Contractantul a respectat obligațiile contractuale prin raportare la termenii contractului de finanțare.

Monitorizarea se va realiza pe tot parcursul proiectului, iar controlul se va realiza cel puțin lunar.

Contractantul are obligația de a furniza date și informații corecte, complete și la timp pentru a facilita activitatea de monitorizare și control.

14.6. ASIGURAREA CALITĂȚII

Ofertantul trebuie să prezinte în cadrul propunerii tehnice o descriere a modului concret de asigurare și control al calității proceselor pe care le derulează în cadrul Contractului.

Ofertantul trebuie să aloce în planul detaliat de implementare timpi suficienți de verificare și validare din punct de vedere calitativ pentru serviciile prestate și pentru revizuirea livrabilelor/documentelor rezultate.

Contractantul va presta serviciile descrise în prezentul caiet de sarcini, asigurând un standard de calitate ridicat și va gestiona toate aspectele administrative și de organizare în vederea realizării serviciilor descrise în prezentul caiet de sarcini.

15. MODALITĂȚI ȘI CONDIȚII DE PLATĂ

Plățile în cadrul contractului se vor realiza pentru produsele efectiv livrate și pentru serviciile efectiv prestate, la prețurile unitare prevăzute în propunerea financiară detaliată a ofertantului declarat câștigător.

Plata se estimează a se efectua în tranșe corespunzătoare jaloanelor definite în „Graficul de prestare" al proiectului, realizat pe baza calendarului de implementare, astfel:

Tranșe de plată	Document recepție	Alte detalii
Plata nr. 1	Documentații / Rapoarte conform " *5.9.2. Serviciile de livrare, instalare și dezvoltare software*" Proces-verbal de recepție cantitativă și calitativă parțial	- după recepția serviciilor de analiză și de proiectare a sistemului – livrabilele nr.1 si nr.2 din sectiunea 5.9.2; - maxim 20% din valoarea cumulată a *liniilor 3.1 si 3.2 din secțiunea 14.3*
Plata nr. 2	Documentații / Rapoarte conform " *Serviciile de livrare, instalare echipamente hardware*" Proces-verbal de recepție cantitativă și calitativă parțial	- după recepția livrării integrale a produselor: ▪ echipamente TIC; ▪ licențe necesare implementării proiectului; ▪ licențe pentru asigurarea securității cibernetice a rețelei și sistemului informatic dezvoltat; - după recepția serviciilor de instalare și configurare software de bază
Plata nr. 3	Documentații / Rapoarte conform "*Lista minimă de documentații de livrat pentru dezvoltare software*" Proces-verbal de recepție cantitativă și calitativă final	Restul de plată: - după recepția serviciilor de dezvoltare, migrare date,testare și asigurarea calității sistemului - după recepția serviciilor de instruire (utilizatori și administratori de sistem); - după punerea în producție a sistemului

Contractantul va emite facturile în sistemul Ro-eFactura, potrivit prevederilor OUG nr. 120/2021, aprobată cu modificări prin Legea nr. 139/2022, pentru produsele livrate și acceptate.

Plățile se vor efectua în lei, prin virament în contul de trezorerie al Contractantului, într-un termen de maximum 30 de zile de la data înregistrării facturii fiscale de către Autoritatea contractantă însoțită de toate documentele justificative prevăzute în prezentul caiet de sarcini, în conformitate cu prevederile art. 6 alin. (1) lit. c) din Legea nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și autorități contractante.

Fiecare factură va avea menționat numărul contractului, codurile CPV, datele de emitere și de scadența ale facturii respective.

Fiecare factură emisă va purta mențiunea ”Proiect finanțat de .....” precum și numărul și data contractului de finanțare.

Fiecare factură va fi emisă după semnarea de către Autoritatea Contractantă a proceselor verbale de recepție calitativă și cantitativă parțiale/final, acceptate fără obiecțiuni. Procesele verbale de recepție calitativă și cantitativă vor însoți factura în mod obligatoriu și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute în prezentul caiet de sarcini.

16. CERINȚE GENERALE PREDARE CODURI SURSĂ

În conformitate cu prevederile art. 12 din Ordonanță de urgență nr. 41 din 28 iunie 2016 privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative, pentru modulele/componentele software dezvoltate, cu excepția produselor standard, este obligatoriu ca Contractantul să pună la dispoziția beneficiarului codul sursă al aplicației/aplicațiilor sau configurărilor/customizărilor efectuate împreună cu toată documentația aferentă astfel:

a. Toate codurile sursă vor fi predate de către Contractant beneficiarului pe serverul său, cu toate versionările;
b. Autoritatea contractantă împreună cu Contractantul va verifica daca codul sursă predat pe serverul său, coincide cu codul sursă deployat in producție;
c. Toate codurile sursă vor include și comentarii scrise în limba română şi în acord cu standardele/convențiile de dezvoltare a codului (în forma susținută de limbajul de programare aferent, de exemplu comentarii în interiorul codului);
d. Toate codurile sursă vor fi predate în clar, fără a se aplica procedee de ascundere (”obfuscate”);
e. Acceptarea predării codului sursă de către Contractant și preluării acestora de către beneficiar se va realiza doar după validarea acestora de către Autoritatea contractantă în infrastructură, la recepția sistemului informatic implementat.

Notă: codurile sursă dezvoltate /configurate vor deveni proprietatea Autorității contractante, cu drept de acces, modificare și punere la dispoziție și pentru terți. Toate componentele dezvoltate/ configurate trebuie ofertate cu drepturi perpetue de exploatare.

Codul sursă va fi furnizat cu respectarea următoarelor bune practici și standarde:

a) Indentarea liniilor de program în conformitate cu secvențialitatea modulelor de program, a funcțiilor, a procedurilor, a porțiunilor de declarări de variabile, a porțiunilor în care se execută comenzi de lucru cu bazele de date, etc.;
b) Comentarea liniilor de program care nu sugerează prin însuși conținutul lor, pentru un programator care ar încerca modificarea sau depanarea codului, funcționalitatea sau scopul dorit;
c) Comentarea obligatorie, explicită și detaliată, a fiecărui început de modul, funcție, procedura, porțiune de declarare de variabile, porțiune în care se execută comenzi de lucru cu bazele de date etc. Comentariul va conține detalii explicite despre parametrii de intrare, rezultatele așteptate ale modulului, funcției, etc.;
d) Se va ține cont de posibilitatea reutilizării codului în alte dezvoltări viitoare. Astfel, codul utilizat va fi optimizat pentru rularea rapidă, fără erori, va evita posibilitatea apariției pe anumite porțiuni a fenomenului de serializare, etc.;
e) De-a lungul întregului cod sursă se vor implementa submodule de interceptare a erorilor și a excepțiilor care vor realiza afișarea într-un mod explicit, "human readable", a cauzei care a generat eroarea sau excepția. Posibilele excepții care pot apărea din incompatibilitatea parametrilor cu valorile acceptate vor fi anticipate și tratate astfel încât end-userul nu va interacționa cu mesaje sistem de eroare sau cu crush-uri de aplicație și pierderi de date introduse. Submodulele de interceptare și tratare a erorilor și excepțiilor vor fi, de asemenea, comentate în detaliu, într-un mod explicit;
f) Sursele vor fi însoțite de o documentație detaliată, în special componentele care nu rezidă în mod explicit, în sistem, sub formă de fișiere (ex: comenzi de tip

scheduler, setări de sistem, indiferent că au fost introduse în fișiere ANSI sau prin interfețe GUI, setări și parametri de deployment pe application server, etc.);

g) Sistemul de prelucrare a informației, în mod exhaustiv, nu va conține puncte de single failover, erori de logică a fluxului de date și a prelucrării datelor, va fi construit folosindu-se elementele cele mai actuale de bune practici recomandate de documentațiile și manualele de bune practici ale produselor folosite;
h) Pe toata perioada desfășurării proiectului, Contractantul va realiza un transfer continuu și activ de cunoștințe către echipele tehnice și funcționale ale beneficiarilor, pentru ca acestea să poată prelua operarea, mentenanța si să poată realiza dezvoltări ulterioare ale sistemului creat, fără a depinde de serviciile Contractantului.

Pe tot parcursul Caietului de sarcini cod/codul sursă reprezintă set de instrucțiuni / fișiere care conțin instrucțiuni necompilate.

17. MODUL DE PREZENTARE A OFERTELOR TEHNICE

Toate specificațiile tehnice din prezentul Caiet de sarcini sunt obligatorii și minimale pentru toți ofertanții.

Propunerea tehnică, inclusiv documentele anexă (cu excepția documentațiilor tehnice ale producătorilor care sunt în limba engleză), în cazul în care sunt emise în altă limbă decât română, vor fi transmise în limba de origine, însoțite de o traducere autorizată a acestora în limba română. În cazul în care certificatele/diplomele/documentele care confirmă experiența profesională indicată sunt emise în altă limbă decât româna, acestea vor fi transmise în limba de origine, însoțite de o traducere autorizată a acestora în limba română.

Prin propunerea tehnică depusă, ofertantul are obligația de a face dovada conformității serviciilor și produselor care urmează a fi prestate și livrate cu cerințele prevăzute în caietul de sarcini.

Propunerea tehnică va fi prezentată într-o formă narativă, în care ofertanții vor include în ordine următoarele **capitole**:

1. Abordare și metodologie - Cerințele sunt detaliate în secțiunea ”ABORDAREA, METODOLOGIA ȘI PLANUL DE LUCRU ÎN CADRUL CONTRACTULUI” din prezentul caiet de sarcini;

2. **Descrierea arhitecturii soluției propuse**, suficient de detaliată astfel încât să se poată verifica îndeplinirea tuturor cerințelor privind arhitectura din caietul de sarcini;

3. **Denumirile echipamentelor ofertate**, menționând pentru fiecare produs următoarele informații:
   a. producătorul;
   b. denumirea comercială, tipul/versiunea produsului;
   c. configurațiile produselor ofertate detaliind toate subansamblele și accesoriile incluse, cu part-number-ele producătorilor;
   d. rolul și facilitățile funcționale relevante pentru scopul utilizării în cadrul soluției ofertate;

4. **Lista produselor software ofertate**, specificând în clar numele licenței de la producător, ediția, producătorul, cantitatea și unitățile de licențiere specifice producătorului precum „User” sau „Processor Core” precum și corelarea acestora cu cerințele caietului de sarcini.

Lista licențelor trebuie să cuprindă toate licențele propuse de ofertant. Toate componentele ofertate vor trebui să fie regăsite în oferta financiară și prezentate în oferta tehnică sub formă de tabel după cum urmează:

Nr. crt.	Denumire componentă (*)	Producător	Nume produs propus (**)	Cant.	UM	Modul de licențiere (***)

(*) Denumirea componentei conform Caietului de Sarcini.

(**) Denumirea completă dată de producător, inclusiv ediția (exemplu „Standard", „Enterprise", dacă este cazul). Se va insera câte un singur produs pe un rând.
(***) Va conține detalierea modului de licențiere al producătorului cu explicații privind modalitatea de îndeplinire a cerințelor caietului de sarcini.

5. **Lista mașinilor virtuale / containerelor necesare** pentru soluția propusă, având în vedere cerințele de înaltă disponibilitate și performanță a soluției solicitate, indicând pentru fiecare mașină virtuală/container: rolul acesteia, sistemul de operare necesar, software-ul instalat, numărul de nuclee de procesare necesar a fi alocat, memoria RAM necesar a fi alocată, storage necesar a fi alocat.

6. **Descrierea soluției tehnice propuse** pentru îndeplinirea obiectivelor stabilite prin caietul de sarcini. Pentru sistemele/ subsistemele/ componentele solicitate, ofertantul va include/descrie în mod obligatoriu în oferta tehnică și modalitatea de implementare a funcționalităților solicitate.

7. **PLANUL DE LUCRU PENTRU REALIZAREA SERVICIILOR**
Cerințele sunt detaliate în Capitolul "ABORDAREA, METODOLOGIA ȘI PLANUL DE LUCRU ÎN CADRUL CONTRACTULUI" din prezentul caiet de sarcini.

8. **PERSONALUL UTILIZAT PENTRU REALIZAREA SERVICIILOR ȘI ORGANIZAREA ACESTUIA**
Cerințele sunt detaliate în Capitolul "ABORDAREA, METODOLOGIA ȘI PLANUL DE LUCRU ÎN CADRUL CONTRACTULUI" din prezentul caiet de sarcini.

Propunerea tehnică narativă reprezintă documentul central al propunerii tehnice, toate documentele suport prezentate pentru demonstrarea îndeplinirii tuturor cerințelor trebuie să fie menționate în aceasta, atașate ca anexe.

În mod obligatoriu, Ofertanții vor numerota fiecare pagină a Propunerii tehnice narative. Nu se acceptă descrierea detaliată a modului în care este îndeplinită cerința prin copierea conținutului cerinței. Ofertele care în conținutul lor vor avea elemente de conținut copiat fără detalieri relevante din care să rezulte clar modul în care oferta respectivă îndeplinește acea cerință vor fi respinse ca neconforme în baza art. 137 alin (3) litera a din HG 395/2016. În această coloană nu se vor include poze, capturi de ecran sau referințe de tip URL. Ofertantul va prezenta răspunsuri detaliate la toate cerințele Caietului de Sarcini prin care să arate modul concret în care cerințele sunt îndeplinite.

Se vor menționa informații care asigură posibilitatea verificării facile a corespondenței cu cerințele, cum ar fi: trimiteri la documentațiile de produs atașate, la documente cu capturi de ecran, referințe URL sub formă de hyperlink la documentații publicate pe website-uri ale producătorilor.
În cazul trimiterilor la documentațiile de produs atașate se vor preciza numele documentului/fișierului și pagina/paginile unde se poate verifica informația.
În cazul capturilor de ecran, aceasta vor fi incluse într-un document separat și numerotate, astfel încât trimiterile la ele să indice numele documentului/fișierului și numărul figurii/figurilor. Este interzisă includerea de capturi de ecran în tabelul cu matricea de conformitate.

Documentația tehnică și documentele suport necesare pentru identificarea soluției ofertate se prezintă ca anexe la propunerea tehnică, structurat, pe tipuri de componente, respectând ordinea de prezentare a acestora din caietul de sarcini

În mod obligatoriu, Ofertanții vor numerota fiecare pagină.

Lipsa din ofertă a oricăror informații dintre cele solicitate în acest capitol sau prezentarea unor descrieri nerelevante sau care nu demonstrează îndeplinirea fiecărei cerințe, poate conduce la declararea ofertei ca fiind neconformă și, implicit, la descalificarea Ofertantului.

Toate produsele ofertate vor fi prezentate cantitativ în Propunerea tehnică și cantitativ-valoric în Propunerea financiară, specificându-se prețul unitar al fiecărui produs ofertat. Prețul produselor va include garanția și/sau suportul tehnic solicitat.

Prețul serviciilor va fi detaliat pentru fiecare fază/etapă.

În cazul constatării unor neconcordanțe, specificațiile oficiale ale Producătorului produsului (valabile la data limită de depunere a ofertelor) vor fi considerate ca referință, conținutul acestora primând asupra specificațiilor tehnice prezentate de ofertant.

În conformitate cu prevederile art.123 alin.(1) din HG nr. 395/2016, fiecare ofertant va indica, motivat, în propunerea tehnică depusă informațiile care sunt confidențiale, clasificate sau sunt protejate de un drept de proprietate intelectuală, în baza legislației aplicabile.

18. CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT

Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Contractantul trebuie să respecte toate prevederile legale, aplicabile la nivel național, dar și regulamentele aplicabile la nivelul Uniunii Europene (acolo unde se impune).

Pe perioada realizării tuturor activităților din cadrul Contractului, Contractantul este responsabil pentru implementarea celor mai bune practici, în conformitate cu legislația și regulamentele existente la nivel național și la nivelul Uniunii Europene. Contractantul va fi ținut deplin responsabil pentru subcontractanții săi în prestarea serviciilor prevăzute în Caietul de Sarcini, urmând să răspundă față de Autoritatea Contractantă, pentru orice nerespectare sau omisiune a respectării oricăror prevederi legale și normative aplicabile.
Autoritatea Contractantă nu va fi ținută responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant sau de către subcontractanții acestuia a oricărei prevederi legale sau a oricărui act normativ aplicabil precum și atât pentru prestarea serviciilor cât și pentru rezultatele generate de prestarea serviciilor.

În cazul în care intervin schimbări legislative, Contractantul are obligația de a informa Autoritatea Contractantă cu privire la consecințele asupra activităților care fac obiectul Contractului și de a-și adapta activitatea în funcție de decizia Autorității Contractante în legătură cu schimbările legislative. În cazul în care o astfel de situație este aplicabilă trebuie precizat în Contract mecanismul de soluționare a unor astfel de situații.

Ofertantul devenit Contractant are obligația de a respecta in executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

- Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
- Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
- Convenția nr. 29 a OIM privind munca forțată;
- Convenția nr. 105 a OIM privind abolirea muncii forțate;
- Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
- Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
- Convenția nr. 100 a OIM privind egalitatea remunerației;
- Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;
- Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;
- Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);
- Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);
- Convenția de la Rotterdam privind procedura de consimțământ prealabil în cunoștință de cauză, aplicabilă anumitor produși chimici periculoși și pesticide

care fac obiectul comerțului internațional (UNEP/FAO) (Convenția PIC), 10 septembrie 1998, și cele trei protocoale regionale ale sale.

Ofertantul va prezenta o declarație pe proprie răspundere, privind faptul ca la elaborarea ofertei a ținut cont de obligațiile relevante din domeniile mediului, social și al relațiilor de muncă pe toată durata de îndeplinire a contractului de servicii, în conformitate cu prevederile art. 51 din Legea nr.98/2016 privind achizițiile publice.
Actele normative și standardele indicate mai jos sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă.

Instituțiile competente de la care operatorii economici pot obține informațiile detaliate privind obligațiile relevante din domeniile mediului, social și al relațiilor de muncă sunt Ministerul Mediului și Ministerul Muncii, Familiei, Protecției Sociale și Persoanelor Varsnice și de la Inspectoratele Teritoriale de Munca, respectiv și - site-ul: http://www.anpm.ro/web/guest/legislatie; http://www.inspectmun.ro/legislatie/ legislatie.html.

18.1. LEGISLAȚIE EUROPEANĂ

- Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012;
- Regulamentul (UE) nr. 241/2021 al Parlamentului European și al Consiliului din 12 februarie 2021 de instituire a Mecanismului de redresare și reziliență;
- Regulamentul Delegat (UE) 2021/2106 al Comisiei din 28 septembrie 2021 de completare a Regulamentului (UE) 2021/241 al Parlamentului European și al Consiliului de instituire a Mecanismului de redresare și reziliență prin stabilirea indicatorilor comuni și a elementelor detaliate ale tabloului de bord privind redresarea și reziliența;
- Decizia de punere în aplicare a Consiliului de aprobare a evaluării planului de redresare și reziliență al României din 29 octombrie 2021;
- Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană;
- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

18.2. LEGISLAȚIE NAȚIONALĂ

- Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;
- Normele metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică /acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, aprobate prin HG nr. 395/2016, cu modificările și completările ulterioare;
- Legea nr. 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică, a contractelor sectoriale și a contractelor de

concesiune de lucrări și concesiune de servicii, precum și pentru organizarea și funcționarea Consiliului Național de Soluționare a Contestațiilor, cu modificările și completările ulterioare;
- Legea nr. 190/2018 privind masurile de aplicare a GDPR.

18.3. CONFLICT DE INTERESE

Se aplică prevederile art. 61 alin. (1) din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 și legislația națională în vigoare cu privire la conflictul de interese.

Pentru a se asigura independența Ofertantului, acesta va confirma prin completarea în DUAE Partea III lit.C), neîncadrarea în situațiile potențial generatoare de conflict de interese și va informa Autoritatea Contractantă în cazul în care se va afla la un moment dat pe parcursul implementării contractului în situația de conflict de interese, chiar potențial, în timpul îndeplinirii sarcinilor pentru care a fost contractat.

18.4. CONFIDENȚIALITATE

Atât contractantul, cât și personalul pus la dispoziție de acesta trebuie să păstreze confidențialitatea informațiilor și datelor la care au acces pe parcursul implementării contractului.

Contractantul va pune la dispoziția Autorității Contractante lista completă a personalului său (inclusiv cel care aparține asociaților și subcontractanților, dacă este cazul) care va fi implicat în derularea contractului și prestarea serviciilor și care vor necesita acces în locațiile de instalare şi acces la informații despre acestea.

Datorită caracterului confidențial al informațiilor la care persoanele nominalizate vor avea acces, Autoritatea Contractanta își rezervă dreptul de a verifica personalul respectiv, conform normelor sale interne privind accesul la date şi informații cu caracter confidențial și de a interzice accesul în amplasamente sau la informații legate de contract acelor persoane care nu îndeplinesc condițiile impuse de Autoritatea Contractantă.

Atât contractantul, cât și personalul pus la dispoziție de acesta trebuie să păstreze confidențialitatea tuturor informațiilor și datelor la care au acces pe parcursul implementării contractului.

În etapa de implementare a Contractului, pentru fiecare persoană nominalizată în echipă ca expert, se va prezenta declarația de confidențialitate, semnată de către persoana respectivă (olograf sau semnată cu semnătură electronică extinsă bazat pe un certificat calificat, valabil, eliberat de un furnizor de servicii de certificare acreditat în condițiile legii), din care se rezulte că persoana respectivă:
- va păstra confidențialitatea în legătură cu faptele, informațiile sau documentele de care ia la cunoștință pe perioada derulării Contractului;
- nu va face cunoscut Contractul sau orice prevedere a acestuia unei terțe părți, în afara persoanelor implicate în îndeplinirea Contractului;
- se angajează ca dezvăluirea oricărei informații față de persoanele implicate în îndeplinirea Contractului să se facă în mod confidențial și să se extindă doar asupra acelor informații necesare în vederea îndeplinirii Contractului;

- se angajează să ia toate măsurile necesare pentru a asigura ca toate informațiile confidențiale sunt tratate ca și confidențiale și că nu sunt divulgate sau folosite în alte scopuri decât în relație strictă cu Contractul.

18.5. DREPTURI DE PROPRIETATE INTELECTUALĂ

Toate documentele ce vor fi elaborate în executarea Contractului (livrabile, rapoarte, clauze contractuale, etc.) vor face obiectul dreptului exclusiv de proprietate (inclusiv, dar fără a se limita la drepturi de autor și/sau orice alte drepturi de proprietate intelectuală) al Autorității Contractante, care le poate utiliza, publica sau transfera după cum consideră necesar, fără nicio limitare geografică sau de alta natură.

Orice documente (livrabile, studii, analize, rapoarte, planuri, proceduri, metodologii, diagrame, descrieri, materiale de instruire dacă este cazul, alte materiale) elaborate, obținute, rezultate, compilate de către Contractant sau de către personalul său salariat ori contractat în implementarea contractului, orice rezultate (inclusiv cod sursă), orice drepturi, inclusiv drepturi de autor sau alte drepturi de proprietate intelectuală ori industrială, dobândite în implementarea contractului, vor trece în proprietatea exclusivă a Autorității Contractante la momentul semnării fără obiecții a procesului verbal de recepție cantitativă și calitativă final aferent contractului, iar Autoritatea Contractantă le va putea utiliza, publica, cesiona ori transfera așa cum va considera de cuviință, fără limitare geografică ori de altă natură, cu excepția situațiilor în care există deja asemenea drepturi de proprietate intelectuală ori industrială.

Drepturile patrimoniale de autor asupra soluțiilor tehnice dezvoltate/create de Contractant în cadrul contractului, se transferă către Autoritatea Contractantă, conform art.12 alin.(1) din Ordonanța de urgență nr. 41/2016, privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea unor acte normative: „*Instituțiile publice și organele de specialitate ale administrației publice centrale, au obligația de a prevedea explicit în caietele de sarcini și în contractele aferente procedurilor de achiziție publică demarate de la data intrării în vigoare a prezentei ordonanțe de urgență, care includ dezvoltări de programe informatice la solicitarea instituției sau autorității, faptul că toate drepturile patrimoniale de autor asupra operelor create de către contractant sau membrii asocierii, aferente produsului sau serviciului livrat, se transferă către autoritatea contractantă*”.

După încetarea contractului, Contractantul nu va păstra copii ale documentelor elaborate, obținute, rezultate, compilate de către Contractant sau de către personalul său salariat ori contractat în implementarea contractului și nu le va utiliza în scopuri care nu au legătură cu respectivul contract fără acordul scris prealabil al Autorității Contractante.

Cu excepția informațiilor publice, Contractantul nu va publica articole sau informații referitoare la obiectul contractului, nu va face referire la acestea către terți și nu va divulga informațiile obținute de la Autoritatea Contractantă, fără acordul scris al acesteia.

Contractantul are obligația de a ceda în favoarea Autorității Contractante drepturile de autor/ drepturile de proprietate ce decurg din executarea contractului, cu respectarea prevederilor Ordonanței de Urgență a Guvernului nr. 89/2022.

Pentru soluțiile și funcționalitățile ofertate dar care nu au fost dezvoltate/ create special pentru Autoritatea Contractantă în cadrul contractului, în situația în care

cedarea drepturilor de proprietate nu este posibilă, Contractantul va asigura drepturile de utilizare permanentă a acestora de către Autoritatea Contractantă.

Toate informațiile vehiculate în legătură cu implementarea contractului sunt proprietatea Autorității contractante, aceasta fiind singura îndreptățită să le utilizeze în mod legitim, sau să confere drept de acces la datele în cauză terților în condiții stipulate în mod expres.

19. INFORMAȚII SUPLIMENTARE / ADMINISTRATIVE

Limba de lucru: română.

Ofertantul își asumă răspunderea exclusivă pentru legalitatea și autenticitatea tuturor documentelor prezentate în original, copie și/sau copie „conformă cu originalul" în vederea participării la procedură. În acest scop, analizarea de către comisia de evaluare a documentelor prezentate de ofertanți nu angajează din partea acesteia nicio răspundere sau obligație fată de acceptarea respectivelor documente ca fiind autentice sau legale și nu înlătură răspunderea exclusivă a ofertantului sub acest aspect. În acest sens, operatorii economici care, fie nu prezintă sau prezintă informații parțiale cu privire la propria lor situație privind incidența motivelor de excludere sau îndeplinirea cerințelor minime / criteriilor de calificare sau care se fac vinovați de declarații false în conținutul informațiilor transmise la solicitarea autorității contractante vor fi respinși, cu aplicarea în mod corespunzător a dispozițiilor / consecințelor legale incidente.

Autoritatea contractantă nu este responsabilă pentru nici un fel de cheltuieli suplimentare față de serviciile incluse în contract. Toate cheltuielile generate de încălcările și/sau nerespectările prevederilor de mai sus vor fi suportate de către Contractant și nu vor fi decontate de autoritatea contractantă.

Ofertantul suportă toate cheltuielile datorate elaborării și prezentării ofertei sale.

Toate documentele / informațiile folosite / prelucrate pe parcursul derulării contractului vor fi puse la dispoziția autorității contractante, în format electronic și editabil.

Pentru a demonstra o foarte bună înțelegere a caietului de sarcini, propunerea tehnică, metodologia și planul de lucru trebuie să fie adaptate cerințelor specifice ale caietului de sarcini, trebuie să fie prezentate și dezvoltate într-o manieră proprie și originală, **nefiind permise abordările de tip copy-paste**. Fiecare cerință va fi prezentată detaliat, la modul cum urmează a fi implementată, **nefiind permise abordările de răspuns doar cu "DA" sau "NU", sau prin copierea ad-literam** a cerinței impuse.

Nu se acceptă trimitere către link-uri, ci doar documente atașate ofertei, dacă este cazul.

Neregăsirea în propunerea tehnică a cerințelor minime din caietul de sarcini, va presupune declararea ofertei ca fiind neconformă. Propunerea tehnică va fi astfel prezentată încât să asigure posibilitatea verificării conformității acesteia cu cerințele minime obligatorii prevăzute în caietul de sarcini.

Documentele ofertei vor fi semnate de o persoană sau persoane autorizate de drept să semneze în numele Ofertantului și vor fi **prezentate atât in format .pdf (semnate cu semnătură electronică), cât și, în mod OBLIGATORIU, ÎN FORMAT EDITABIL WORD (.doc) sau EXCEL (.xls)**. O ofertă care va fi prezentată în orice alt format sau nu va fi transmisă conform cerințelor de mai sus (în format .pdf semnată electronic și în format editabil), va fi respinsă ca fiind inacceptabilă.

Paginile Ofertei vor fi numerotate, organizate pe diferite secțiuni ținând cont de fiecare categorie de cerințe din caietul de sarcini; oferta va include un **OPIS** care să

poată face trimitere la fiecare secțiune (indicând pagina și/sau paragraful), toate paginile fiind numerotate corespunzător, pentru a permite o identificare rapidă, conform cerințelor din caietul de sarcini.

Traian Ionică CRAINIC
Director Direcţia IT-LPIS

Florentin CONSTANTIN
Șef Serviciu DMPSI, DIT-LPIS

Valeriu Popescu
Șef Serviciu,SDPSIIS DIT-LPIS

Cătălin Dumitru ZGONDEA
consilier DIT-LPIS

Cristian JURUBIȚĂ
consilier, DIT-LPIS

Timotei Micu
consilier DIT-LPIS

Eduard Scundeanu
consilier DIT-LPIS

Florentina Georgeta PISICĂ
consilier juridic, Direcția Juridică

Marius Pricop
consilier juridic, Direcția Juridică

Gina Prodan, sef Serviciul Relatii cu Publicul si Comunicare

Stefanita CONSTANTIN, consilier, Serviciul Relatii cu Publicul si Comunicare

Mihaela Oprea, consilier, Serviciul Relatii cu Publicul si Comunicare

Cristian Iortoman, consilier, Serviciul Relatii cu Publicul si Comunicare

Radu Croitoru, consilier, Serviciul Relatii cu Publicul si Comunicare

Daniela Molan, consilier, Control Administrativ și Autorizare Plăți

Bogdan Cârstocea, consilier, Direcţia Antifraudă, Control Intern

Melinda Klara Kerekes
Director Direcţia Economică

Sabina Ionela DARIE
Sef serviciu Contabilitate UE - Direcţia Economică;

Carmen Madalina Constantin
Sef birou Raportare UE - Direcţia Economică

Dorina -Ruxandra Stancu
Sef serviciu Buget Finante si Fonduri Europene - Direcţia Economică;

Marius Săceanu
Sef Serviciu Recuperare Debite- Direcţia Economică

Lucian Ichim
Sef serviciu Plăţi UE- Direcţia Economică

Alice Iorgulescu, consilier Direcţia Măsuri de Piaţă, Comerţ Exterior

Adriana Mirela Darjanschi, consilier, Directia Management Resurse Umane

Cristina Georgeta SĂNDULESCU
consilier, Directia Management Resurse Umane

Oana STAVARACHI
consilier, Directia Management Resurse Umane

Cristina Brasoveanu, consilier Direcţia Măsuri de Piaţă, Comerţ Exterior

Simona Vasile
Direcția Intervenții IACS – Sector Vegetal și Condiționalitate

Mogaru Diana, consilier, Direcţia Control pe Teren

Sima Cristina, consilier, Direcţia Control pe Teren

Manuela Perianu, consilier, Direcţia Plăţi Directe – Sector Zootehnic

Adela Ionescu, consilier, Direcţia Plăţi Directe – Sector Zootehnic