



Finanțat de
Uniunea Europeană



"Platforma Națională de Interoperabilitate - PNI" ", Cod MySMIS: 333977

NR. 13PNI/06.02.2026

Aprob,
PREȘEDINTE,
Dragoș-Cristian VLAD

Vlad Dragos-Cristian
2026.02.06 19:22:36
+02'00'



Avizat,
SECRETAR GENERAL,
Dragoș-Cosmin NICULESCU

Niculescu Dragos-
Cosmin

Digitally signed by Niculescu
Dragos-Cosmin
Date: 2026.02.06 18:41:53 +02'00'

CAIET DE SARCINI pentru achiziția de SERVICII DE DEZVOLTARE PLATFORMĂ SOFTWARE

în cadrul proiectului:
„Platforma națională de interoperabilitate - PNI”

CPV principal

72262000-9 - Servicii de dezvoltare software (Rev. 2)

CPV-uri secundare

32412000-4 Rețea de comunicații, 48000000-8

Pachete software și sisteme informatice

48820000-2 Servere

32428000-9 Extensie de rețea

32570000-9 Echipamente de comunicații



AUTORITATEA
PENTRU
DIGITALIZAREA
ROMÂNIEI

Proiect co-finanțat din Fondul European de Dezvoltare Regională prin Programul Creștere Inteligentă, Digitalizare și Instrumente
Financiare 2021-2027 (PoCIDIF)

www.mfe.gov.ro



1.	INTRODUCERE 4	
2.	CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII	5
2.1.	Informații despre autoritatea contractantă	6
2.2.	Informații despre contextul care a determinat achiziționarea serviciilor.....	6
2.3.	Descrierea proiectului în cadrul căruia se realizează achiziția	7
2.4.	Obiectivul general al proiectului	8
2.5.	Obiectivul general la care contribuie prestarea serviciilor	8
2.6.	Obiectivele specifice ale proiectului	8
2.7.	Obiectivele specifice la care contribuie prestarea serviciilor	10
2.8.	Informații despre beneficiile anticipate de către autoritatea contractantă	10
2.9.	Alte inițiative/proiecte/programe asociate cu această achiziție	11
2.10.	Factori interesați și rolul acestora	11
3.	SERVICIILE ȘI PRODUSELE SOLICITATE	12
3.1.	CERINȚELE FUNCȚIONALE ALE SISTEMULUI	12
3.2.	ARHITECTURA FUNCȚIONALĂ A SISTEMULUI.....	18
3.3.	MANAGEMENTUL UTILIZATORILOR ȘI ACCESUL LA SISTEM	19
3.4.	SECURITATEA SISTEMULUI	20
3.5.	CONFIDENȚIALITATEA DATELOR	23
3.6.	ARHITECTURA TEHNICĂ.....	24
3.7.	COMPONENTELE HARDWARE ȘI DE COMUNICAȚII	27
3.8.	COMPONENTELE SOFTWARE	52
3.9.	SERVICII.....	106
4.	RESURSE	117
4.1.	Experți cheie	119
4.2.	Experți non-cheie	127
4.3.	Resurse materiale	131
5.	GARANȚIE ȘI SUSTENABILITATE	132
5.1.	Garanția sistemului.....	132
5.2.	Sustenabilitate	135
6.	LOCUL ȘI DURATA CONTRACTULUI	136
6.1.	Locul desfășurării activităților	136
6.2.	Durata prestării serviciilor.....	137
6.3.	Opțiuni de suplimentare	138
7.	IPOTEZE ȘI RISCURI. MĂSURI DE GESTIONARE A RISCURILOR.....	139
7.1.	Ipoteze	139
7.2.	Riscuri	139
8.	ATRIBUȚIILE ȘI RESPONSABILITĂȚILE PĂRȚILOR	141
8.1.	Obligațiile principale ale Contractantului	141
8.2.	Obligațiile principale ale Autorității Contractante	142
9.	DOCUMENTE CE TREBUIE FURNIZATE AUTORITĂȚII CONTRACTANTE	143





10. PROCEDURA DE ACCEPTANȚĂ	144
11. MANAGEMENTUL CONTRACTULUI ȘI ACTIVITĂȚI DE RAPORTARE	145
11.1. METODOLOGIA.....	148
11.2. PLANUL DE LUCRU (DE IMPLEMENTARE).....	148
11.3. ORGANIZAREA ȘI PERSONALUL	149
11.4. GESTIONAREA RELAȚIEI DINTRE CONTRACTANT ȘI AUTORITATEA CONTRACTANTĂ	149
11.5. RAPORTARE	152
12. MODALITĂȚI SI CONDIȚII DE PLATĂ.....	160
13. CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT (INCLUSIV ÎN DOMENIILE MEDIULUI, SOCIAL ȘI AL RELAȚIILOR DE MUNCĂ).....	160
13.1. Legislație europeană.....	162
13.2. Legislație națională	162
13.3. Conflict de interese	163
13.4. Confidențialitate.....	163
13.5. Drepturi de proprietate intelectuală	164
14. INFORMAȚII SUPLIMENTARE / ADMINISTRATIVE	165





1. INTRODUCERE

Caietul de Sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora fiecare ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru realizarea serviciilor care fac obiectul Contractului ce rezultă din această procedură.

În cadrul acestei proceduri, **Autoritatea pentru Digitalizarea României** (denumită în continuare **ADR**) îndeplinește rolul de autoritate contractantă.

În prezentul Caiet de Sarcini, operatorii economici potențial interesați de procedură sunt denumiți **ofertanți**, iar operatorii economici declarați câștigători sunt denumiți **contractanți**.

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.

Ofertele care nu îndeplinesc toate cerințele minimale vor fi declarate neconforme. Nu se acceptă depunerea de oferte alternative. Nu se admit ofertele parțiale din punct de vedere cantitativ și calitativ, ci numai ofertele integrale, care corespund tuturor cerințelor stabilite prin prezentul Caiet de sarcini. Orice ofertă care se abate de la cerințele minimale va fi considerată admisibilă numai în condițiile în care aceasta asigură un nivel calitativ superior cerințelor minimale.

În conformitate cu regulile de elaborare a documentației de atribuire din Legea nr. 98/2016, privind achizițiile publice, cu modificările și completările ulterioare (denumită în continuare Legea nr. 98/2016) art. 156 alin (2) și (3) specificațiile tehnice din prezentul Caiet de Sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate și care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică se consideră a fi însoțite de cuvintele „sau echivalent”, indiferent dacă aceste cuvinte sunt prevăzute expres sau nu în prezentul document.



2. CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII

ADR are rolul de a realiza și coordona implementarea strategiilor și a politicilor publice în domeniul transformării digitale și societății informaționale.

ADR funcționează în baza HG nr. 89/2020, cu modificările și completările ulterioare. În contextul importanței tot mai mari a tehnologiilor și a infrastructurilor digitale în viața noastră, misiunea ADR este esențială. Transformarea digitală vizează optimizarea modului de lucru și a procedurilor pentru o productivitate mai ridicată într-o organizație. Acest lucru se realizează prin adoptarea, cu celeritate și la toate nivelurile, a noilor tehnologii digitale.

Interoperabilitatea reprezintă capacitatea unor organizații distincte de a interacționa în scopul realizării unor obiective care aduc beneficii reciproce, sunt convenite mutual, și care implică partajarea de informații și cunoștințe, utilizând schimbul de date între respectivele sisteme informatice deținute de acestea.

Primul avantaj al interoperabilității sistemelor este costul mic, însă proiectarea, stabilirea, dezvoltarea, operarea și întreținerea acestora implică alegeri comune de standarde, de modele de schimb de informații, alegeri semantice comune. Pentru a facilita transferul de informații și date este obligatorie introducerea și adoptarea de standarde digitale coerente în cadrul diferitelor procese și proceduri. De asemenea, este necesară specificarea și documentarea detaliată a acestora. Mai mult, modelarea uniformă a datelor va permite trecerea de la partajarea datelor de tip nestructurat (.pdf, .jpg) la partajarea datelor de tip structurat în mesaj criptat.

Aplicată la sectorul public, interoperabilitatea optimă presupune un nivel ridicat, care permite un schimb de date mai eficient și mai sigur pentru a furniza servicii publice neîntrerupte. Un nivel scăzut de interoperabilitate face ca cetățenii și întreprinderile să se confrunte cu sarcini administrative inutile, iar administrațiile publice să aibă de suportat costuri mai mari.

Un schimb reușit între părțile interesate necesită luarea în considerare a diferitelor aspecte care pot fi definite ca „niveluri de interoperabilitate”, în acord cu Cadrul european și național de interoperabilitate.

Fiecărui nivel îi corespund standarde și principii la care părțile trebuie să se alinieze pentru a concepe și a efectua schimburi eficiente.

2.1. Informații despre autoritatea contractantă

AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI (ADR)

Sediul principal: Bd. Libertății nr 14, sector 5, București, România, cod poștal 050706

Sediul secundar: Str. Italiană nr 22, sector 2, București, România, cod poștal 020976 Cod

fiscal: R042283735

Telefon: 021 3052710

Fax: 021 3032899

Programul de lucru normal - L-J - 8.30-17.00 V-8.30-14.30

Autoritatea pentru Digitalizarea României, denumită în continuare ADR, se organizează și funcționează ca structură cu personalitate juridică în subordinea Ministerului Cercetării, Inovării și Digitalizării, având rolul de a realiza strategiile și politicile publice în domeniul transformării digitale și societății informaționale și de a coordona implementarea acestora, precum și rolul de a asigura monitorizarea și controlul asupra respectării reglementărilor interne și internaționale în domeniul transformării digitale și societății informaționale.

2.2. Informații despre contextul care a determinat achiziționarea serviciilor

În ceea ce privește cadrul de reglementare european, realizarea interoperabilității la nivelul UE se sprijină pe Regulamentul (UE) 2024/903 al Parlamentului European și al Consiliului din 13 martie 2024 de stabilire a unor măsuri pentru un nivel ridicat de interoperabilitate a sectorului public în întreaga Uniune (Regulamentul privind Europa interoperabilă).

Coordonatele esențiale în materie de interoperabilitate ale acestora sunt desprinse din Cadrul European de interoperabilitate (EIF), un set de recomandări care specifică modul în care administrațiile, întreprinderile și cetățenii comunică între și în cadrul Uniunii Europene, transfrontalier.

La nivel național, lipsa interoperabilității sistemelor informatice din administrația publică este un obstacol major în dezvoltarea serviciilor digitale centrate pe utilizatorul final. Sistemele existente sunt în general fragmentate, fiind proiectate și dezvoltate izolat de către diferite instituții ale statului, în afara unui cadru național integrat.

Uniunea și statele membre lucrează de peste două decenii pentru a sprijini modernizarea administrațiilor publice prin transformarea digitală și pentru a promova interconexiunile profunde necesare pentru un spațiu digital cu adevărat european. În comunicarea sa din 9 martie 2021 intitulată „Busola pentru dimensiunea digitală 2030: modelul european pentru deceniul digital”, Comisia subliniază necesitatea de a se accelera digitalizarea serviciilor publice până în 2030, inclusiv prin asigurarea interoperabilității la toate nivelurile administrației și în toate serviciile publice. În plus, Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului (4) stabilește un obiectiv clar ca 100 % din serviciile publice esențiale să fie furnizate online până în 2030. Prin regulamentul menționat este încurajată

crearea unei comunități dinamice în jurul soluțiilor tehnologice deschise pentru administrație.

Interoperabilitatea respecta dreptul fundamental la protecția datelor cu caracter personal este protejat în special prin Regulamentele (UE) 2016/679 (7) și (UE) 2018/1725 (8) ale Parlamentului European și ale Consiliului. Directiva 2002/58/CE a Parlamentului European și a Consiliului (9) protejează, de asemenea, viața privată și confidențialitatea comunicațiilor, inclusiv prin condiții prevăzute pentru orice stocare de date cu și fără caracter personal în echipamentele terminale și pentru orice acces la acestea. Respectivele acte legislative ale Uniunii asigură temeiul prelucrării durabile și responsabile a datelor, inclusiv atunci când seturile de date conțin un amestec de date cu caracter personal și de date fără caracter personal. Prezentul regulament completează dreptul Uniunii privind protecția datelor cu caracter personal și a vieții private, în special Regulamentul (UE) 2016/679, Regulamentul (UE) 2018/1725 și Directiva 2002/58/CE, fără a le aduce atingere. Nicio dispoziție regulamentelor prezentate nu ar trebui să fie aplicată sau interpretată în sensul diminuării sau limitării dreptului la protecția datelor cu caracter personal sau a dreptului la viață privată și la confidențialitatea comunicațiilor.

În ceea ce privește implementarea Regulamentului privind identitatea digitală, sistemul de autentificare național (denumit în continuare „ROeID”) este aliniat cu cerințele nivelurilor de asigurare eIDAS definite în Regulamentul de punere în aplicare (UE) 2015/1502 al Comisiei în temeiul articolului 8 alineatul (3) din Regulamentul (UE) nr. 910/2014 al eIDAS, îndeplinind cerințele pentru nivelul de asigurare „Substantial”.

În dezideratul atingerii jaloanelor asumate prin Planul Național de Redresare și Reziliență (PNRR), Componenta C7 - Transformare digitală și în vederea dezvoltării arhitecturii integrate a infrastructurii serviciilor digitale, a fost adoptată Legea privind schimbul de date între sisteme informatice și crearea platformei naționale de interoperabilitate. Această lege garantează principiul „doar o singură dată” și direcționarea serviciilor publice disparate și sinuoase în jurul utilizatorului final.

Actul normativ instituie Platforma Națională de Interoperabilitate necesară în vederea asigurării interoperabilității sistemelor informatice publice pentru furnizarea serviciilor publice, precum și accesarea informațiilor de către persoane juridice de drept privat sau persoanele fizice care exercită profesii libere reglementate, iar ADR este desemnată ca unic administrator al platformei naționale de interoperabilitate.

2.3. Descrierea proiectului în cadrul căruia se realizează achiziția

Autoritatea pentru Digitalizarea României a demarat în data de 23.07.2025 implementarea proiectului „Platforma Națională de Interoperabilitate”, cod SMIS 333977, finanțat prin Programul Creștere Inteligentă, Digitalizare și Instrumente Financiare 2021-2027 (PCIDIF),

Măsura 1: Servicii publice destinate cetățenilor și/sau firmelor identificate în CSP gestionat de ADR și/sau în concordanță cu Politica eGuv, Acțiunea 2.2 E-guvernarea și digitalizarea în beneficiul cetățenilor - 2.2.1: E-guv în administrația/instituțiile publice.

2.4. *Obiectivul general al proiectului*

Obiectivul general al proiectului constă în realizarea Platformei Naționale de Interoperabilitate, necesară în vederea asigurării interoperabilității sistemelor informatice publice pentru furnizarea serviciilor publice, precum și accesarea informațiilor de către persoane juridice de drept privat sau persoanele fizice care exercită profesii libere reglementate.

Platforma va asigura din punct de vedere tehnic crearea, operaționalizarea și administrarea instrumentului/mijlocului necesar pentru livrarea într-un format integrat a mai multor servicii electronice.

2.5. *Obiectivul general la care contribuie prestarea serviciilor*

Platforma Națională de Interoperabilitate (PNI) este necesară în vederea asigurării interoperabilității sistemelor informatice pentru furnizarea serviciilor publice, precum și pentru accesarea informațiilor de către persoane juridice de drept privat sau persoane care exercită profesii libere reglementate.

Se asigură, astfel, din punct de vedere tehnic, crearea, operaționalizarea și administrarea instrumentului/mijlocului necesar pentru livrarea într-un format integrat a mai multor servicii electronice.

PNI va implementa procesele tehnice stabilite prin Normele de referință pentru realizarea interoperabilității (NRRI) în domeniul tehnologiei informației și comunicațiilor, pentru asigurarea schimbului de date între sistemele informatice deținute de participanții la schimbul de date și pentru îmbunătățirea colaborării și a prestării comune a serviciilor publice.

2.6. *Obiectivele specifice ale proiectului*

Obiectivele specifice sunt:

- **Optimizarea operațiunilor guvernamentale prin interconectarea, consolidarea activelor IT și reutilizarea datelor.** Cetățenii vor beneficia de un guvern conectat și eficient. Instituțiile publice vor opera și vor interacționa printr-o platformă tehnologică comună pentru a oferi servicii de înaltă calitate. Cetățenii vor putea să ofere date cu

caracter personal guvernului o singură dată, iar instituțiile publice vor putea reutiliza aceste date pentru furnizarea de servicii.

- **Realizarea PNI**, care să ofere servicii de schimb de date care să permită schimbul de elemente justificative pentru procedurile online, prin aplicarea principiului “once-only”.
- Integrări cu sistemele informatice ale furnizorilor de registre de baza si ale instituțiilor publice care utilizeaza date din registrele de baza.
- Integrarea cu nodul EIDAS și proiectul PSCID/RoelD, care va furniza autentificarea digitală a cetățenilor români.
- Integrarea cu portalul Single Digital Gateway - proiectul PDURo.
- Integrari cu serviciile electronice din portalurile instituțiilor guvernamentale sectoriale (sistemele de tip hub de servicii - ex. MAI, MMJS, ONRC, ANAF, Ministerul Educatiei, MAE).
- Servicii publice integrate oferite cetățenilor și mediului de afaceri, precum și reducerea de sarcini administrative la accesarea serviciilor publice naționale.
- Cooperarea interinstituțională va ajuta la dezvoltarea practicilor organizaționale de gestionare a datelor în administrația publică, precum și a serviciilor tehnice de schimb de date.
- **Realizarea Registrului Național al Registrelor, denumit în continuare RNR.**

RNR reprezintă fundamentul organizării registrelor de bază, a datelor conținute de acestea și indică autenticitatea datelor conținute de aceste registre, instituțiile și autoritățile publice care au acces la aceste date, fundamentele legale pentru transmiterea datelor, descrierea proceselor colectării datelor, precum și modalitatea utilizării datelor colectate.

Catalogul Național Semantic (semantic.gov.ro) este o componenta a RNR destinat configurării, managementului și evidenței activelor semantice gestionate de entități, instituții din România, pentru a oferi informații actualizate despre activele semantice disponibile, dar și metadata relevante schimbului de date.

Catalogul Național Semantic este disponibil și poate fi accesat de către utilizatori prin intermediul *PNI*. Acesta conferă posibilitatea utilizatorilor de a identifica în mod clar tipurile de date și registre de bază corespunzătoare.

Realizarea acestor obiective va schimba modul în care sectorul public gestionează și utilizează tehnologia. Aplicarea unui cadru de investiții IT inteligent și colaborarea extinsă cu sectorul privat vor conduce la o abordare coordonată și coerentă în IT.

Reformele bazate pe IT vor elimina practicile ineficiente ale interacțiunii guvernamentale cu cetățenii și funcționarea internă. Procesele ineficiente și redundante vor fi restructurate pentru a reduce duplicarea resurselor și a eforturilor prin standardizarea proceselor și partajarea resurselor similare.

Pentru a reduce numărul de conexiuni de date, prin PNI autorităților li se oferă un instrument care oferă informații despre:

- ce informații sunt disponibile,
- pe ce bază legală,
- ce autoritate detine datele.

PNI furnizează astfel informații despre locurile în care datele necesare din registrele de baza sunt deja utilizate, astfel încât, în viitor, informațiile trebuie colectate doar o singură dată.

Ca instrument transparent de informare și analiză, va sprijini administrația în optimizarea proceselor administrative digitale.

2.7. Obiectivele specifice la care contribuie prestarea serviciilor

Obiectivele platformei naționale de interoperabilitate:

- **Cooperarea** - Facilitarea cooperării între diferitele aplicații de guvernare electronică și registrele de bază pentru a realiza un schimb eficient de informații între guvern și cetățeni, întreprinderi și alți parteneri;
- **Reutilizabilitatea** - Reutilizarea modelelor de procese și de date, a sistemelor, serviciilor și componentelor în diverse proiecte de guvernare digitală pentru a genera sinergii;
- **Deschidere** - Includerea de standarde deschise în aplicațiile de guvernare digitală pentru a promova capacitatea de utilizare pe termen lung a acestora;
- **Reducerea costurilor și a riscurilor** - Creșterea eficienței și reducerea costurilor din sectorul public din România prin modernizarea administrației;
- **Scalabilitate** - Asigurarea capacității de utilizare a aplicațiilor pe măsură ce cerințele se modifică în ceea ce privește volumul și frecvența tranzacțiilor;
- **Integritatea, coerența și disponibilitatea datelor** - Asigurarea validității, consecvenței, acurateței și consistenței datelor, inclusiv asigurarea continuă (fără întreruperi) a datelor/informațiilor/documentelor și resurselor de infrastructură necesare activităților specifice curente.

2.8. 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 guvernamental, instituțional și de colaborare între instituțiile implicate în procesul de atribuire a identității electronice (G2G) precum și în cel de declanșare a proceselor de validare a eligibilității și rezolvării solicitărilor cetățenilor.

Platforma va fi disponibilă în regim public și va asigura o serie de avantaje pentru toți utilizatorii sistemului informatic (persoane fizice, persoane juridice, instituții publice

centrale sau locale):

- Reducerea costurilor și timpului necesar pentru rezolvarea solicitărilor;
- Facilitarea dialogului și a cooperării rapide între autoritățile competente, persoanele fizice și persoanele juridice;
- Reducerea birocrăției;
- Istoric centralizat al comunicării avute de către autoritatea competentă, atât cu persoanele juridice, cât și cu alte autorități;
- Creșterea transparenței și accesibilității persoanelor juridice la serviciile oferite de către autoritățile competente;
- Creșterea gradului de satisfacție a persoanelor juridice în relația acestora cu autoritățile;

Beneficii pentru instituții publice (G2G)

Pentru instituțiile publice, implementarea proiectului aduce următoarele beneficii:

- Costuri reduse în administrarea sistemelor implementate la nivelul sistemelor informatice proprii prin utilizarea PNI;
- Creșterea calității serviciilor publice electronice oferite către cetățeni și firme;
- Accesul la serviciile oferite de instituțiile publice partenere în mod securizat;
- Asigurarea unor politici și strategii coerente la nivel administrativ prin integrarea și consolidarea datelor referitoare la cetățeni;
- Costuri scăzute pentru dezvoltarea aplicațiilor și serviciilor oferite prin asigurarea dezvoltării integrate, corelate consolidate la nivelul platformei naționale;
- Implementarea sistemului “once only” prin realizarea portalului și a mecanismului de schimb de date de tip hub care va realiza schimbul de date conform inițiativelor once-only;
- Colaborare intra-guvernamentală îmbunătățită prin relizarea de interfețe standardizate și folosirea regiștrilor naționali;
- Adoptarea flexibilă a noilor reglementări guvernamentale și implementarea rapidă de noi servicii electornice.

2.9. Alte inițiative/proiecte/programe asociate cu această achiziție

Informații suplimentare despre proiectele/programele derulate de ADR pot fi regăsite la următoarea adresă de internet - <https://www.adr.gov.ro>, secțiunea Programe și proiecte.

2.10. Factori interesați și rolul acestora

Din punct de vedere al actorilor care vor participa în fluxul de oferire al serviciilor publice electronice prin PNI vor exista următoarele categorii importante de entități conectate:

- ADR - administratorul PNI

- Instituțiile administrației publice centrale și locale, care oferă servicii de e-Guvernare
- administratorii registrelor de bază: autorități publice centrale prevăzute în Legea nr 242/2022
 - o administrația publică în calitate de utilizator al datelor
 - o utilizatorii persoane juridice de drept privat, persoanele care exercită profesii liberale reglementate, instanțe judecătorești, alte entități care pot interoga registrele de bază prin PNI.

Participanții la schimbul de date pot avea simultan rol de furnizor și de consumator de date, conform al 5, art 13 al Legii 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate.

3. SERVICIILE ȘI PRODUSELE SOLICITATE

3.1. CERINȚELE FUNCȚIONALE ALE SISTEMULUI

Cerințele funcționale care stau la baza sistemului integrat PNI sunt:

- **Consolidarea și interconectarea** sistemelor IT existente în instituțiile publice care furnizează/utilizează registrele de bază;
- **Alinierea** sistemelor IT **cu procesele guvernamentale (NRRI)** în vederea realizării serviciilor publice electronice care vor fi puse la dispoziția cetățenilor;
- **Obligativitatea utilizării datelor primare;**
- **Funcționalități de billing pentru consumul de date prin PNI.**

Mijloace tehnice pentru furnizarea G2G a unor dovezi sau certificări ale datelor deja colectate.

Datele utilizate în furnizarea serviciilor publice trebuie preluate exclusiv din registrele de bază disponibile prin intermediul platformei.

Mijloace tehnice pentru distribuirea sau reutilizarea informației într-o manieră transparentă și securizată, cu respectarea principiului colectării și stocării exclusiv a informațiilor necesare și a regulilor de protecție a datelor personale.

Sistemele vor fi conectate la platformă prin adaptoare care vor transforma, valida și cripta/decripta mesajele din/în formatul specific sistemului conectat, într-un format unificat, operat de platformă.

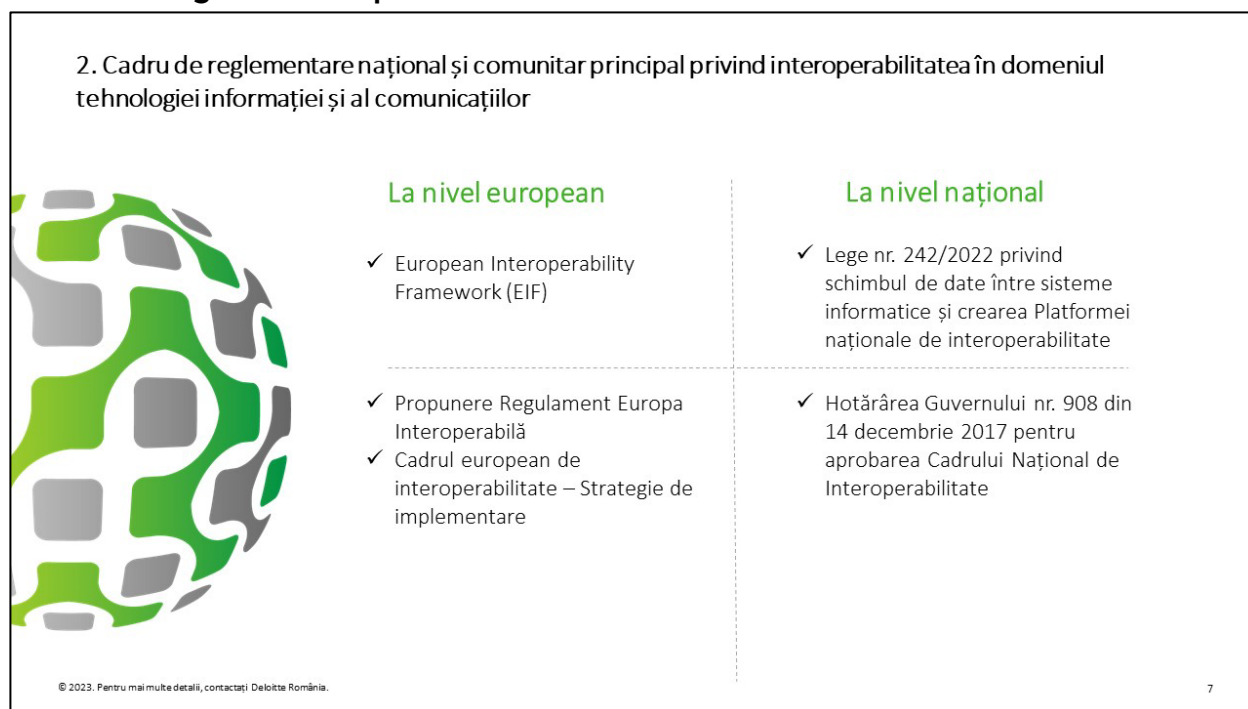
Procesul de conectare a unui sistem la platformă va fi reglementat la nivel tehnic și va include reguli de utilizare a standardelor și catalogului semantic, politici de versiune, precum și detalii tehnice privind conectarea la rețelele fizice, testarea/pilotarea și acceptarea sistemelor.

În vederea îmbunătățirii eficienței procesului de conectare, **PNI va include un mediu de testare distinct implementat.** Mediul de testare va include posibilitatea generării de date de test.

Toate serviciile PNI vor fi disponibile pentru reutilizare în vederea uniformizării conectării sistemelor informatice ce informatizează serviciile publice electronice.

Furnizorul va pune la dispoziție și va folosi pentru toate componentele sistemului informatic sisteme de operare recomandate de producătorii produselor software oferite.

Cadrul de reglementare pe care se bazează PNI



2. Cadru de reglementare național și comunitar principal privind interoperabilitatea în domeniul tehnologiei informației și al comunicațiilor

La nivel național: Scopul

- Facilitarea accesului instituțiilor private la datele deținute de instituții publice și viceversa;
- Asigurarea securității și confidențialității schimburilor de date;
- Crearea și actualizarea anuală a unui registru permanent al aplicațiilor informatice utilizate de autoritățile și instituțiile publice;
- Identificarea și definirea furnizorilor de date primare;
- Facilitarea integrării în piața unică digitală europeană;
- Asigurarea că implementarea funcționalităților implică alinierea infrastructurilor naționale de identificare și autorizare cu statele membre ale Uniunii Europene într-o schemă transnațională.

Obligațiile și responsabilitățile participanților la schimbul de date prin PNI

4. Obligații și responsabilități ale participanților la schimbul de date

Administratorul Platformei Naționale de Interoperabilitate (PNI)



- ☐ Propunerea de norme subsecvente în aplicarea NRRI și adaptarea constantă a acestora la realitățile și dezvoltările tehnice;
- ☐ Stabilirea datelor necesare asigurării interoperabilității sistemelor publice pentru furnizarea serviciilor publice care trebuie puse la dispoziția Platformei naționale de interoperabilitate de către autoritățile și instituțiile publice;
- ☐ În colaborare cu administratorii registrelor de date, stabilirea categoriilor de date care sunt partajate de fiecare autoritate și instituție publică și acordarea drepturilor de acces celorlalte autorități și instituții publice, persoane juridice de drept privat, respectiv persoane care exercită profesii liberale reglementate, pentru fiecare categorie de date;
- ☐ Prezentarea în mod transparent și nemijlocit a informațiilor administratorului registrului de date și titularului datelor;
- ☐ Administrarea, monitorizarea și supravegherea Platformei naționale de interoperabilitate;
- ☐ Stabilirea atribuțiilor și responsabilităților participanților la schimbul de date, monitorizarea și controlul utilizării Platformei naționale de interoperabilitate și sancționarea refuzului de a participa la platformă sau a utilizării abuzive sau necorespunzătoare;
- ☐ Popularizarea NRRI și a normelor de aplicare la nivelul administrației publice centrale și locale.

4. Obligații și responsabilități ale participanților la schimbul de date

Administrația publică în calitate de utilizator al datelor furnizate prin PNI



- ☐ Instituțiile și autoritățile publice **au obligația de a utiliza doar PNI** pentru accesarea datelor necesare furnizării serviciilor publice, respectiv interogarea registrelor de bază;
- ☐ Instituțiile și autoritățile **asigură prestarea serviciilor publice fără a solicita documente suplimentare**, care conțin informații disponibile prin PNI sau în scopul obținerii unor date, care pot fi furnizate prin intermediul PNI.
- ☐ Instituțiile și autoritățile publice care oferă servicii publice **nu au dreptul să solicite persoanelor fizice și juridice dovezi sau certificări ale datelor deja colectate sau disponibile prin PNI** sau create de către administratorii registrelor de bază.
- ☐ Instituțiile publice **pot reutiliza sau distribui date pe care persoanele fizice și juridice le-au furnizat unei instituții sau autorități publice**, în conformitate cu Regulamentul (UE) 2022/868 privind guvernarea datelor la nivel european.
- ☐ Instituțiile și autoritățile publice **au obligația de a-și schimba procedurile de lucru**, pentru a presta serviciile publice aflate în responsabilitatea lor, exclusiv în baza datelor ce pot fi obținute prin PNI.

© 2023. Pentru mai multe detalii, contactați Deloitte România.

17

4. Obligații și responsabilități ale participanților la schimbul de date

Administratorii registrelor de bază (autorități centrale sau locale sau alte entități publice)



- ☐ Autoritățile și instituțiile publice centrale și locale iau măsurile necesare și **încorporează tehnologiile necesare pentru interconectarea sistemelor informatice și schimbul de informații și servicii** între acestea;
- ☐ Autoritățile și instituțiile publice centrale, precum și cele locale care dețin un registru de bază sunt **obligate să se integreze cu Platforma națională de interoperabilitate în maximum 18 luni de la punerea în funcțiune a platformei** și să ofere acces la aceste date prin Platforma națională de interoperabilitate;
- ☐ În termen de 5 ani de la data intrării în vigoare a legii, **autoritățile și instituțiile publice vor furniza serviciile publice și în mod electronic, prin intermediul portalurilor proprii**, atunci când acest lucru este posibil;
- ☐ Autoritățile și instituțiile publice **stabilesc condițiile și instrumentele pentru înființarea și prestarea serviciilor publice electronice**, cu respectarea principiilor transparenței, publicității, responsabilității, calității, siguranței, disponibilității, accesibilității, neutralității și interoperabilității;
- ☐ Autoritățile și instituțiile publice care participă la schimbul de date **asigură resursele umane, financiare și tehnologice necesare** și iau măsurile necesare sau recomandate de autoritatea competentă în scopul asigurării conectării la Platforma națională de interoperabilitate, a continuității și securității schimbului de date, precum și a caracterului actual al datelor furnizate.

© 2023. Pentru mai multe detalii, contactați Deloitte România.

16

Contractul de schimb de date prin PNI

4. Contractul de schimb de date prin PNI



01

Forma contract

- Contractul de schimb de date prin intermediul platformei de interoperabilitate se va încheia între două părți - administratorul PNI și utilizatorii persoane juridice de drept privat.



02

Obligații administrator PNI

- Să anunțe participantul privat despre certificatele noi obținute pentru sistemele informaționale integrate în PNI cu cel puțin 10 zile lucrătoare înainte de expirarea celor utilizate curent;
- Să asigure interogarea datelor pentru participantul privat, prin PNI, fără denaturarea acestora.



03

Obligații utilizatori

- Să justifice scopul, volumul și modul de utilizare a informației consumate prin PNI;
- Să respecte regimul corespunzător de confidențialitate și securitate a informației;
- Să obțină și să gestioneze, pe cont propriu, certificatele fiecărui sistem informațional deținut, care urmează a fi integrat cu PNI.

© 2023. Pentru mai multe detalii, contactați Deloitte România.

19

Conectarea la PNI

5. Procedura de conectare și participare la platforma națională de interoperabilitate și a schimbului de date



© 2023. Pentru mai multe detalii, contactați Deloitte România.

21

5. Procedura de conectare și participare la platforma națională de interoperabilitate și a schimbului de date Accesul la registrele de bază



Elaborare

- Administratorul PNI, în colaborare cu administratorii registrelor de bază, elaborează un model de gestionare a registrelor de bază, care să asigure coerența informațională și disponibilitatea datelor pentru a implementa interoperabilitatea între sistemele informatice și resursele informaționale și pentru a menține securitatea informațiilor.



Documente esențiale

- Documentarea Registrelor de bază – informații esențiale



Modificări

- Administratorul PNI trebuie informat, în cel mult 30 de zile, în privința oricăror modificări referitoare la resursele de date pentru actualizarea registrelor și a PNI.

5. Procedura de conectare și participare la platforma națională de interoperabilitate și a schimbului de date Catalogul Național al Serviciilor Publice corelat cu PNI

Elemente

- descriptori ai serviciului electronic;
- descrierea API, utilizând unul dintre limbajele de descriere a interfețelor prevăzute pentru a utiliza serviciul electronic;
- documentația accesoriilor și manualele de utilizare a serviciului electronic.

Scop

- încurajează utilizarea serviciilor digitale prin publicarea acestora și prin punerea la dispoziție a documentației tehnice aferente;
- facilitarea gestionării ciclului de viață al serviciilor publice digitale;
- atenuarea creării de interfețe redundante și/sau de interfețe cu semantică suprapusă sau incompatibilă.

5. Procedura de conectare și participare la platforma națională de interoperabilitate și a schimbului de date Catalogul Național Semantic (semantic.gov.ro)

01



Registru de date creat pentru asigurarea evidenței activelor semantice, care constituie sursa unică și autentică de active semantice, organizată cu scopul asigurării interoperabilității semantice.

02



Catalogul Național Semantic (semantic.gov.ro) este un sistem informațional destinat configurării, managementului și evidenței activelor semantice gestionate de entități, instituții din România, pentru a oferi informații actualizate despre activele semantice disponibile, dar și metadata relevante schimbului de date.

© 2023. Pentru mai multe detalii, contactați Deloitte România.

24

3.2. ARHITECTURA FUNCȚIONALĂ A SISTEMULUI

Pentru asigurarea obiectivelor PNI (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, către furnizorii de servicii publice electronice și furnizorii de registre de baza;
- *Nivel de aplicații* - componentele necesare funcționării PNI;
- *Nivelul de date* - componentele de stocare a datelor gestionate în cadrul platformei respectiv 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 (criptare, firewall etc.);

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 între furnizorii registrelor de baza și instituțiile ce vor utiliza datele din cadrul acestora;
- Sistem de **gestiune a bazelor de date** în cadrul căruia se vor stoca toate instanțele bazelor de date aferente modulelor funcționale și portalului;
- O componenta de **analiză și raportare**;
- Componenta de **interoperabilitate** ce va permite schimbul de informații între diferite sisteme existente dar și viitoare la nivelul instituțiilor publice
- Componenta de **API management** - bazată pe tehnologie de tip API management;

- O soluție de **administrare a identității utilizatorilor** care va asigura următoarele procese:
 - o Conectarea cu platforma identităților electronice ROeID;
 - o Crearea și mentenanța identităților digitale și a rolurilor în platforma, pentru identitățile care nu fac obiectul ROeID (exemplu: reprezentanți ai administrației);
 - o 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 Definirea privilegiilor și serviciilor care vor fi gestionate de PNI;
 - o Autorizare și acces la serviciile electronice;
- O soluție de **monitorizare date, sisteme și aplicații** ce va permite detectarea și remediarea imediată, pe cât posibil automată, problemelor de funcționare care afectează utilizarea în bune condiții a sistemului informatic și îndeplinirea sarcinilor de serviciu;
- O soluție de **disaster recovery** ce va facilita procesul de recuperare a componentelor software și a datelor stocate în cazul unui dezastru;
- Componenta **SIEM** ce oferă posibilitatea colectării și monitorizării log-uri din cadrul sistemului;
- Componenta **concentrator VPN** ce va facilita conectarea mediului de producție al sistemului PNI din Cloud-ul Privat Guvernamental cu mediul de disaster recovery din Centrul de Date STS prin utilizarea unei soluții avansate de Virtual Private Network (VPN).

3.3. MANAGEMENTUL UTILIZATORILOR ȘI ACCESUL LA SISTEM

Autentificarea participanților - reprezentanți ai instituțiilor la schimbul de date realizat prin PNI se va putea realiza prin soluția RoelD.

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
- 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:
 - o Operarea și administrarea soluției în mod proactiv și eficient
 - o Monitorizarea permanentă a funcționării sistemului cu alertarea anomaliilor - erori sau avertizări legate de funcționalitate.
 - o Readucerea sistemului în parametrii normali de operare

- Persoane cu nivel mediu de cunoștințe IT și a produselor 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
- Va audita și monitoriza traficul în vederea realizării funcționalității de billing pentru consumul de date prin PNI.

3.4. SECURITATEA SISTEMULUI

Cerinte minime:

- Participanții la schimbul de date sunt obligați să informeze autoritatea competentă despre vulnerabilitățile și incidentele de securitate în utilizarea platformei de interoperabilitate în termen de cel mult 24 de ore din momentul depistării acestora.
- Datele transportate prin intermediul platformei sunt transportate în formă criptată.
- Transferul datelor este 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 prin intermediul platformei de interoperabilitate se realizează cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.
- Determinarea accesului la date are loc în condițiile art. 16 (f) pentru fiecare instituție și autoritate publică în parte. Fiecare instituție va acorda angajaților și colaboratorilor săi drepturile de acces la date conform alin. (8) al prezentului articol.
- Persoana vizată are dreptul să primească informațiile prevăzute la art. 13 și 14 din Regulamentul nr. 679/2016 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 în condițiile art. 12 din Regulament, la intervale rezonabile, dar nu mai mari de 1 an.
- Administratorii registrelor de date au următoarele obligații:

- să asigure implementarea cerințelor minime de securitate cibernetică prevăzute de legislația națională, europeană și de standardele și specificațiile naționale, europene și internaționale aplicabile în domeniul securității cibernetică;
- să asigure existența unor procese și proceduri pentru a asigura securitatea operațională 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 printr-o combinație de protecție a rețelei și criptare;
- să nu permită accesul fără drept la datele din platforma de interoperabilitate 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 gestioneze și să rezolve de îndată incidentele de securitate cibernetică;
- să nu afecteze, prin acțiunile proprii, securitatea altor infrastructuri cibernetică;
- să se asigure că personalul este instruit corespunzător pentru utilizarea platformei de interoperabilitate și controlat periodic pentru a preveni erori umane sau încălcări de securitate;

Utilizatorii de date nu trebuie să se angajeze în nicio activitate care să compromită siguranța platformei.

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 aceasta 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 astfel 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 baza 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 a nodului). 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 aplicat 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

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).

3.5. CONFIDENȚIALITATEA DATELOR

Confidențialitatea 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;

3.6. ARHITECTURA TEHNICĂ

Din punct de vedere tehnic, arhitectura sistemului PNI va include un mediu de producție ce va fi găzduit în Cloud-ul Privat Guvernamental și două medii ce vor fi găzduite în Centrul de Date STS din Cristian, Jud. Brașov: unul de testare-dezvoltare și unul de disaster recovery.

Arhitectura sistemului va fi constituită din soluții redundante, cu asigurarea disponibilității și balansarea încărcării (cluster HA) pentru următoarele componentele funcționale ale sistemului:

- Componenta portal
- Soluția de management documente
- Sistemul de gestiune a bazelor de date în cadrul căreia se vor stoca toate instanțele bazelor de date aferente modulelor funcționale și portalului
- Componenta de interoperabilitate
- Componenta de API management

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

- a) **Mediul de producție** - asigură funcționarea în producție a sistemului PNI și reprezintă mediul care va fi utilizat în mod direct de către instituțiile publice pentru schimbul de informații electronice și furnizarea serviciilor electronice expuse de către acestea 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 PNI în urma unui dezastru al mediului de producție din Cloud-ul Privat Guvernamental în mediul de disaster recovery din Centrul de Date STS din Cristian, Jud. Brașov 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.

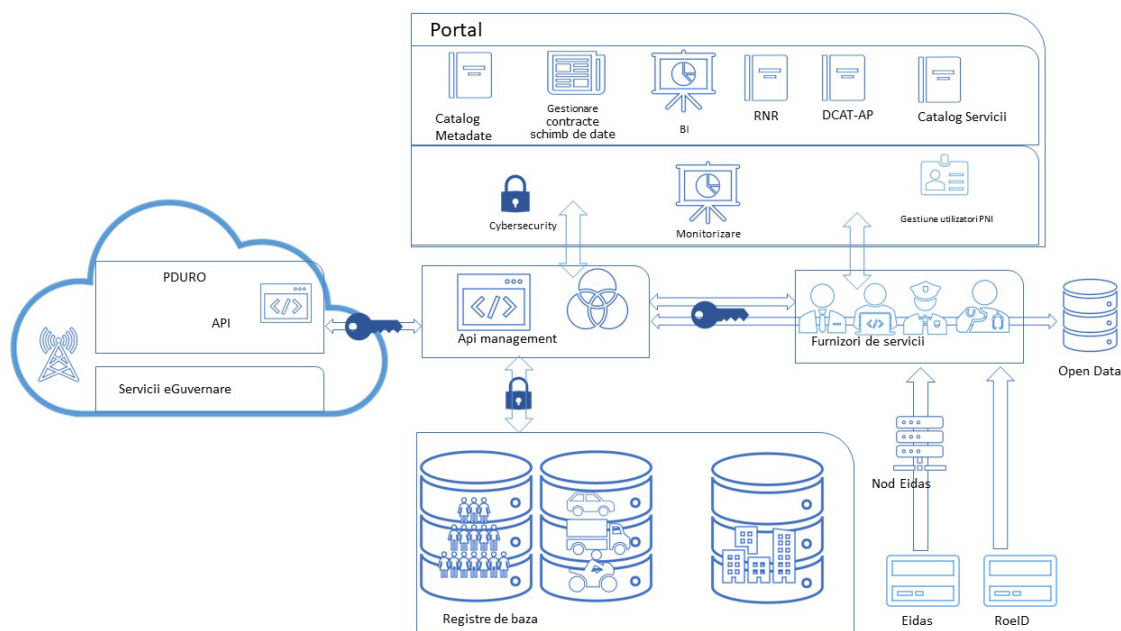
Mediul de producție va fi dimensionat fără limitarea din punct de vedere al licențierii pe infrastructura hardware minimă solicitată; în cazul soluțiilor cu alta metrică sau modalitate de licențiere, infrastructura software va trebui să asigure un minim de 3000 de instituții ale administrației publice la PNI.

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 PNI și pentru funcționarea acestuia pentru o perioadă scurtă de timp, până la repunerea în funcțiune a mediului de producție.

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 emisie, 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.



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

Dimensionarea componentelor funcționale și a celor de suport ale mediului de producție vor 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 fizice minime pe nod producție	Memorie RAM (GB) minim necesară per nod producție
1.	Componenta portal	2	Cluster HA	8	32
2.	Solutia de management documente	2	Cluster HA	8	64
3.	Sistemul de gestiune a bazelor de date	2	Cluster HA	8	256
4.	Componenta de business intelligence	2	Cluster	16	256
5.	Componenta de interoperabilitate	2	Cluster HA	16	256
6.	API management	2	Cluster HA	8	256
7.	Platforma pentru administrarea identitatii utilizatorilor	2	Cluster	8	64
8.	Componenta de securizare a accesului privilegiat	2	Cluster	8	32
9.	Monitorizare date, sisteme si aplicatii	1		24	128
10.	Solutia de disaster recovery	1		8	32
11.	Solutia de tip SIEM	1		16	64
12.	Solutie concentrator VPN	1		8	32

Ofertanții vor dimensiona, instala și configura mediul de Disaster Recovery (DR) în regim activ-pasiv, complet separat de mediul de producție, dimensionat corespunzător astfel încât să asigure funcționarea integrală a aplicațiilor și serviciilor critice în scenariu de failover, fără degradări majore de performanță. Dimensionarea se va realiza pe baza specificațiilor hardware ale mediului de producție furnizate mai sus. Toate componentele software (sisteme de operare, baze de date, aplicații middleware etc.) vor fi licențiate corespunzător pentru scenariul activ-pasiv, cu respectarea politicilor producătorilor. Soluția va asigura replicarea datelor între producție și DR astfel încât să fie respectate următoarele obiective: RPO = 15 minute și RTO = 2 ore. Ofertantul este responsabil pentru analiza necesarului de resurse, furnizarea licențelor, implementarea și documentarea arhitecturii DR, precum și

pentru demonstrarea fezabilității soluției prin testarea planului de disaster recovery.

3.7. COMPONENTELE HARDWARE ȘI DE COMUNICAȚII

Echipamentele hardware vor fi instalate în cadrul Centrului de Date STS din Cristian, Jud. Brașov, în maxim 2 rack-uri. Se vor folosi resursele de infrastructură disponibile în locație.

Cerintele minime pentru echipamentele hardware și de comunicații sunt:

3.7.1. Sistem integrat de procesare și stocare date

Soluția propusă va avea la bază: • sistem de procesare și stocare de tip hyper-convergent format din cel puțin 8 noduri în configurație identică; • sistem de stocare a datelor de tip unificat; • noduri de procesare dedicate bazei de date • switch-uri pentru interconectare LAN și SAN; • sistem pentru realizarea salvării și restaurării datelor; Soluția propusă va fi în format rack-mountable maxim 24U și va include șine, captive pentru montare în cabinetul de tip rack existent la Autoritatea Contractantă. Vor fi livrate toate cablurile și accesorii necesare pentru interconectarea echipamentelor.	
Sistem de procesare și stocare de tip hyper-convergent format din cel puțin 8 noduri în configurație identică, fiecare nod având următoarele cerințe minime:	
Caracteristică	Cerințe tehnice minime
Procesor	Tehnologie: • Tip: CISC 64 biți tip Intel Xeon generația a cincea sau echivalent; • Nuclee: minim 24 nuclee fizice per procesor; • Frecvența de bază: minim 2,9 GHz; • Cache: minim 60 MB Smart Cache per procesor sau echivalent; • Magistrală: 3 x UPI 20 GT/s sau echivalent; • Putere consumată: maxim 250 W per procesor; • Număr de procesoare instalate: minim 2;
Memorie RAM	Instalat cel puțin 1024 GB DDR5 ECC 5600 MT/s, suport pentru tehnologii de protecție de tip Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection sau echivalent; Minim 32 sloturi de memorie (din care cel puțin 16 libere) disponibile în șasiu;

	Posibilitate de creștere la minim 2048 GB de memorie RAM DDR5 RDIMM prin adăugarea ulterioară de module de aceeași capacitate cu cele existente.
Capacitate de stocare internă	Va dispune de cel puțin 10 sloturi hot-plug / hot-swap, de tip 2.5” instalate și disponibile în șasiu pentru instalarea modulelor de stocare NVMe. Va fi echipat cu cel puțin: • 2 module de 960 GB NVMe flash hot-plug / hot-swap în RAID 1 cu controller hardware dedicat, pentru rularea sistemului de operare; • 3 module de 3.84 TB NVMe flash hot-plug / hot-swap cu rol pentru stocarea datelor;
Interfețe rețea	Va fi echipat cu cel puțin: • 4 porturi 100 Gbps Ethernet, dispuse pe cel puțin 2 adaptoare de rețea distincte, compatibile cu switch-urile pentru interconectare LAN și SAN; • 2 porturi 1 Gbps Ethernet RJ-45
Porturi	Minim: 2 x VGA sau display port (din care 1 frontal), minim 2 x USB 2.0 (din care 1 frontal) și 1 x USB 3.0, 1 x RJ-45 management;
Sloturi de expansiune	Pentru instalarea modulelor IO, echipamentul va dispune de sloturi PCI Express: minim 3 sloturi extensie, PCIe x16 Gen4 (cu 16 lane-uri PCI Express conectate);
Management Hardware	Nodul trebuie să fie livrat cu capabilități hardware și software, instalate, activate și licențiate perpetuu pentru următoarele funcționalități: • management de la distanță; • redirectare interfață grafică cu tastatură și mouse; • suport pentru virtual clipboard: copiere, taiere, lipire text de pe consola virtuală pe serverul gazdă; • posibilitate de pornire/oprire de la distanță; • suport pentru remote media (virtual CD si floppy); • suport pentru SSL (Secure Socket Layer); • integrare cu Active Directory / LDAP (Lightweight Directory Access Protocol); • autentificare two-factor; • monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice; • managementul evenimentelor și alarmelor; • inventarul și monitorizarea componentelor (inclusiv module optice SFP); • instalarea update-urilor și patch-urilor;

	• analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat; • realizarea de rapoarte de performanță pe baza datelor transmise de senzori (streaming telemetry) care indică utilizarea resurselor sistemului de calcul (procesor, memorie, I/O), consumului de energie electrică, temperatură, independent de sistemul de operare și fără a consuma resurse de procesor din server; • repornirea și reconfigurarea automată a serverului; • permite generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere similare din infrastructură; • permite stocarea pe un NAS extern cu funcționalități de retenție a fișierelor pentru a asigura protecția la ștergere și modificare a fișierelor de update, șabloanelor de configurare și imaginilor de sistem de operare; • permite ștergerea securizată a unităților de stocare de tip SSD și HDD; • validare a configurației serverului față de o referință; • RESTful API cu suport Redfish; • Interfețe acces utilizator: HTML5 Web GUI, SSH; • Funcționalitățile vor fi asigurate fără a fi necesară instalarea de agenți software. • Port dedicat 1 Gigabit Ethernet RJ-45 ce permite accesarea sistemului de management indiferent de stadiul de funcționare al nodului de procesare și stocare; • Pentru a asigura compatibilitatea, modulul hardware de administrare trebuie să fie furnizat de același producător cu cel al nodului de procesare și stocare.
Securitate	Trusted Platform Module 2.0 inclus; Posibilitatea de a dezactiva butonul de pornire (power) din BIOS; Capabilități incluse pentru chassis intrusion detection ce utilizează sistemul de management încorporat, monitorizând și detectând: accesul la șasiu, îndepărtarea sau înlocuirea unei componente a serverului; Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate; Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS boot loader și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze;

	Suport hardware inclus pentru verificarea și validarea autenticității firmware-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare); Update-urile de firmware trebuie să fie semnate criptografic de către producătorul echipamentului oferat pentru a fi autentificate la instalare; Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Log-urile acestor informații de audit vor fi securizate și vor putea fi accesate doar din componenta de management a soluției propuse; Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului; Suport inclus pentru utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare și posibilitatea de a utiliza un certificat personalizat pentru semna un Linux OS boot loader; Firmware rollback; Protecție pe perioada transportului la intervenție asupra hardware: suport inclus pentru verificarea securizată a componentelor echipamentului livrat la beneficiar prin care să se asigure că echipamentul este exact cum a plecat de la producător.
Alimentare electrică	Nodul va fi dispune de alimentare electrică redundantă, din două surse de tip hot-swap, de min. 1100W fiecare, 200-240V 50Hz. Vor fi incluse cabluri de alimentare electrică de cu conectori tip C13-C14.
Format carcasă	Se va livra cu șine glisante de montare în rack adecvate sistemului livrat și braț de gestionarea a cablurilor; Spațiu ocupat în rack: maxim 1U/nod de procesare și stocare;
Ventilatoare	Ventilatoare redundante, hot-plug / hot-swap, viteză de rotație variabilă;
Interconectare	Pentru interconectarea echipamentelor, a nodurilor și traficul mașinilor virtuale, soluția va fi prevăzută cu două echipamente de tip switch pentru interconectare LAN și SAN, fiecare cu următoarele caracteristici minime: compatibile cu switch-urile infrastructură pentru interconectare LAN și SAN compatibile cu switch-urile infrastructură pentru interconectare LAN și SAN - 32 porturi de capacitate 100GbE QSFP28; fiecare port QSFP28 trebuie să fie multirate și să suporte breakout în 4 x 10 GbE, 4 x 25 GbE, 1 x 40GbE, 2 x 50GbE; 24 cabluri QSFP28 la QSFP28 de lungime 10m, 2 cabluri QSFP28 la 4xSFP28 de lungime 5m, 1 cablu QSFP28 la QSFP28 de lungime 1m ;

	- Capacitate de switching full duplex: cel puțin 6.4 Tbps - Capacitate de forwarding full duplex: cel puțin 4.8 Bpps - Latenta maximă acceptată: 900 nano secunde - Suport pentru: Virtual LANs, 802.1t RPVST, 802.1w RSTP, 802.1s MST, 802.3ad LACP, 802.1ab LLDP, Port Monitoring, mecanism de tip MC-LAG ce poate fi integrat cu funcționalități L3 (inclusiv rutare dinamică pe echipamentele configurate în MC-LAG); - Număr minim de VLAN-uri disponibile: 4.000; - Memorie buffer pentru pachete: minim 32MB; - Surse redundante de alimentare electrică, hot-swap, 200-240V 50Hz; - Rackmountable 1U; Pentru interconectarea echipamentelor și managementul OOB va fi inclus cel puțin un switch Gigabit Ethernet având 48 porturi 1 GbE RJ-45, 4x10G SFP+, 2x100G QSFP28; Vor fi incluse toate cablurile, modulele care să asigure interconectarea echipamentelor; Switch-urile vor dispune de surse redundante de alimentare electrică, hot-swap, 200-240V 50Hz și vor avea format rackmountable 1U; Pentru a preveni posibile incompatibilități și probleme de performanță, echipamentele de tip switch vor fi compatibile și certificate pentru funcționarea în cadrul soluției de hiperconvergență.
Nodurile de procesare dedicate pentru baza de date trebuie să îndeplinească următoarele cerințe minimale (2 bucăți):	
Procesor	Tehnologie: • Tip: CISC 64 biți tip Intel Xeon generația a cincea sau echivalent; • Nuclee: minim 16 nucleu fizice per procesor; • Frecvența de bază: minim 3.6 GHz; • Cache: minim 45 MB Smart Cache per procesor sau echivalent; • Magistrală: 3 x UPI 20 GT/s sau echivalent; • Putere consumată: maxim 300 W per procesor; • Număr de procesoare instalate: minim 2;
Memorie RAM	Instalat cel puțin 1024 GB DDR5 ECC 5600 MT/s, suport pentru tehnologii de protecție de tip Demand Scrubbing, Patrol Scrubbing, Permanent Fault Detection sau echivalent; Minim 32 sloturi de memorie (din care cel puțin 16 libere) disponibile în șasiu;

	Posibilitate de creștere la minim 2048 GB de memorie RAM DDR5 RDIMM prin adăugarea ulterioară de module de aceeași capacitate cu cele existente.
Capacitate de stocare internă	Server cu cel puțin 8 sloturi hot-plug / hot-swap, de tip 2.5” instalate și disponibile în șasiu pentru instalarea modulelor de stocare NVMe; Serverul va fi echipat cu cel puțin 2 module 960 GB NVMe SSD, hot-plug / hot-swap, configurate în RAID 1;
Controller RAID intern	Controller RAID PCIe cu suport pentru 8 module NVMe 2.5” hot-swap, suport pentru RAID 0, 10, 1, 5, 50, 6, 60; Memorie cache nevolatilă instalată la nivelul controller-ului de minim 8 GB de tip DDR4 2666 MT/s sau superior; Controller-ul RAID trebuie să dispună de mecanisme interne de mărire a capacității online, configurare de disk hot-spare dedicat și global;
Interfață video	Interfață video integrată ce suportă o rezoluție minimă de 1920 x 1200
Interfețe rețea	Va fi echipat cu cel puțin: • 4 porturi 100 Gbps Ethernet, dispuse pe cel puțin 2 adaptoare de rețea distincte, compatibile cu switch-urile pentru interconectare LAN și SAN; • 2 porturi 1 Gbps Ethernet RJ-45
Porturi	Minim: 2 x VGA sau display port (din care 1 frontal), minim 2 x USB 2.0 (din care 1 frontal) și 1 x USB 3.0, 1 x RJ-45 management;
Sloturi de expansiune	Pentru instalarea modulelor IO, echipamentul va dispune de sloturi PCI Express: minim 3 sloturi extensie, PCIe x16 Gen4 (cu 16 lane-uri PCI Express conectate);
Management	Sistem încorporat de monitorizare a: procesoarelor, memoriilor, HDD-urilor, interfețelor IO, ventilatoarelor, surselor de alimentare, temperaturii; analize predictive de eroare pentru componentele sistemului cu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componente.
	LCD display sau panou cu LED-uri ce trebuie să permită indicarea stării de funcționare cu panoul frontal instalat, fără operațiuni suplimentare;
	Aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului, capabilă de instalare locală și de la distanță, în mod neasistat, inclusiv configurare RAID;
	Echipamentul trebuie să fie livrat cu capabilități hardware și software, instalate, activate și licențiate perpetuu pentru următoarele funcționalități: • management de la distanță; • redirectare interfață grafică cu tastatură și mouse;

	• suport pentru virtual clipboard: copiere, taiere, lipire text de pe consola virtuală pe serverul gazdă; • posibilitate de pornire și oprire server de la distanță; • suport pentru remote media (virtual CD si floppy); • suport pentru SSL (Secure Socket Layer); • integrare cu Active Directory / LDAP (Lightweight Directory Access Protocol); • autentificare two-factor; • monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice; • managementul evenimentelor și alarmelor; • inventarul și monitorizarea componentelor (inclusiv GPU, module optice SFP); • instalarea update-urilor și patch-urilor; • analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat; • realizarea de rapoarte de performanță pe baza datelor transmise de senzori (streaming telemetry) care indică utilizarea resurselor sistemului de calcul (procesor, memorie, I/O), consumului de energie electrică, temperatură, independent de sistemul de operare și fără a consuma resurse de procesor din server; • repornirea și reconfigurarea automată a serverului; • permite generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere similare din infrastructură; • permite stocarea pe un NAS extern cu funcționalități de retenție a fișierelor pentru a asigura protecția la ștergere și modificare a fișierelor de update, șabloanelor de configurare și imaginilor de sistem de operare; • permite ștergerea securizată a unităților de stocare de tip SSD și HDD; • validare a configurației serverului față de o referință; • RESTFul API cu suport Redfish; • integrare cu Microsoft System Center și cu VMware vCenter; • interfețe acces utilizator: HTML5 Web GUI, SSH; • Funcționalitățile vor fi asigurate fără a fi necesară instalarea de agenți software. • Port dedicat 1 Gigabit Ethernet RJ-45 ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului.
--	--

	Pentru a asigura compatibilitatea, modulul hardware de administrare trebuie să fie furnizat de același producător cu cel al serverelor.
Aplicație administrare	Trebuie să permită administrare și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți; Pentru a asigura compatibilitatea, aplicația trebuie să fie furnizată de același producător cu cel al server-elor; Trebuie să permită inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, interfețe IO, controllere RAID, unități de stocare; Trebuie să permită update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticității acestora; Trebuie să permită generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură; Trebuie să permită instalarea sistemelor de operare și virtualizare pe serverele aflate în administrare; Permite stocarea pe un storage extern cu funcționalitate de retenție a fișierelor sau server web, pentru a asigura protecția la ștergere și modificare a fișierelor de update, template-urilor de configurare și imaginilor de sistem de operare; Trebuie să ofere funcționalitatea de validare a configurației față de o referință; Monitorizează starea de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică; Permite ștergerea securizată a unităților de stocare de tip SSD si HDD. Trebuie să genereze grafice cu nivele de încărcare și utilizare ale serverelor cu un istoric pe o perioada configurabilă de cel puțin 1 an.
Format	Serverul rackabil trebuie să fie montabil în rack-uri standard de 19". Înălțimea maximă a serverului rackabil trebuie să fie maxim 1 RU. Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (șine glisante, braț de gestionare a cablurilor, șuruburi/captive). Serverul rackabil trebuie să aibă LED de localizare pentru identificarea poziției în rack. Panou frontal cu mecanism de închidere pentru securizare acces la discuri și LCD sau LED-uri pentru indicarea stării de funcționare a sistemului.
Securitate	Trusted Platform Module 2.0; Posibilitatea de a dezactiva butonul de pornire (power) din BIOS; Capabilități incluse pentru chassis intrusion detection ce utilizează sistemul de management încorporat, monitorizând și detectând:

	accesul la șasiu, îndepărtarea sau înlocuirea unei componente a serverului; Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate; Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS boot loader și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze; Suport hardware inclus pentru verificarea și validarea autenticității firmware-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare); Update-urile de firmware trebuie să fie semnate criptografic de către producătorul echipamentului oferit pentru a fi autentificate la instalare; Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Log-urile acestor informații de audit vor fi securizate și vor putea fi accesate doar din componenta de management a soluției propuse; Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului; Suport inclus pentru utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare și posibilitatea de a utiliza un certificat personalizat pentru semna un Linux OS boot loader; Firmware rollback; Protecție pe perioada transportului la intervenție asupra hardware: suport inclus pentru verificarea securizată a componentelor echipamentului livrat la beneficiar prin care să se asigure că echipamentul este exact cum a plecat de la producător.
Surse alimentare electrică	Serverul trebuie alimentat printr-un sistem de surse de alimentare electrică care trebuie să îndeplinească următoarele cerințe: • număr surse interne instalate: minim 2; • funcționare în regim „N+1”; • surse de tip „hot pluggable”; • clasa de eficiență: 80 PLUS Titanium • putere: minim 1100 W per sursă. Ofertantul trebuie să livreze minim 2 cabluri de alimentare electrică de tip C13-C14 pentru conectarea la PDU, de lungime minim 2m.

Sistem de operare	Serverul trebuie să fie compatibil cu sistemele de operare: Microsoft Windows Server 2019, 2022, 2025 Hyper-V, Red Hat Enterprise Linux 8,9, SUSE Linux Enterprise Server 15, Ubuntu Server LTS 22.04, 24.04, VMware ESXi 7.0, 8.0;
Sistemul hyper-convergent propus va avea la bază un nivel de virtualizare a resurselor fizice pentru rularea resurselor în varianta mașini virtuale. Sistemul de virtualizare trebuie să fie de tip COTS cu licențiere perpetuă sau sub forma de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție. Astfel, soluția propusă trebuie să nu depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea și funcționalitatea serverelor, respectiv a mașinilor virtuale care rulează pe serverele respective. Amprenta pe disc a hypervisor-ului să fie cât mai mică astfel încât instalarea hypervisor-ului să se poată realiza foarte rapid (direct pe server) chiar și din rețea, oferind totodată posibilitatea de boot-are de pe stick USB. Suport pentru USB 3.0 și rularea de aplicații grafice (DirectX 9 sau OpenGL2.1) pe mașinile virtuale și suport pentru accelerare video hardware pentru mașinile virtuale cu sisteme de operare Linux, Windows. Cerințe privind soluția software pentru virtualizare: • Soluția de virtualizare propusă trebuie să ofere o scalabilitate crescută prin configurarea în clustere de înaltă disponibilitate de minim 64 de host-uri. • Soluția ofertată va trebui să permită managementul unificat al tuturor nodurilor în aceeași consolă centralizată de management. • Să dispună de funcționalități de failover astfel încât, în cazul defectării unui host (nod), mașinile virtuale care rulează pe acel host să fie repornite automat pe celelalte host-uri din cluster; • 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 permită identificarea și evitarea situațiilor de split-brain prin monitorizarea stării host-urilor atât la nivelul rețelei de management cât și la nivelul storage-urilor comune; • Soluția de virtualizare propusă trebuie să asigure o disponibilitate continuă (fără întreruperea serviciilor și fără pierdere de date) pentru mașinile virtuale configurate cu 8 virtual CPU-uri și 128 GB RAM, în cazul defectării fizice a host-urilor pe care rulează; • Soluția de virtualizare propusă trebuie să asigure posibilitatea mutării simultane a cel puțin 8 mașini virtuale aflate în funcționare, de pe un host pe altul/altele, fără întreruperea serviciilor și fără pierdere de date, pentru balansarea încărcării la nivel de cluster sau pentru a se putea executa activități de mentenanță pe host-ul respectiv;	

- Să permită mutarea mașinilor virtuale peste rețele IP cu latente ridicate, de până la 150ms (ex. rețele naționale sau continentale) dând astfel posibilitatea migrării mașinilor în funcționare între centre de date distante;
- Să permită gruparea mai multor volume de stocare cu performanțe similare în clustere pentru simplificarea managementului și plasarea inteligentă, respectiv balansarea încărcării în funcție de spațiu stocare sau timp de acces) mașinilor virtuale în mod automat la nivel de cluster;
- Să asigure balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vedere asigurării resurselor optime pentru funcționare;
- Să ofere mecanisme automate de economisire a energiei electrice prin concentrarea masivă a mașinilor virtuale pe câteva host-uri și oprirea host-urilor nefolosite în momentul în care încărcarea mașinilor virtuale scade. În mod similar, atunci când încărcarea mașinilor virtuale crește, host-urile oprite vor fi pornite în vederea asigurării resurselor de calcul corespunzătoare prin balansarea automată a încărcării pe fiecare host din cluster;
- Să ofere posibilitatea executării operațiunilor de mentenanță sau upgrade la storage fără afectarea funcționării mașinilor virtuale;
- Să asigure rate mari de consolidare a mașinilor virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memoriei (ex “Memory Ballooning”, “Transparent Page Sharing”, “Memory Compression”, “Swap to disk”) pentru reducerea costurilor asociate infrastructurii fizice (ex. număr host-uri, număr porturi de rețea/switch-uri);
- Soluția de virtualizare propusă trebuie să fie compatibilă și să permită instalarea de mașini virtuale rulând următoarele sisteme de operare: Microsoft Windows (Server: 2022, 2019, 2016, 2012 R2, 2008 R2, 2003 R2, Desktop: 11, 10, 8.1, 7), Red Hat, SUSE, Ubuntu, FreeBSD, CentOS, Solaris, Oracle Linux, Mac OS X Server;
- Să suporte diverse tipuri de storage (SAN, NAS, iSCSI) și protocoale de acces (FC, NVMe/TCP, NVMe/FC, iSCSI, NFS) și să permită prioritizarea și garantarea performanțelor I/O (SLA) ale mașinilor virtuale, la nivel de cluster;
- Soluția de virtualizare să asigure suport larg din partea ISV (Independent Software Vendors) terți pentru aplicațiile importante (de ex. Microsoft SQL, Exchange, SharePoint, Oracle DB & App);
- Soluția de virtualizare trebuie să asigure posibilitatea utilizării unor echipamente de stocare externe pentru mai multe host-uri; storage-urile trebuie să poată stoca atât mașinile virtuale cât și hard disk-urile virtuale asociate acestora;
- Accesul către sistemul de stocare extern să poată fi făcut pe mai multe căi (multipathing), asigurându-se suport pentru failover și load balancing, oferind și posibilitatea de alegere a politicii de stabilire a căii de acces (ex. fixă, MRU, Round Robin);

- Sistemul de fișiere va permite accesul concurrent a mai multor servere fizice (host) și a mai multor mașini virtuale la aceeași resursă de stocare;
- Sistemul de fișiere trebuie să asigure că o mașină virtuală este accesată doar de pe un singur host (sistem de blocarea accesului); în caz de defectare a host-ului mașina virtuală trebuie să poată fi repornită de pe alt server fizic;
- Sistemul de fișiere va asigura posibilitatea migrării în timp real (fără întreruperea funcționării) unei mașini virtuale de pe un host pe altul, de pe o capacitate de stocare pe alta;
- Soluția de virtualizare trebuie să permită adăugarea de procesoare virtuale, memorie RAM, interfețe de rețea și disk-uri la mașinile virtuale fără a necesita oprirea acestora (în funcție de suportul asigurat de sistemul de operare instalat în mașina virtuală);
- Soluția de virtualizare să asigure configurarea switch-uri virtuale de rețea, distribuite peste toate host-urile din cluster, care să permită configurarea centralizată a rețelei, eliminând greșelile de configurare;
- 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 prezentarea unui adaptor de rețea PCIe (PCI Express) ca mai multe adaptoare logice direct către mașinile virtuale, reducând astfel latența rețelei respectivelor mașini virtuale (I/O offload) și oferind performanțe ridicate;
- Trebuie să asigure suport pentru aplicarea centralizată a actualizărilor (patch-urilor) pentru host-uri, mașini virtuale sau appliance-uri virtuale;
- Trebuie să permită managementul salvărilor contextuale (snapshot) ale mașinilor virtuale fără afectarea stării de funcționare, astfel încât o mașină virtuală se va putea restaura din orice salvare anterioară;
- Interfața unică de management bazată pe web, accesibilă de pe browser Firefox, Google Chrome, Microsoft Edge pentru simplificarea managementului;
- Soluția de management centralizat să fie disponibilă ca appliance virtual pentru simplificarea instalării, actualizării și administrării precum și pentru reducerea costurilor asociate (ex. licența Windows, licență bază de date SQL sau Oracle);
- 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).

Soluția propusă pentru zona de stocare trebuie să fie una care să utilizeze discurile interne ale nodurilor în vederea definirii unui zone comune de stocare disponibilă la nivelul clusterului.

Soluția propusă trebuie să răspundă cel puțin următoarelor cerințe minimale:

- Soluția va utiliza mediile de stocare interne ale nodurilor pentru prezentarea unei capacități de stocare comună resurselor virtualizate, funcționalitate ce va oferi performanțe și disponibilitate ridicate: repornirea automată a mașinilor

virtuale, în cazul defectării unui sistem gazdă (server fizic) din cluster, pe celelalte sisteme disponibile; protecția continuă a mașinilor virtuale contra defectării sistemelor gazdă; migrarea în timpul funcționării a mașinilor virtuale; balansarea încărcării pe sistemele gazdă la nivelul întregului cluster;

- Soluția va fi integrată în hipervizor pentru a asigura o cale optimizată de I/O, în vederea asigurării unor performanțe ridicate și cu impact minim asupra procesorului și memoriei sistemului gazdă;
- Soluția va oferi performanțe ridicate, de nivelul unui sistem de stocare Enterprise, prin accelerarea citirilor și a scrierilor I/O folosind un mecanism de caching integrat, bazat pe dispozitive Flash (NVMe) instalate în sistemele gazdă;
- Soluția trebuie să permită scalabilitate / extindere foarte ușoară a capacității de stocare, fără întreruperea funcționării aplicațiilor și a serviciilor care rulează la nivelul mașinilor virtuale, atât prin adăugarea de medii de stocare (NVMe) suplimentare pe sistemele gazdă din cluster cât și prin adăugarea de noi sisteme gazdă (servere fizice) cu capacitate adițională de stocare în cluster; extinderea capacității în acest fel se va face cu redistribuirea automată și uniformă a blocurilor de date la nivelul nodurilor clusterului;
- Soluția trebuie să asigure toleranță la defectări prin tehnologie tip RAID 5, 6 sau echivalent (pentru protecția datelor stocate cu simplă și dublă paritate) și prin cache mirroring (pentru protecția cache-ului), asigurând astfel protecția datelor în cazul unor defectări la nivel de disk, sistem gazdă, rețea sau chiar rack (prin distribuirea sistemelor gazdă în mai multe rack-uri);
- Soluția de stocare permite realizarea unui management bazat pe politici definite la nivel de mașină virtuală, care asigură automatizarea provizionării și balansării resurselor de stocare în vederea asigurării stocării și serviciilor de stocare aferente mașinilor virtuale;
- Administrarea soluției trebuie să fie cât mai simplă pentru un administrator de mediu virtual, fiind integrată în sistemul de management al mediului virtual;
- Soluția trebuie să permită, în mod eficient, realizarea de până la 32 de snapshot-uri și/sau clone ale unei mașini virtuale;
- Soluția trebuie să permită prezentarea unui sistem de stocare de tip block, folosind protocolul iSCSI, pentru accesul dinspre servere ne-virtualizate (servere externe cluster-ului de virtualizare);
- Soluția trebuie să asigure un management îmbunătățit al SLA-ului privind performanțele mașinilor virtuale, prin stabilirea de limite IOPS la nivel de mașină virtuală, eliminând astfel problemele de tip noisy neighbor, în care o mașină virtuală non-critică generează un număr foarte mare de IOPS, influențând negativ performanțele mașinilor virtuale critice / de producție;
- Soluția are inclusă funcționalitatea de deduplicare și compresie a datelor inline (în timp real) pentru arhitecturile all-flash, asigurând astfel reducerea spațiului ocupat și creșterea eficienței soluției de stocare;

- Soluția va asigura, în mod automat, integritatea datelor, prin verificarea automată a blocurilor de date stocate, pentru evitarea situațiilor de corupere a acestora prin erori de disc nedetectate;
- Soluția trebuie să asigure protecția la defectarea componentelor (disk, rețea, host) la nivel local (prin mecanismele de protecție la nivel de disk și host);
- Managementul zonei de stocare trebuie să fie integrat la nivelul consolei de management unitară a sistemului propus, astfel încât toate operațiile de administrare să fie posibile din această interfață.

Soluția propusă va avea o platformă unificată de management care va permite vizualizarea resurselor hardware, consumul acestora, erori și evenimente, cât și posibilitatea de a se conecta direct la portalul de suport al producătorului pentru deschiderea și gestionarea tichetelor de service (evenimente hardware, evenimente software). Întreaga soluție va avea un singur punct de contact din punct de vedere al asigurării suportului hardware (nodurile de procesare și stocare, switch-uri fizice) și software (virtualizare, management, stocare, switch-uri virtuale) ce va pune la dispoziție atât un număr de contact telefonic cât și un portal unificat în care să apară istoricul evenimentelor de service, starea evenimentelor în desfășurare cât și perioada de garanție și suport a echipamentului. În cadrul portalului vor fi disponibile actualizări ale software-ului ce rulează pe platformă, ghiduri de configurare și administrare, cât și informații despre securizarea platformei. Portalul trebuie să faciliteze interacțiunea cu inginerii de service ai producătorului prin intermediul unor instrumente interactive (chat/WebEx/Teams/Zoom/VoIP).

Soluția propusă va avea o interfață de management unificată care să asigure atât managementul resurselor virtuale (mașini virtuale, grupuri de resurse), managementul infrastructurii fizice, cât și upgrade-ul unitar al soluției (versiuni de software noi, patch-uri, upgrade de firmware, drivere). Pachetul software pentru upgrade va fi unitar (firmware platformă hardware, drivere pentru soluția de virtualizare, hypervisorul ce rulează pe noduri, platforma de management, interfață unică de management a sistemului integrat) testat și validat pentru tot sistemul. Upgrade-ul software se va face online (fără întreruperea funcționalităților mașinilor virtuale) și automatizat (utilizatorul va executa încărcarea pachetului de upgrade, iar sistemul va realiza automat toate operațiile fără intervenția operatorului) fără scoaterea sistemului din producție. În cadrul procesului de update, sistemul trebuie să poată asigura programarea update-ului la o anumită dată și oră pentru a facilita executarea acestuia cu impact redus în producție, în perioadele de încărcare minimă. Din cadrul interfeței de management unitar se va putea face adăugarea de resurse (noduri noi) în cluster cu rebalansarea automată a resurselor pe nodurile noi adăugate. Procesul de înlocuire a disk-urilor va putea fi inițiat din cadrul interfeței unitare de management (GUI), astfel încât acest proces să fie unul intuitiv și simplu de realizat la nivelul administratorului.

Sistemul hyper-convergent propus va include un echipament extern de stocare a datelor, de tip unificat, compatibil și validat pentru funcționare în soluția propusă.

Echipamentul de stocare a datelor de tip unificat trebuie să îndeplinească următoarele cerințe minime:

Controller: Echipamentul trebuie să aibă cel puțin două controlere active prin care se pot scrie și citi datele în mod block (SAN) și în mod file (NAS), redundante, hot-swap; fiecare controller va fi echipat cu minim 2 procesoare de tip Intel Xeon cu cel puțin 24 de nuclee per procesor, la 2.2 GHz.

Arhitectură: sistemul stocare solicitat trebuie să fie de tip all-flash, să folosească protocolul NVMe pentru conectarea drive-urilor flash propuse la controller-e și să suporte medii de stocare NAND NVMe cu rol de medii de stocare persistente pentru date; sistemul trebuie să includă tehnologii "inline" (în timp real) de reducere a datelor prin compresie și deduplicare, activate.

Clasă echipament: midrange / enterprise, cu disponibilitate de 99.9999%

Protocoale suportate pentru accesul la date: Echipamentul oferat trebuie să aibă suport inclus, unificat, pentru: Fibre Channel, NVME/FC, iSCSI, VVols 2.0, SMB 2, 3, NFS v3, 4, 4.1, FTP, SFTP, NVMe/TCP sau RoCE;

Porturi instalate (conectivitate):

Echipamentul oferat trebuie să dispună de cel puțin:

- 8 porturi 10/25 Gbps Ethernet (4 porturi per controller) pentru acces de tip file (SMB, NFS) respectiv block (iSCSI, NVMe/TCP sau RoCE), compatibile cu switch-urile pentru interconectare LAN și SAN;
- 8 porturi 100 Gbps Ethernet (4 porturi per controller) pentru acces de tip block (iSCSI, NVMe/TCP sau RoCE), compatibile cu switch-urile pentru interconectare LAN și SAN;

Echipamentul va include porturi de management 1Gbps Ethernet pe fiecare controller. Echipamentul va permite conectarea directă a serverelor, în mod redundant, atât pe Fibre Channel cât și pe Ethernet.

Memorie Cache (tip RAM): minim 1 TB memorie cache de tip RAM pe sistem, în configurația propusă (min. 512 GB pe fiecare controller).

Nivele RAID suportate: RAID 5 (sau echivalent cu simplă paritate) sau RAID 6 (sau echivalent cu dublă paritate);

Dimensiune maximă file system: Cel puțin 250 TB

Dimensiune maximă LUN: Cel puțin 250 TB

Număr maxim LUN-uri: Cel puțin 15000

Număr host-uri suportate: Cel puțin 1000 host-uri SAN

Medii de stocare instalate:

- pentru stocarea datelor, echipamentul va avea instalată la livrare o capacitate brută de minimum 290 TB folosind cel puțin 19 drive-uri NVMe flash, hot-swap, de aceeași capacitate;
- echipamentul de stocare va fi configurat având cel puțin 210 TiB capacitate de stocare utilă realizată doar pe module flash NVMe, hot-swap, de aceeași capacitate; nu se acceptă drive-uri flash de tip QLC (Quad-Level Cell).

- datele stocate pe drive-urile propuse vor fi protejate printr-o configurație RAID 5 (sau echivalent cu simplă paritate) sau RAID 6 (sau echivalent cu dublă paritate);
- sistemul va include cel puțin un drive hot-spare sau echivalent capacitate de rezervă (hot-spare) de dimensiunea unui drive, distribuită pe toate drive-urile propuse, pe care să se reconstruiască în mod automat datele pierdute în cazul defectării unui drive;

Capacitatea de stocare efectivă:

- Pentru seturi de date brute (necompresate, nededuplicate, necriptate) tip baze de date, mașini virtuale, sistemul de stocare va asigura o capacitate de stocare efectivă, garantată de către ofertant, de cel puțin 800 TiB, în configurația propusă, prin deduplicarea și compresia inline a datelor.
- În cazul neîndeplinirii cerinței minime de capacitate de stocare efectivă, ofertantul va asigura în mod gratuit drive-uri flash adiționale, controllere (dacă este cazul) și toate componentele necesare asigurării capacității de stocare utile efective;

Performanță:

În configurația ofertată echipamentul trebuie să asigure o performanță de cel puțin 200 000 IOPS pentru workload cu 50% / 50% rata de citire / scriere, 50% / 50% random / secvențial, cu dimensiunea block-urilor IO de 32KB, prin protocol NVMe/TCP sau RoCE sau iSCSI. Această performanță trebuie să fie susținută în următoarele condiții:

- Capacitatea alocată și activă minim 50% din totalul disponibil;
- Durata de menținere a parametrilor de minim 24 ore;
- Funcționalități inline de deduplicare și compresie activate pe toate seturile de date;
- Timp de răspuns către servere mai mic sau egal cu 1 ms;

Parametrii vor fi demonstrați printr-un raport certificat de producător pentru configurația propusă.

Extensie capacitate de stocare:

Soluția propusă trebuie să suporte configurarea mai multor sisteme diferite într-un cluster multi-controller (de cel puțin 8 controller-e) în vederea creșterii performanței și capacității de stocare; suport pentru balansarea online a datelor, workload-urilor între sistemele din cluster.

Echipamentul ofertat trebuie să permită upgrade ulterior la cel puțin 350 de module NVMe prin adăugarea de controller-e și sertare de expansiune cu conectare pe NVMe, prin magistrale redundante.

Sistemul va permite o scalabilitate la minimum 5 PB capacitate de stocare totală brută respectiv 20 PB capacitate de stocare efectivă, în configurație maximă.

Funcționalități de management:

Sistemul intern de management și monitorizare al echipamentului de stocare va oferi minimum următoarele facilități:

- Va fi accesibil de la distanță prin interfață grafică web-based HTML 5, CLI, REST API;
- Va dispune de acces securizat SSL;
- Va permite definirea de utilizatori locali având roluri cu permisiuni diferite, precum și suport LDAP pentru integrarea cu sisteme Active Directory sau echivalent;
- Va permite pentru exporturile prin vVols vizualizarea minimum a numelui mașinii virtuale, a capacității provizionate și a capacității ocupate efectiv pe datastore;
- Se va integra cu aplicația de management a mediului virtual permițând provizionarea de capacitate de stocare din aplicația de management a mediului virtual;
- Va include suport pentru accelerarea hardware a operațiunilor ce au loc între hipervizor și sistemul de stocare, prin degrevarea unor procese de la nivelul hipervizorului și preluarea lor la nivelul echipamentului de stocare. Aceasta funcționalitate va permite accelerarea mutării unei mașini virtuale între două volume de date ale hipervizorului și accelerarea efectuării de copii ale mașinilor virtuale;
- Va asigura suport inclus pentru analiza și monitorizarea volumelor alocate către sistemele host. Sistemul de stocare va permite vizualizarea în mod grafic din interfața de management locală a parametrilor de tip lățime de bandă (bandwidth), numărul total de IOPS și timpul de răspuns la nivel de volum. Toate informațiile vor fi disponibile pe o perioadă de minimum un an de zile (în urmă) de la momentul la care se face interogarea;
- Va permite update, upgrade software și hardware al echipamentului de stocare menținând accesul la date, fără întreruperea serviciilor;
- Volumele definite vor putea fi grupate în grupuri de volume asupra cărora se vor putea aplica politici de protecție colective;
- Sistemele host vor putea fi grupate astfel încât un volum să poată fi mapat la un grup de sisteme host configurate în cluster;
- Sistemul va dispune de mecanisme interne inteligente care să analizeze încărcarea din punct de vedere a capacității la nivelul controller-elor, a stării acestora și a limitărilor maxime de resurse ce pot rula pe ele. Astfel, în cazul în care sistemul detectează o anomalie în funcționare (defect hardware, controller offline, capacitate insuficientă), realizează o analiză predictivă a resurselor bazată pe date istorice și prezintă un set de recomandări care va permite migrarea online a volumelor între oricare dintre controller-ele sistemului. Migrarea va putea fi făcută atât asistat cât și manual. La definirea de volume noi, sistemul va lua în calcul datele rezultate din mecanismele interne inteligente și va oferi o propunere de plasare automată a volumului care va lua în calcul toți parametrii menționați pentru o stare și o încărcare optimă a întreg sistemului;

- Suport inclus pentru deduplicarea și compresia inline (în timp real) a datelor pentru volume cu acces prin protocol de tip block (FC, iSCSI) respectiv protocol de tip file (SMB, NFS);
- Va asigura vizualizarea detaliilor despre rata globală de reducere a datelor prin deduplicare și compresie per sistem, per volum sau grup de volume, vizualizarea cantităților de date nereductibile;
- Va asigura definirea unor politici de tip QoS la nivel de volum, grup de volume de date care să asigure cel puțin limitarea lățimii de bandă și a numărului de IOPs;
- Soluția propusă va oferi o platformă unificată de management care va permite vizualizarea resurselor hardware, consumul acestora, erori și evenimente, cât și posibilitatea de a se conecta la portalul de suport al producătorului pentru deschiderea și gestionarea tichetelor de service (evenimente hardware, evenimente software). Producătorul echipamentului de stocare va pune la dispoziție atât un număr de contact telefonic cât și un portal web în care să apară istoricul evenimentelor de service, starea evenimentelor în desfășurare cât și posibilitatea de a deschide unele noi. Tot în cadrul portalului vor fi disponibile actualizări ale software-ului ce rulează pe platforma, ghiduri de configurare și administrare, cât și informații despre garanția soluției și suportul software. Portalul va facilita interacțiunea cu inginerii de service ai producătorului prin intermediul unor instrumente interactive (Chat / WebEx / Skype / Teams / Zoom).

Protecția și replicarea datelor:

Suport inclus pentru a realiza copii complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp (snapshot). Sistemul va permite realizarea de clone ale volumelor existente, bazate pe snapshot-uri, astfel încât acestea să poată fi montate imediat către sistemele host în mod read-write. La rândul lor volumele de tip clonă vor putea avea definite snapshot-uri.

Sistemul trebuie să permită realizarea de snapshot al oricărui snapshot de date. Snapshot-urile trebuie să poată fi accesate atât în mod „read-only”, cât și în mod „read-write”. Se va asigura suport pentru minim 512 de snapshot-uri per volum de date (LUN).

Suport inclus pentru a realiza cel puțin 225 000 de snapshot-uri pentru volumele block și cel puțin 25 000 de snapshot-uri pentru sistemele de fișiere, definite la nivel de sistem de stocare, în configurația ofertată.

Sistemul de stocare trebuie să includă nativ capacitatea de a realiza snapshot-uri read-only și de a le păstra într-un mod imuabil (pe perioada definită de retenție aceste snapshot-uri nu pot fi șterse manual) realizând astfel protecția datelor la ștergerea rea intenționată, atac de tip ransomware.

Suport software inclus pentru replicarea nativă a datelor în mod asincron, la distanță, între echipamente de stocare similare. Replicarea va putea fi parametrizată la nivel de RPO (Recovery Point Objectiv) într-un interval de la 5 minute la 24 ore.

Suport software inclus pentru replicarea nativă a datelor în mod sincron, între echipamente de stocare similare și realizarea clustere metro (Windows, Linux, VMware) care să asigure replicarea sincronă a datelor în mod bidirecțional, permițând accesul simultan în mod read&write la aceleași volume de date din două centre de date aflate la distanță (zero RPO și zero RTO).

Sistemul va permite definirea de politici de protecție aplicabile la nivel de volum (inclusiv volume de tip clonă) și de grupuri de volume, în care să poată fi incluse politicile de realizare a snapshot-urilor și politicile de replicare.

Suport inclus pentru integrarea sistemului de stocare cu soluții de tip server anti-virus pentru scanarea fișierelor vehiculate de serverele NAS, prin protocol CIFS/SMB, astfel încât să asigure identificarea și eliminarea amenințărilor înainte ca acestea să infecteze sistemul ce accesează fișierele stocate.

Sistemul de stocare trebuie să permită acces simultan la nivel de sistem de fișiere atât prin protocol de tip SMB cât și prin NFS cu configurarea drepturilor de acces corespunzătoare. Pentru a preveni accesul neautorizat sau ștergerea accidentală a fișierelor, echipamentul de stocare trebuie să asigure definirea unor politici de retenție la nivel de fișiere pe o perioadă de timp specificată de administratorul uman al resursei respective (Write Once Read Many - file WORM).

Suport inclus pentru protocol NDMP în configurație 3-way pentru asigurarea interconectării cu sisteme de tip librărie de benzi în vederea realizării operațiunilor de backup, cu suport atât pentru backup-uri full cât și incrementale.

Echipamentul de stocare oferit trebuie să includă integrare directă cu echipamentul de realizare și stocare a backup-ului pe disc prin maparea directă a echipamentului de backup la echipamentul de stocare astfel încât procesul de backup al datelor de pe volumele LUN să se realizeze direct în echipamentul de backup.

Licențiere software:

Toate funcționalitățile software solicitate vor fi activate, licențiate perpetuu pe echipamentul oferit, indiferent de capacitatea de stocare prezentă sau viitoare, indiferent de numărul de host-uri ce se vor conecta la echipamentul de stocare.

Sisteme de operare suportate:

Windows Server 2016, 2019 și 2022, Microsoft Hyper-V, VMware ESXi 7.0, 8.0, Red Hat Enterprise Linux 8.x, 9.x, Suse Enterprise Linux 15, Solaris 10, 11 Sparc&x86, HP-UX 11i v3, IBM AIX 7.2, 7.3;

Echipamentul de stocare trebuie să includă licențele necesare accesului sistemelor de operare suportate.

Format:

Rackmountable 19". Echipamentul de stocare va include șine pentru montarea în rack și va ocupa maxim 2U.

Securitate și conformitate:

Suport inclus pentru criptarea datelor pe echipamentul de stocare, la nivel de controller sau disc, cu management intern respectiv extern al cheilor de criptare.

Echipamentul oferit trebuie să fie certificat și validat conform cu standardele: SEC rule 17a-4(f), FIPS 140-2 level 2, TLS 1.2, TLS 1.1, EN 62368-1:2014 +A11:2017, EN

62311:2008, EN 62479:2010, EN 55035:2017 +A11:2020, EN 55032:2015 +A11:2020, EN 61000-3-2:2014, EN 61000-3-3:2013, RoHS EN IEC 63000:2018.

Sistemul hyper-convergent propus va include o soluție software și hardware pentru backup ce trebuie să îndeplinească următoarele cerințe minime:

- Soluția trebuie să fie bazată pe aplicații și sisteme hardware ce vor asigura rularea unor procese automate de salvare și restaurare a datelor, protecția directă a aplicațiilor, monitorizarea politicilor de protecție, eficientizarea acestora prin politici avansate de deduplicare și compresie, replicarea mașinilor virtuale, integrarea cu medii de arhivare pentru păstrarea datelor pe termen mediu și lung.
- Soluția ofertată va include un sistem specializat de backup de tip appliance hardware și un sistem specializat de backup de tip appliance software virtual, având ficționalități similare, certificate de producător pentru protecția și securitatea datelor.
- Sistemul de tip appliance virtual va include suport pentru instalarea în medii virtuale VMware, KVM, Hyper-V.
- Sistemul de tip appliance virtual trebuie să susțină deduplicarea globală a datelor cu cel puțin 90 de procese paralele de salvare respectiv 50 de procese de restaurare, utilizând interfețe multiple de rețea, fără a afecta integritatea datelor.
- Sistemul de tip appliance hardware trebuie să susțină deduplicarea globală a datelor cu cel puțin 250 de procese paralele de salvare respectiv 75 de procese de restaurare, utilizând interfețe multiple de rețea fără a afecta integritatea datelor.
- Sistemul de tip appliance software va permite definirea unei capacități utile de stocare de min. 20 TB folosind discuri virtuale ce vor fi provizionate din infrastructura de stocare a datelor existentă la Autoritatea Contractantă.
- Sistemul de tip appliance hardware va avea o capacitate de stocare utilă de min. 200 TB în urma configurării în RAID 6, având cel puțin două discuri hot-spare sau echivalent capacitate hot-spare, cu posibilitatea de creștere a capacității de stocare prin adăugarea de discuri.
- Procesul de deduplicare a datelor trebuie să se desfășoare “inline” (în timp real) fără stocare temporară și fără sisteme de calcul intermediare între sursă și destinație, utilizând un algoritm global de deduplicare, indiferent de sursa datelor și protocoalele de salvare a datelor.
- Sistemele de tip appliance hardware, software oferite trebuie să asigure susținerea proceselor de salvare și restaurare de date prin protocoale multiple: minim CIFS, NFS, DDBOOST sau CATALYST sau echivalent.
- Pentru extinderea capacității de stocare, appliance-urile hardware și software de backup trebuie să se poată integra cu sisteme de stocare de arhivare pentru păstrarea datelor pe termen mediu și lung, prin mecanisme de tiering

programat, pentru mutarea și păstrarea segmentelor unice de date deduplicate în cazul aplicării unor politici adiționale de retenție.

- Administratorul soluției va putea rula simultan mai multe mașini virtuale utilizând exclusiv resurse ale sistemelor appliance dedicate protecției datelor cu posibilitatea de a le transfera către mediul de producție fără oprirea acestora sau acționarea unui proces separat de restaurare.
- Soluția ofertată trebuie să includă capabilități de securizare a datelor salvate și prin criptarea și sigilarea acestora conform politicilor de protecție și a perioadelor de retenție definite de utilizator.
- Datele deduplicate și compresate scrise pe sistemele de backup trebuie să poată fi protejate prin mecanisme de tip WORM pentru securizarea acestora față de eventualele acțiuni de ștergere ale unor intervenții neautorizate. Implementarea acestei funcționalități trebuie să fie realizată în interiorul soluției de stocare (fără a necesita alte soluții adiționale) și să fie certificată SEC Rule 17a-4.
- Sistemele de backup trebuie să susțină mecanisme de evaluare și corecție preventivă a datelor salvate, a sistemelor de fișiere, prin care asigură verificarea continuă a segmentelor de date deduplicate și disponibilitatea de restaurare granulară sau completă a fiecărui proces de salvare finalizat cu succes.
- Sistemele de tip appliance software, hardware de backup oferite trebuie să includă mecanisme de protecție de tip snapshot și funcționalități avansate de securitate, astfel încât, pentru comenzi de modificare a datelor sistemelor să fie necesară o dublă autentificare care să confirme operațiunea (de ex. ștergerea sistemului de fișiere, modificarea parametrilor de timp).
- Procesele de expirare și ștergere a datelor scrise pe sistemele de backup trebuie să se facă în mod automat permițând proceselor de salvare și restaurare să se desfășoare fără oprire.
- Sistemele de tip appliance hardware, software vor include funcționalitatea de replicare nativă a datelor între echipamente fizice și virtuale diferite, transferând doar segmentele de date unice.
- Echipamentul hardware va include conectivitate pentru host-uri:
 - minim 8 porturi 10/25 Gigabit Ethernet SFP28, dispuse pe cel puțin 2 adaptoare de rețea distincte;
- Transferul datelor de la sursa datelor la echipamentul hardware va putea utiliza toate resursele de rețea disponibile în echipament, folosind conexiuni multiple prin mecanisme de tip load balancing și fail-over.
- Viteza de backup a echipamentului hardware va asigura un throughput min. 60 TB/oră
- Echipamentul hardware trebuie să includă o capacitate de stocare de tip SSD, minim 2x3.84TB, destinată exclusiv memorării și accesării rapide a indecșilor procesului de deduplicare indiferent de capacitatea utilizată.

- Capacitatea logică de stocare suportată în interiorul echipamentului hardware oferat: 11 PB
- Echipamentul hardware oferat trebuie să fie capabil să suporte cerințele de protecție cibernetică, cu funcții anti-ransomware și airgap/seif.
- Echipamentul hardware trebuie să utilizeze funcții de criptare conforme cu FIPS 140-2 și un modul hardware dedicat compresiei datelor fără utilizarea resursele de procesare ale sistemului.
- Echipamentul hardware oferat trebuie să fie certificat și conform cu standardele: FIPS 140-2 Level 1, SEC 17a-4, EN55032, EN55035, EN 61000-3, RoHS EN IEC 63000:2018
- Format rackmountable 19”.
- Echipamentul hardware va dispune de surse de alimentare electrică redundante, hot-swap.

Sistemul hyper-convergent propus trebuie să ofere acces la o platformă software disponibilă în Cloud, accesibilă de oriunde, capabilă să preia date de telemetrie de la toate componentele sistemelor HCI în vederea monitorizării, raportării și forecast-ării resurselor cluster-elor HCI. Printre funcționalitățile ce trebuie să fie oferite de aceasta platformă, pe baza datelor de telemetrie, se numără:

- monitorizarea și raportarea centralizată pentru toate cluster-ele HCI instalate în mediul clientului,
- managementul centralizat al mai multor cluster-e HCI ce va permite update-area sincronizată a software-ului pentru toate acestea,
- agregarea informațiilor și alertelor de la toate componentele hardware și software ale cluster-ului HCI și calcularea unui scor al disponibilității componentelor / resurselor cluster-ului (health score), pentru o mai ușoară monitorizare a întregului mediu HCI și a fiecărei componente în parte;
- alertarea asupra posibilelor probleme și prezentarea de recomandări de rezolvare prin intermediul articolelor de tip Knowledge Base relevante, disponibile de la producător;
- prognozarea resurselor necesare în perioada următoare, pentru o planificare facilă a capacității viitoare (de ex. când spațiul de stocare urmează să ajungă la utilizare maximă),
- monitorizarea avansată a performanței întregului sistem, cu detectarea anomaliilor și corelarea încărcării / utilizării diferitelor componente (CPU, memory, disk, networking) în aceeași fereastră de timp, în vederea diagnosticării rapide a problemelor;
- furnizarea de recomandări de configurare pentru atingerea performanțelor optime.

Pentru respectarea normelor de securitate sistemul hyper-convergent propus trebuie să fie certificat EAL 2+.

3.7.2. Platforma unificată de securitate

Soluția propusă va include:

- O soluție ce va fi configurată în cluster de tip software appliance de NGFW, licențiat pentru minim 8vCPU pentru fiecare nod și care să permită următoarele:
 - Implementarea unui cluster în mod activ-pasiv cu failover rapid
 - Sistemul va fi livrat cu următoarele licențe: IPS, Application Control, Antivirus, Webfiltering, Antispam

3.7.3. Platforma de balansare a traficului de aplicație

Soluția va include un set complet de cel puțin două dispozitive care funcționează în cluster pentru a asigura disponibilitate ridicată a serviciilor de aplicație. Aceasta va oferi echilibrare transparentă a aplicațiilor, accelerare și servicii de protecție. Platforma trebuie să îndeplinească cel puțin următoarele cerințe funcționale specifice:

- Minimum 4 conectori 1Gbps RJ45 cupru;
- Minimum 4 interfețe 10Gbps SFP+, toate echipate cu optic pentru distanță scurtă, multimode;
- Stocare internă de cel puțin 450GB;
- Memorie RAM de minimum 64GB;
- Sursă de alimentare AC redundantă, cu posibilitatea de înlocuire fără întreruperea funcționării;
- Performanță de procesare trafic de minimum 30Gbps la L4/7 per dispozitiv;
- Minimum 20Gbps performanță pentru compresie hardware a traficului;
- Minimum 20Gbps performanță pentru criptarea hardware a traficului;
- Minimum 1.200.000 cereri pe secundă la nivel 7;
- Minimum 14.000 tranzacții SSL pe secundă folosind ECC și minimum 14.000 tranzacții SSL pe secundă folosind RSA;
- Posibilitatea creșterii performanței prin module software adiționale;
- Distribuția încărcării de procesare pentru protocoalele TCP și UDP;
- Suport pentru utilizarea SNAT;
- Posibilitatea monitorizării serverelor aplicației prin mecanisme de verificare pentru protocoale standard;
- Suport pentru ToS, QoS (marcare/păstrare/imitare).

Load Balancer:

- Suport pentru scripturi personalizate pentru monitorizarea disponibilității serviciilor;
- Optimizare TCP pentru fiecare client conectat, independent;
- Suport pentru compresie și caching;
- Ogândirea sesiunilor și conexiunilor SSL între mai multe dispozitive ADC;

- Ajustare dinamică și configurare a parametrilor TCP;
- Posibilitatea conectării la unelte terțe de monitorizare prin API deschis;
- Jurnalizare detaliată a tuturor părților comunicării per aplicație;
- Capacitatea de a gestiona chei de 4K (4096 biți);
- Suport pentru mai mult de 19 metode de echilibrare a sarcinii;
- Suport pentru filtrare de pachete;
- Echilibrare bazată pe raport cu persistență CARP;
- Suport pentru redimensionarea dinamică a pachetelor TLS;
- Mod automat TCP Nagle;
- Ajustare automată a buffer-ului TCP;
- Posibilitatea verificării disponibilității sistemului de a primi comenzi prin CLI/REST API;
- Posibilitatea rulării testelor/sondelor din interfața web;
- Suport pentru TLS Session Hash și Master Secret Extension (RFC 7627);
- Suport pentru protocolul MQTT;
- Suport pentru TLS 1.3;
- Proxy HTTP/2 complet;
- Limbaj de scripting personalizat cu suport HTTP/2;
- Posibilitatea de a converti cereri HTTP/3 de la clienți în HTTP/2 și HTTP/1 pe partea de backend;
- Suport pentru HTTP/3.

WAF (Web Application Firewall)

- Protecție împotriva atacurilor la nivelul aplicației (L7);
- Detectarea și atenuarea atacurilor DoS L7;
- Detectarea și atenuarea atacurilor brute-force;
- Detectarea și atenuarea atacurilor pe URL-uri complexe;
- Detectarea și atenuarea atacurilor OWASP TOP 10;
- Firewall pentru XML;
- Protecție pentru apeluri JSON și AJAX;
- Validarea credentialelor și fluxului aplicației;
- Detectarea și atenuarea roboților și activităților non-umane, inclusiv headless bots;
- Protecție împotriva scurgerilor de date sensibile prin blocare și mascarea informațiilor;
- Corelare automată a atacurilor multiple într-un singur incident;
- Suport pentru politici de securitate pozitive și negative;
- Suport pentru detectarea și blocarea atacatorilor pe baza geolocației;
- Suport pentru scanarea fișierelor prin ICAP;
- Protecție la nivel de aplicație pentru protocoalele SMTP și FTP;
- Conformitate cu PCI-DSS, HIPAA, SOX, Basel II;
- Politici predefinite de securitate pentru Microsoft Outlook Web Access și Microsoft SharePoint;
- Posibilitatea aplicării unor politici diferite de securitate în funcție de adresă IP, nume

de domeniu și URI;

- Opțiune de import a rezultatelor testelor de penetrare web;
- Suport pentru filtrarea și aplicarea politicilor pentru comunicații WebSocket;
- Blocarea adreselor IP care încalcă repetitiv politica de securitate direct în componente hardware dedicate;
- Suport pentru generarea unei amprente unice a dispozitivului/clientului;
- Suport pentru politici de securitate pe mai multe niveluri;
- Suport pentru aplicarea globală a setărilor și funcțiilor de securitate pentru toate politicile;
- Evaluarea reputației clientului pentru construirea automată a politicilor de securitate;
- Suport pentru aplicații Single Page Applications (SPA);
- Detectare automată a tipului de server backend;
- Suport pentru parsarea parametrilor JSON;
- Configurare automată a parametrilor pentru protecția L7 DDoS;
- Mod „learning” (fără aplicare) pentru anumite domenii;
- Posibilitatea dezactivării semnăturilor specifice pentru URL, antete HTTP și parametri;
- Suport pentru implementare pe porturi SPAN/Mirror;
- Opțiune de criptare a datelor sensibile pe partea clientului fără a modifica aplicația protejată;
- Detectarea modificărilor automate ale datelor din formulare pe partea clientului fără modificarea aplicației protejate;
- Suport pentru aplicații bazate pe GraphQL;
- Opțiune pentru reducerea falselor pozitive folosind un model ML offline;
- Detectarea și atenuarea atacurilor SSRF (Server-Side Request Forgery);
- Posibilitatea exportării completei politici WAF în format JSON;
- Suport pentru serializare OpenAPI pentru parametri Array, Style, Explode și Path;
- Bază de date actualizată cu IP-uri malițioase;
- Inteligență actualizată despre campanii active de atac.

DNS

- Protecție adaptivă împotriva atacurilor DDoS - detecție și atenuare bazată pe AI/ML a atacurilor volumetrice la nivelurile 3, 4 și 7;
- Protecție împotriva atacurilor de tip amplificare DNS - reguli de firewall avansate pentru atenuarea amenințărilor DDoS specifice DNS;
- Funcții de accelerare DNS - rezolvarea DNS în memoria dispozitivului pentru răspunsuri mai rapide către clienți;
- Configurare profil caching DNS - setări detaliate pentru comportamentul cache-ului;
- Firewall DNS - protecție împotriva DDoS, cache poisoning și alte atacuri DNS;
- Suport pentru DNSSEC;
- Echilibrare de sarcină pentru cererile DNS;
- Global Server Load Balancing (GSLB) avansat - rutare optimizată a cererilor între centre de date distribuite geografic.

Componentă virtuală

Se va asigura în cadrul proiectului un appliance software virtual de la același producător ce va rula în Cloud-ul Privat Guvernamental pentru interconectarea platformei de balansare a traficului de aplicație între mediul de producție cu mediul de disaster recovery.

3.8. COMPONENTELE SOFTWARE

Cerințele minime pentru componentele software de mai jos sunt descrise în cadrul capitolele următoare:

Nr. crt.	DESCRIERE
1	Componenta Portal
2	Soluția de management documente
3	Sistemul de gestiune a bazelor de date
4	Componenta de Business Intelligence
5	Componenta de interoperabilitate
6	Componenta de API management
7	Platforma pentru administrarea identității utilizatorilor
8	Componenta de securizare a accesului privilegiat
9	Monitorizare date, sisteme și aplicații
10	Soluție de disaster recovery
11	Componenta SIEM
12	Soluția concentrator VPN

3.8.1. Componenta Portal

Portalul din cadrul PNI reprezintă componenta prin intermediul căreia se va realiza punctul unic administrativ de acces către furnizorii de servicii de eguvernare și furnizorii de registre de baza.

Portalul va include următoarele secțiuni principale împreună cu funcționalitățile specifice asociate:

- Secțiune publică - de informare;
- Secțiune privată pentru operatorii din cadrul autorităților competente;
- Secțiune privată pentru administratorii registrelor;
- Secțiune privată pentru administratorii din cadrul autorităților competente;

Portalul va fi realizat pe o platformă flexibilă și scalabilă, capabilă să asigure un grad înalt de standardizare și reutilizare a resurselor și serviciilor, cu acces rapid la aplicații.

Portalul trebuie să permită actualizarea rapidă și facilă a conținutului, acțiune care se va realiza fără aportul specializat al unor resurse de dezvoltare, distribuirea conținutului.

Soluția Portal trebuie să asigure următoarele funcționalități minime:

- unic punct de acces către aplicațiile din sistem și către rapoartele specifice;
- include toate instrumentele necesare pentru construirea și administrarea unui portal complex, structurat pe mai multe niveluri de acces;
- include funcționalități specifice de administrare de conținut pe bază de partajare, colaborare și automatizare de procese;
- asigură suport pentru apelul la distanță a portlet folosind standardul Web Services for Remote Portlets (WSRP);
- asigură autentificarea unică a utilizatorilor prin intermediul rolurilor și privilegiilor ce vor fi definite și acordate fiecărui utilizator în parte;
- interfața prezentată utilizatorului după autentificare trebuie să prezinte acces doar la informațiile/paginile web și aplicațiile la care utilizatorul are drept de utilizare conform cu rolul său în cadrul sistemului;
- conținutul accesat prin Portal trebuie să fie automat ajustat, pe baza rolurilor predefinite ale utilizatorilor în funcție de drepturile acordate;
- interfața oferită utilizatorilor de Portal va fi în limba română, cu stil de organizare unitar, indiferent de utilizator și de drepturile alocate acestuia;
- asigură efectuarea de căutări agregate folosind mai multe metode de căutare pentru interogarea și regăsirea informațiilor existente în sistem;
- asigură crearea facilă de noi pagini în Portal, pentru a menține în permanență actualizată informația din Portal;
- include mai multe stiluri predefinite de organizare și prezentare a paginilor de Portal, iar dintre aceste stiluri se va putea selecta un stil de prezentare specific Beneficiarului;
- utilizatorii trebuie să aibă posibilitatea de a particulariza paginile la care au acces la nivel de conținut, poziționare sau stil, în funcție de drepturile de personalizare acordate;
- administratorii de portal trebuie să poată controla drepturile utilizatorilor de a particulariza propriile pagini, funcție de rolul acestora, sau funcție de regulile definite;
- soluția Portal trebuie să permită utilizarea profilelor de utilizatori, administratorul putând seta astfel preferințele atât la nivel de profil, grup cât și la nivel de utilizator. Aceste preferințe specifică atât accesul pe care îl vor avea la diverse porțiuni ale portalului cât și drepturile asupra acestor zone;
- utilizatorii și drepturile de acces sunt stocate și gestionate în cadrul unui sistem standard de autentificare unică. Accesul la oricare din aplicațiile componente ale soluției se va face utilizând o autentificare unică la începutul sesiunii de lucru. La autentificare, soluția de portal trebuie să analizeze permanent nivelul de risc aferent autentificării utilizatorilor utilizând factori de risc ca: locația geografică, echipamentul utilizat pentru autentificare și comportamentul utilizatorului. Pe baza acestei analize, soluția va lua decizii automate care trebuie să includă cel puțin:

- permite / refuză accesul utilizatorului,
 - transferă informațiile și operațiunea de autentificare la un operator pentru analiză detaliată,
 - decizie privind acceptul/refuzul accesului sau solicită un element suplimentar de autentificare.
- de asemenea, soluția trebuie să permită configurarea de excepții pe baza cărora regulile specifice analizei de risc să nu fie aplicate pentru anumiți utilizatori / categorii de utilizatori;
 - comunicarea utilizatorilor cu soluția portal (pentru utilizare sau administrare) trebuie să poată fi făcută în deplina siguranță din punct de vedere al comunicației și al accesului la servicii (SSL);
 - soluția Portal trebuie să permită delogarea automată - să ofere un mecanism prin care un utilizator să fie delogat în cazul în care nu a mai efectuat nici o tranzacție într-o perioadă de timp (interval ce trebuie să poată fi setat de administrator);
 - soluția Portal trebuie să ofere opțiuni de a defini perioade de timp în care o resursă din Portal este disponibilă. Dacă accesul se efectuează în această perioadă și utilizatorul are drepturi de acces, atunci acestuia i se va permite accesul. Dacă accesul se efectuează în afara perioadei stabilite, atunci accesul va fi blocat, chiar dacă utilizatorul are drepturi de acces pentru resursa respectivă;
 - să suporte structuri ierarhice de navigare arborescentă pentru documente;
 - să fie flexibil din punct de vedere al clienților de tip browser, al sistemelor de operare și al suportului pentru bazele de date;
 - să asigure administrarea prin intermediul unui browser web și să suporte delegarea administrării pentru controlul accesului;
 - dezvoltarea portalului să se facă ușor, respectând standardele în domeniu. Pentru această soluție trebuie să ofere API-uri (Application Programming Interfaces) bine definite pentru integrarea cu aplicațiile existente, să ofere posibilitatea utilizării serviciilor web pentru a expune date și funcționalități;
 - să ofere posibilitatea de a implementa portalul într-un mediu cluster, având posibilitatea de a realiza balansarea încărcării;
 - să ofere capabilități de preluare a utilizatorilor pe un alt nod, în cazul unei căderi hardware (fail over);
 - să ofere mecanisme de caching pentru paginile mai des utilizate pentru performanțe ridicate;
 - soluția Portal trebuie să permită realizarea de rapoarte analitice.

3.8.2. Soluția de management documente

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

- sistemul va fi licențiat perpetuu și trebuie să ofere performanță optimă pentru minim 50 de utilizatori interni și minim 3.000 de utilizatori externi;
- toate documentele și înregistrările trebuie să fie integrate dintr-un depozit central (Repository);
- aplicația trebuie să fie proiectată într-o arhitectura pe mai multe nivele;
- componenta „Server” trebuie să poată fi implementată pe oricare din următoarele platforme: Microsoft Windows, Linux sau similar;
- pentru a putea fi accesată de pe diferite dispozitive, soluția trebuie să ofere mai multe tipuri de componentă de tip „Client”:
 - o client „web” - care să ruleze cu aceleași funcționalități pe oricare din browserele uzuale, cum ar fi: Microsoft Edge, Mozilla Firefox, Google Chrome, Safari și să fie optimizat pentru afișarea pe dispozitive mobile;
 - o client „mobile” de tip PWA (Progressive Web Application), nativ sau hibrid pentru sisteme de operare ANDROID și iOS, componentă pentru care nivelul de acces la soluție va fi de tip READ;
- suport pentru integrarea cu sistemul de e-mail, inclusiv a documentelor atașate la e-mail;
- sistemul trebuie să ofere suport pentru integrarea cu aplicațiile Microsoft Office;
- sistem independent din punct de vedere tehnologic în conformitate cu standardele sistemelor deschise, pentru a se conecta eficient cu alte sisteme informatice și pentru a partaja eficient informațiile și documentele necesare: sistemul trebuie să aibă o interfață de programare a aplicațiilor (Restful API) pentru integrarea cu alte sisteme informaționale;
- pentru realizarea de personalizări sau pentru integrarea cu alte aplicații externe, soluția trebuie să pună la dispoziție un Restful API (Application Program Interface) detaliat și bine documentat (Ex. Swagger);
- aplicația va putea utiliza drept layer de persistență relațional cel puțin următoarele baze de date: Oracle Database, Microsoft SQL Server, PostgreSQL, MySQL, MariaDB;
- interfața de interoperabilitate Restful va fi independentă de Fluxurile de lucru și va aplica constrângerile formularelor de colectare de date;
- aplicația trebuie să permită notificarea prin e-mail referitor la apariția unei cereri și va conduce utilizatorul automat în pagina unde acesta poate aproba sau refuza această cerere;
- interfața trebuie să fie prietenoasă și customizată în funcție de tipul de utilizator care accesează platforma;
- caracterele românești să fie suportate pentru toate ecranele, meniurile, mesajele de eroare, textele de ajutor online, rapoartele și datele;
- toate datele introduse să fie validate în timp real;
- aplicația trebuie să ofere o interfață comună pentru utilizatori care să aibă același „aspect și impresie” pentru toate modulele din cadrul platformei;
- aplicația va putea fi extinsă cu fluxuri, formulare de introducere de date, rapoarte operaționale și tablouri de bord;

- aplicația să afișeze o pagină de start caracteristică utilizatorului autentificat care va include informații de interes pentru acesta inclusiv tablouri de bord;
- aplicația trebuie să permită definirea de noi fluxuri conform nevoilor speciale ale beneficiarului, precum și acordarea drepturilor de accesare pentru utilizatori și grupuri;
- aplicația trebuie să permită definirea și gestionarea de noi entități de date cu nume intern, etichetă, tip de date, lungime, precizie, vizibilitate în listă, valoare implicită, opțiuni formulă de calcul, asigurând totodată persistența noii entități de date în baza de date;
- aplicația trebuie să permită definirea interfeței utilizator pentru noi entități de date (formulare), vizualizare listă, adăugare înregistrare nouă, editare, ștergere;
- interfața sistemului va fi disponibilă în limba română;
- canalele de comunicație pe care circula documentele și informațiile trebuie să fie securizate utilizând protocoalele SSL și HTTPS;
- soluția se va integra cu LDAP, OpenID, OAUTH2, SAML etc. pentru autentificarea și managementul centralizat al utilizatorilor;
- aplicația trebuie să permită resetarea parolei pentru utilizatori;
- aplicația trebuie să permită gestionarea numărului de încercări pentru introducerea greșită a parolei;
- sistemul trebuie să permită integrarea cu componente software pentru scanare și captarea documentelor;
- modulul va include funcționalități încorporate pentru gestionarea de calendare pentru planificarea sarcinilor;
- sistemul trebuie să ofere suport pentru semnarea digitală a documentelor portabile pdf cu ajutorul certificatelor calificate stocate pe USB Token sau din cloud, direct din interfața cu utilizatorul a componentei, și să permită arhivarea adecvată a acestor documente semnate în conformitate cu legile în vigoare;
- aplicația trebuie să blocheze automat contul utilizatorului după introducerea numărului maxim de încercări (parolă greșită) pentru autentificare. Administratorul trebuie să aibă posibilitatea de a scoate utilizatorii din lista de blocare și de a seta numărul de încercări la care se va bloca accesul, precum și timpul pentru care utilizatorul va fi blocat;
- aplicația să nu permită schimbarea datelor prin alte metode decât editarea autorizată;
- aplicația să nu permită utilizatorilor obișnuiți accesul la datele din baza de date decât prin intermediul funcțiilor incluse în sistemul informatic;
- în caz de avarii, trebuie să existe înregistrate informații de diagnosticare pentru a ajuta la identificarea și soluționarea problemei. Toate modulele funcționale trebuie să populeze un jurnal centralizat (bază de date) disponibil pentru administratori. Administratorul trebuie să poată configura nivelul înregistrării: urmărire, depanare, informații, avertizare, eroare (trace, debug, info, warn, error sau fatal), instalarea să se facă în mod containerizat (Docker sau similar);
- sistemul trebuie să permită auditarea utilizatorilor pe toate tranzacțiile din sistem, de exemplu, fiecare comandă care este efectuată într-un caz/acțiune trebuie înregistrată, specificând cine și când a actualizat documentul și cu păstrarea tuturor versiunilor unui

formular electronic. Toate măsurile de securitate trebuie implementate în cadrul sistemului pentru a preveni accesul accidental sau deliberat neautorizat la datele conținute în sistem;

- soluția trebuie să asigure capacitatea de restabilire în urma dezastrelor (asigurarea securității fizice și logice) ca parte componentă a planului de implementare.

Modul de gestionare a documentelor

Prin acest modul se asigură gestionarea documentelor în format electronic astfel, acesta trebuie să dispună de următoarele caracteristici:

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

- înregistrarea directă a e-mailurilor sau a documentelor atașate la e-mailuri;
 - înregistrarea documentelor prin anexare la dosar / caz;
 - înregistrarea documentelor prin anexare la alte documente electronice structurate (formulare) înregistrate;
- trebuie să permită definirea și validarea metadatelor obligatorii într-o etapă din fluxul de lucru;
- trebuie să permită organizarea documentelor într-o structură intuitivă. Această organizare va fi prezentată într-o structură similară dosarelor. Documentele trebuie să poată fi organizate în structuri care să simuleze modalitatea reală de organizare în dosare;
- trebuie să ofere posibilitatea de organizare a documentelor pe dosare;
- trebuie să permită definirea de “liste filtrate” prin specificarea parametrilor utilizați la filtrare (exemplu: documente de un anumit tip, cu o anumită valoare într-un câmp de indexare sau create de un anumit utilizator sau free-text);
- “Listele filtrate” trebuie să fie specifice numai unui anumit utilizator și pot fi numite sugestiv, utilizatorii își vor putea crea “Listele filtrate” și își vor putea configura coloanele de căutare;
- trebuie să ofere posibilitatea stocării documentelor într-un spațiu centralizat și organizat și posibilitatea de a asocia metadata pentru fiecare document în parte;
- trebuie să permită administratorilor definirea volumului de stocare a documentelor (locația fizică în care vor fi salvate documentele în sistem);
- trebuie să permită administratorului configurarea atributelor (câmpuri de date) fiecărui tip de document;
- trebuie să permită operații multiple executate asupra documentelor:
 - versionarea automată a documentelor, permițând păstrarea tuturor versiunilor prin care trece un document;
 - etichetarea fiecărei versiuni, pentru a permite utilizatorilor să identifice facil versiunea căutată;
 - indexarea automată a documentelor;
- în ceea ce privește prelucrarea documentelor pe tipuri de documente și metadata specifice acestor tipuri, modulul trebuie să permită:
 - arhivarea electronică a documentelor;
 - definirea tipurilor de documente permise pentru fiecare flux de lucru;
 - predefinirea fluxurilor de lucru pentru orice tip de document;
 - indexarea automată a documentelor;
- trebuie să permită suport pentru ciclul de viață al unui document (crearea, modificarea, validarea, aprobarea etc). În funcție de starea unui document sunt disponibile spre utilizare diferite acțiuni asupra documentelor;
- trebuie să permită urmărirea și trasabilitatea modificărilor efectuate pe un document;
- trebuie să permită versionarea documentelor. 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;

- în ceea ce privește căutarea, platforma trebuie să asigure:
 - o căutarea documentelor inclusiv după textul conținut cel puțin pentru: documentele scanate utilizând OCR, fișiere Office (Word, Excel), fișiere PDF și emailuri;
 - o salvarea căutărilor ad-hoc pe parcursul unei sesiuni de lucru pentru utilizare ulterioară;
 - o rafinarea rezultatelor unei căutări prin filtrări și ordonări suplimentare operate doar asupra rezultatelor căutărilor;
 - o căutarea rapidă după valorile din oricare câmp de indexare (metadată), după titlul documentului și după conținutul acestuia (full text);
 - o să realizeze un “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;
 - o exportarea listei de dosare sau documente rezultată în urma operației de căutare, în formate standard, cum ar fi csv sau excel;
 - o definirea de câmpuri care să fie văzute în lista de rezultate precum și ordinea acestora, va permite ordonarea rapidă a rezultatelor după orice câmp;
 - o definirea de “liste filtrate” de documente, vizibile pentru utilizator, prin specificarea parametrilor utilizați la filtrare (exemplu: documente de un anumit tip, create de un anumit utilizator) și a modului de afișare a rezultatelor;
- trebuie să dispună de un cadru integrat de colaborare pe documente prin scrierea de mesaje de colaborare pe document adresate anumitor utilizatori și păstrarea istoricului.
- trebuie să permită integrarea cu alte sisteme informatice, astfel încât să schimbe informații cu acestea sub formă de documente. Această funcționalitate privește (și) interogarea (la nevoie a) arhivelor de către organizații externe.
- trebuie să dispună de integrare cu aplicații Microsoft Office (în vederea asigurării compatibilizării cu sistemele utilizate în prezent de Achizitor), astfel încât să permită:
 - o editarea și/sau salvarea documentelor direct pe server;
 - o pre-vizualizarea (preview) a documentelor direct în interfață, fără să fie nevoie să se deschidă documentele în aplicațiile native asociate, pentru toate tipurile uzuale (PDF, imagine, Word, Excel, Powerpoint etc.);
 - o salvarea din aplicațiile Word și Excel direct în depozitul de documente;
 - o definirea șabloanelor direct în aplicația Microsoft Word. Astfel, orice document existent în format Word va putea fi transformat în șablon, prin definirea zonelor în care vor fi precompletate valorile din metadate;
 - o funcționalitatea de tip „merge” a datelor introduse în formularele structurate cu șabloanele Word;
 - o conversia direct din aplicație a fișierelor Word în fișiere pdf;

- salvarea automată a e-mail-urilor și a atașamentelor în depozitele de stocare a documentelor, cu preluarea automată a câmpurilor de indexare specifice e-mail-urilor: expeditor, recipient, subiect și conținut e-mail;
- trimiterea prin intermediul motorului de flux de lucru notificări de tip email, sms sau nativ în care utilizatorul să poată accesa direct din corpul mesajului de email:
 - documentul aflat pe flux;
 - task-urile de flux de lucru specifice etapei în care se află documentul.
- trebuie să permită transmiterea prin email a documentelor sau a unui link către documentele stocate în depozitul de documente al soluției ("repository");
- trebuie să includă un modul de captură a documentelor;
- trebuie să includă un modul de management de fluxuri de lucru cu documentele;
- trebuie să asigure o securitate ridicată în ceea ce privește accesul la documente, astfel:
 - accesul la documentele gestionate este posibil exclusiv prin intermediul aplicației client și nu prin file-sharing;
 - permisiunile sunt: vizualizare date, editare date, ștergere și de modificare;
 - drepturile de acces se pot asocia la nivel de dosar / caz, utilizând utilizatori și grupuri de utilizatori;
- trebuie să ofere o consolă administrativă, punând la dispoziția administratorilor de sistem o interfață prietenoasă pentru administrare;
- trebuie să ofere posibilitatea creării structurii de date, utilizând o interfață grafică, astfel să permită:
 - configurarea facilă, direct în aplicația de configurare/administrare, la nivel de atribut pentru cel puțin următoarele caracteristici: eticheta afișată utilizatorilor, tipul de date permis (text, număr, data calendaristică, logic = adevărat sau fals), lungimea permisă, valoare implicită (exemplu: utilizator curent, data curentă), lista de valori, formula de calcul funcție de alte metadata;
 - definirea de noi formulare, liste, entități organizatorice, date, relații părinte-copil, relații cu subpagini mapate pe alte tipuri de documente, pe care să le poată publica direct în meniul aplicației pentru utilizatori;
 - administrarea șabloanelor;
- trebuie să permită aflarea numărului de documente gestionat de platformă;
- trebuie să ofere posibilitatea de a monitoriza și notifica evenimentele astfel:
 - monitorizarea fluxurilor de lucru active;
 - generarea de alerte și notificări din fluxuri de lucru;
 - monitorizarea și generarea de alerte pentru fluxurile de lucru care nu sunt executate în numărul de zile stabilit;
 - notificarea utilizatorilor privind modificările ce apar în sistem: a fost creat un nou document, documentul a ajuns într-un nou stadiu etc.
 - notificarea pe e-mail despre o sarcină de efectuat sau neefectuată;
- trebuie să permită auditarea operațiunilor de login, logout, acces la dosare. Informațiile de audit vor conține inclusiv data, ora, utilizatorul și acțiunea efectuată;

- trebuie să permită păstrarea istoricului activității prin intermediul configurărilor aferente proceselor precum introducerea documentelor, aprobări, printări etc;
- trebuie să fie de tip enterprise și să poată fi instalată pe cel puțin unul din sistemele de operare Linux, Windows și Unix;
- trebuie să permită conversia fișierelor Word și a formularelor de introducere de date în fișiere pdf;
- trebuie să permită semnarea electronică a documentelor de tip pdf direct din aplicație, cu semnătură stocată pe token USB sau din cloud;
- trebuie să permită trimiterea documentelor pdf spre semnare, prin intermediul fluxurilor de lucru, către liste de utilizatori;
- utilizatorul trebuie să poată specifica locul în care se va aplica semnătura electronică.
- în situația în care un utilizator refuză semnarea electronică a unui document, trebuie să se poată specifica motivul refuzului;
- trebuie să permită aplicarea de semnătură electronică pe documente, direct din cadrul sistemului fără a fi necesară extragerea și reîncărcarea acestora în sistem.
- Modulul trebuie să ofere funcționalități de generare de documente:
- platforma trebuie să ofere funcționalități pentru gestionarea și configurarea de șabloane Microsoft Word pentru generarea rapidă și automată de noi documente în formate standardizate care să respecte politicile organizației;
- documentele generate de sistem trebuie să poată fi salvate în platforma în formate ca MS Word sau PDF;
- platforma trebuie să permită popularea automată a documentelor generate cu valori ale indecșilor salvați în componentă;
- la generarea unui document în baza unui șablon, platforma trebuie să permită preluarea de informații din toate metadatele dosarului și includerea lor în documentul nou generat;
- platforma trebuie să permită generarea automată de documente prin intermediul unor task-uri de fluxurile de lucru;
- platforma trebuie să permită generarea manuală, la selecția șablonului, de documente și atașarea lor pe dosar sau pe document structurat;
- platforma trebuie să permită administratorilor să creeze, și/sau modifice un șablon existent;
- platforma va permite restricționarea folosirii șabloanelor doar la anumite tipuri de cazuri sau de documente structurate.

Modul registru electronic

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

Modulul registratură trebuie să asigure următoarele funcționalități:

- păstrarea înregistrărilor și procesarea tuturor documentelor primite și care ies, inclusiv primirea, deschiderea, vizualizarea și atribuirea dosarelor și documentelor,

introducerea în evidențele dosarelor și documentelor, împerecherea documentelor, procesarea documentelor, inclusiv producerea și depunerea automată a unei varietăți de documente electronice predefinite în cadrul fluxurilor de lucru, distribuirea documentelor, procesarea rezultatelor către destinatarii din afara organizației, plasarea documentelor în arhivă (arhivare electronică) și păstrarea acestora;

- înregistrarea și prelucrarea electronică a registrelor;
- etichetarea dosarelor, documentelor, corespondenței etc.;
- înregistrarea tuturor documentelor de intrare și de ieșire;
- înregistrarea directă a e-mailurilor sau a documentelor atașate la e-mailuri;
- client e-mail integrat direct în modulul de registratură, configurarea unui cont de e-mail de registratură per utilizator;
- posibilitatea definirii unui număr nelimitat de registre de documente. Pe fiecare registru de documente trebuie să existe posibilitatea definirii drepturilor de înregistrare a documentelor și tipurile de documente permise pentru înregistrare, având ca scop minimizarea greșelilor umane de înregistrare sau după cuvinte din textul documentelor scanate;
- căutarea rapidă a documentelor după numărul de înregistrare sau după cuvinte din textul documentelor;
- posibilitatea definirii de către administrator sau direct de către utilizator a coloanelor care să apară în fiecare registru. Completarea acestora va trebui să se poată face fie manual, fie prin preluare automată din metadatele documentelor înregistrate;
- inițierea fluxurilor de lucru la înregistrarea documentelor pentru transmiterea acestora către compartimentele responsabile;
- să asigure înregistrarea documentelor prin anexare la documente structurate (formulare) înregistrate;
- să asigure crearea unui număr nelimitat de înregistrări și definirea de coloane personalizate;
- să asigure existența unor coloane standard pentru registre, cum ar fi: data înregistrării, numărul, sursa, de la - la, persoane, departament, descriere, număr de pagini, număr de înregistrare și data de primire de la cealaltă parte;
- să asigure atașarea documentelor la anumite numere ale unui registru;
- să asigure definirea drepturilor de editare/vizualizare pentru fiecare registru;
- să asigure exportarea conținutului registrelor în fișiere XLS sau CSV;
- să asigure configurarea drepturilor pentru fiecare registru de utilizatori și grupuri;
- să permită alocarea numărului de înregistrare fără fișier;
- să permită atașarea fișierelor la un număr de înregistrare existent;
- odată înregistrate documentele în platforma de document management, în funcție de tipul de document înregistrat, precum și în funcție de indecșii și meta-datele asociate, documentele vor fi automat rutate de către platforma document management pe traseele electronice (fluxuri de lucru) definite și asociate acestora în sistem, precum și către destinatarii/departamentele asociate documentului în procesul de înregistrare.

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

Modulul trebuie să includă atât instrumentele pentru dezvoltare, cât și mediul de rulare pentru proiectarea, execuția și monitorizarea fluxurilor de documente.

Modulul de fluxuri de lucru cu documente trebuie să asigure următoarele funcționalități:

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

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

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

Modul de raportare

Platforma trebuie să vină însoțită de un modul integrat de raportare care va permite realizarea prin configurare a unor rapoarte sau tablouri de bord care să afișeze în format

tabelar sau grafic informații despre documentele și fluxurile de lucru din sistem. De exemplu:

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

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

Modulul de raportare trebuie să permită prin configurare facilă, de exemplu de tip „drag and drop“:

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

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

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

data creării, data modificării unui document.

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

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

Modul de administrare

Modulul de administrare trebuie să sprijine gestionarea ușoară a taxonomiilor, utilizatorilor, drepturilor utilizatorilor și fluxurilor de lucru, inclusiv, cel puțin, următoarele:

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

Modul de ajutor

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

Modulul de ajutor trebuie să fie o parte integrantă a sistemului și trebuie:

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

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

Având în vedere faptul că această componentă COTS reprezintă o componentă aplicativă care trebuie să poată fi adaptată continuu din punct de vedere funcțional la noile cerințe de business ale beneficiarului generate de, dar fără a se limita la: modificări legislative, modificări procedurale, se dorește ca furnizorul soluției să pună la dispoziția beneficiarului codul sursă pentru această componentă în integralitatea sa, respectiv codul sursă pentru platforma DMS, pentru fluxurile dezvoltate și pentru alte personalizări. Beneficiarul va utiliza codul sursă exclusiv în cadrul acestui proiect, fără drept de utilizare a codului sursă în scopuri comerciale.

3.8.3. Sistemul de gestiune a bazelor de date

Componenta baza de date tranzactionala trebuie sa fie o baza de date de tip relational, sa fie disponibila comercial (COTS - Commercial off the Shelf) si sa ofere posibilitatea de a rula pe diverse platforme hardware, pe sistemele de operare majore existente pe piata (Windows, Linux), oferind acelasi nivel al functionalitatilor pe sistemele de operare mentionate, precum si posibilitatea de a fi instalata intr-o infrastructura Kubernetes. Baza de date tranzactionala va asigura persistenta datelor ce vor fi manipulate la nivelul componentei de interoperabilitate, seturilor de date de tip registru precum si anumite surse de date specifice, oferind astfel capabilitati de tip enterprise necesare indeplinirii functionalitatilor solicitate de catre autoritatea contractanta.

Astfel, pentru a raspunde cerintelor de functionalitate si performanta cerute, componenta de baze de date relationale trebuie sa prezinte urmatoarele functionalitati minime si obligatorii:

Cerinte generale

- Sa ofere suport pentru proceduri stocate, triggeri si tranzactii autonome.
- Sa permită definirea de indecsi pentru acces rapid la date.
- Sa permită executia paralela a operatiilor de tip SELECT, INSERT, UPDATE, DELETE, MERGE, cu blocarea doar a inregistrarilor afectate, nu a intregii tabele.

- Sa permită executia de instructiuni INSERT in mai multe tabele simultan.
- Reorganizarea, mutarea si redefinirea de tabele, indecsi sau fisiere de date fara blocarea activitatii utilizatorilor la datele aflate in curs de modificare, indiferent de dimensiunea acestora.
- Parametrii de memorie sa poata fi ajustati dinamic si automat de catre baza de date astfel incat zonele de memorie sa fie dimensionate in concordanta cu tipul de operatii ce se desfasoara la un moment dat iar pentru a face fata unui numar foarte mare de utilizatori, baza de date trebuie sa ofere un mecanism de connection pooling care sa optimizeze folosirea resurselor server-ului la operatiile de tip login/logout.
- Sa ofere mecanisme de asigurare a consistentei datelor in situatia nefavorabila a unui incident cum ar fi interogarea directa a tabelelor care să prezinte imaginea datelor exact asa cum erau acestea la un moment anterior in timp, anulara unei tranzactii care a fost comise sau restaurare rapida a datelor, la nivel de tranzactie, tabela sau baza de date toate acestea fara a fi necesara restaurarea dintr-un backup, efectuarea de snapshot-uri periodice sau intretinerea prin proceduri de utilizator a unor copii ale datelor.
- Sa ofere un mecanism inclus care sa permita interogarea istoricului modificarilor unei tabele, atat de tip DDL cat si DML, fara a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvarea periodica sau utilizarea functiei de audit.
- Posibilitatea de a suspenda temporar operatii consumatoare de resurse (de exemplu incarcari masive de date), cu reluarea ulterioara a acestora in momentul cand sistemul permite, precum si posibilitatea de a implementa scheme de prioritate in modul de accesare a bazei de date in functie de tipul de utilizator inclusiv limitarea numarului de procesoare folosite de baza de date fara a fi necesara folosirea unei solutii de virtualizare.
- Sa ofere posibilitatea de izolarea din punct de vedere management si securitate a mai multor baze de date in contextul aceleasi instante de baza de date.
- Sa ofere suport pentru date de tip multimedia.
- Sa ofere suport pentru tipuri de date de tip XML, JSON.
- Sa permita definirea tabelor de tip „immutable” (datele din aceste tabele nu pot fi modificate, sunt permise doar operatiuni de insert), acestea putand fi utilizate la nivelul aplicatiei, fara a fi necesare modificari.
- Sa ofere un framework de dezvoltare de tip „low-code”, ce va permite dezvoltarea rapida a aplicatiilor fara a fi necesare cunostinte avansate de dezvoltare.
- Sa ofera posibilitatea facila de a defini servicii de tip REST, peste obiecte sau proceduri stocate definite la nivelul bazei de date

Inalta disponibilitate

- Baza de date trebuie sa permita functionarea intr-o arhitectura de inalta disponibilitate de tip cluster, o singura baza de date putand fi instalata pe mai multe noduri asigurandu-se toleranta la defecte hardware sau nefunctionare planificata.

- Baza de date va permite balansarea incarcarii intre noduri, la nivelul cererilor si executiilor pe baza de date cluster, indiferenta de natura cererilor, astfel se va permite citirea si scrierea pe oricare din nodurile clusterului de baza de date, fara impunerea niciunei limitari.
- Securitate tranzactionala in cazul aparitiei unor erori hardware sau software in clusterul de baza de date trebuie sa fie tratata de mecanismele interne ale bazei de date iar in cazul unei defectiuni hardware si/sau software sa permita reconectarea automata la nodul sau nodurile ramase disponibile.
- Sa ofere posibilitatea de upgradare si aplicare a patch-urilor online
- Sa ofere posibilitata adăugării de noduri suplimentare în cazul în care sistemul necesită mai multă putere de calcul (scalare pe orizontală).

Securitate si confidentialitate

Ca si mecanisme de securitate oferite, componenta de baza de date tranzactionala trebuie sa includa restrictionarea accesului la nivelul obiectelor bazei de date, aplicarea simultana a mai multor politici de securitate pe un acelasi obiect al bazei de date precum si mecanisme native de restrictionare a accesului utilizatorilor la nivel de inregistrare si coloana intr-o tabela. Baza de date trebuie sa permita configurarea autentificarii utilizatorilor pe baza de certificate digitale iar pentru sporirea sigurantei datelor trebuie sa asigure mecanisme robuste de criptare a datelor stocate cat si a celor vehiculate in timpul sesiunilor dintre utilizatori si baza de date. Toate operatiile de criptare trebuie sa poata fi implementate intr-un mod transparent, fara a implica modificari la nivel de aplicatie de business sau client si sa poata fi facute, in functie de nevoie, la nivel de coloana, tabela sau chiar baza de date si sa suporte cel putin urmasorii algoritmi de criptare : 3DES (minim 168 bit) si AES (minim 256 bit).

Din punctul de vedere al activitatilor de audit, baza de date va oferi o lista cu operatiile pe care un grup sau o clasa de utilizatori le poate executa si va avea abilitatea de a se ajusta la gradul de detalii capturate de catre facilitatea de audit, prin introducerea de politici de audit care sa determine cand un utilizator este sau nu auditat (spre exemplu situatia cand utilizatorul acceseaza doar anumite informatii dintr-o tabela sau cand conectarea nu se face printr-o anumita aplicatie).

De asemenea, baza de date va oferi nativ posibilitatea de a restrictiona accesul utilizatorilor si administratorilor (DBA) la nivelul anumitor obiecte din baza de date si sa permita impunerea de restrictii inclusiv asupra comenzilor pe care acestia le pot executa. Controlul accesului la baza de date se va asigura in mod transparent fata de aplicatii prin implementarea unui mecanism de autentificare si autorizare conditionata, in functie de parametri ca adresa de retea, ora la care se incearca conectarea, tip utilizator, locatie de conectare. Astfel, baza de date va permite separarea atributiilor administratorilor la nivelul bazei de date, prin definirea de domenii de date, astfel incat administratorii bazei de date (DBA) sa nu aiba acces la aceste domenii, ci doar administratorii de date desemnati explicit; In vederea cresterii nivelului de securitate, baza de date va oferi suport pentru clasificarea

datelor în cadrul tabelelor bazei de date, astfel încât un utilizator să aibă acces doar la datele care corespund nivelului său de clasificare. În ceea ce privește accesul la date, baza de date va permite restricționarea accesului utilizatorilor la anumite randuri din tabele bazei de date pe baza de etichete și politici de securitate și va permite protejarea informației stocate în baza de date la nivel de tabelă, prin oferirea accesului doar la un subset de informații (randuri), pe baza rolului și responsabilităților aceluși utilizator;

Pentru asigurarea securității și confidențialității datelor exportate în vederea provizionării mediilor de test, baza de date trebuie să includă mecanisme de anonimizare și mascare a subseturilor de date astfel încât să poată fi păstrate relațiile logice și caracteristicile acestora (tipuri de date, dimensiune, pondere, etc) dar ascunzând valoarea lor inițială. Operațiile de anonimizare trebuie realizate fie static (situație în care datele sunt exportate sau mutate într-un alt mediu) fie dinamic (situație în care datele sunt anonimizate în timp real pentru utilizatorii ce accesează baza de date).

Backup

Din punctul de vedere al operațiunilor de backup, baza de date trebuie să permită operațiuni de backup și restaurare a datelor în regim de lucru online, salvarea totală și/sau parțială a bazei de date iar toate aceste operațiuni să fie făcute într-o formă unitară, centralizată și ușor de administrat. De asemenea, pentru optimizarea timpului alocat acestor operațiuni baza de date trebuie să ofere mai mulți algoritmi de compresie pentru datele salvate și să permită efectuarea de backup numai pentru fișierele care au suferit schimbări de la ultimul backup și pentru cele nou create (backup incremental). Operațiile de backup trebuie să permită citirea și scrierea paralelă (simultan din/în mai multe fișiere) în funcție de nevoie, baza de date trebuie să permită, pe baza datelor de backup restaurarea parțială la o imagine consistentă a acesteia de la un moment de timp specificat de cel ce realizează operația de restaurare.

Replicare

Baza de date trebuie să includă mecanisme de replicare software pentru menținerea uneia sau mai multe baze de date (standby) sincronizate cu o bază de date primară, în vederea prevenirii pierderilor de date sau de nefuncționare din cauza corupției de date, erorilor de sistem, erorilor umane, sau în caz de dezastre, precum și posibilitatea de a utiliza bazele de date standby pentru activități de raportare.

Această componentă va trebui să ofere următoarele funcționalități:

- posibilitatea de a fi configurată în moduri diferite în funcție de scopul propus, spre exemplu disponibilitate ridicată, performanță maximă, protecție maximă
- se integrează nativ cu baza de date, replicarea făcându-se la nivelul tranzacțiilor de date

- sa permita configurarea replicarii atat in mod sincron cat si asincron
- validarea continuă a datelor pentru a detecta și a preveni coruperi. Componenta va folosi algoritmi interni ai bazei de date pentru mentinere integritatii datelor si prevenirea inconsistentelor la nivel de tranzactie
- resincronizare automată după întreruperile de rețea;
- failover automat utilizând moduri de transport de date sincron sau asincron;
- sa permita configurarea mai multor baze de date de tip standby
- sa ofere mecanisme ce permit sincronizarea datelor la distante mari fara pierderi de data si fara a exista un impact pe baza de date primara.
- bazele de date standby pot fi utilizate pentru raportări, copii de siguranță, precum și activități de testare;

Administrare si operare

Pentru asigurarea performantei maxime si asigurarea unui raspuns proactiv la eventualele degradari ale acesteia, baza de date trebuie sa ofere mecanisme interne de monitorizare si diagnosticare continua, automatizand colectarea parametrilor de funcționare ai bazei de date, precum si stocarea acestora pentru a putea furniza o imagine pe termen lung a modului de funcționare a bazei de date. Procesului de optimizare a instrucțiunilor SQL, trebuie sa se faca automat, explorand in mod cuprinzator toate modalitatile de optimizare ale unei instructiuni SQL (inclusiv recomandarea de a fi creati indecsi sau partitii aditionale), oferind sugestii de implementare pentru administratori inclusiv posibilitatea de implementare fara a fi necesara modificarea codului aplicatiei.

Din punct de vedere al operatiunilor de administrare, solutia de baza de date trebuie sa ofere o unealta cu interfata grafica accesibila web pentru administrarea bazei de date, care sa includa urmatoarele facilitati:

- construirea si executare scripturi SQL
- gestionarea obiectelor bazei de date
- efectuarea de functii de backup si restaurare
- administrare a utilizatorilor
- monitorizarea bazei de date si vizualizarea fisierelor de tip log
- vizualizarea in timp real a incarcarii bazei de date, a activitatii utilizatorilor (inclusiv a interogarilor SQL pe care acestia le ruleaza), a operatiilor mari consumatoare resurse (I / O si CPU) precum si rapoartarea acestor evenimente catre administratori

3.8.4. Componenta de Business Intelligence

Componenta de analiză și raportare trebuie sa fie disponibila comercial (COTS - Commercial off the Shelf), sa ofere posibilitatea de a rula pe diverse platforme hardware precum si pe sistemele de operare majore existente pe piata (Windows, Linux). Rolul acestei componente este de a defini analize detaliate si rapoartele necesare urmarii modului de functionare a componentelor software dezvoltate la nivelul platformei, modului in care datele sunt

schimbate între diverse entități, precum și posibilitatea de unificare a datelor din surse multiple de date. Pentru a îndeplini scopul mai sus descris, componenta de analiză și raportare trebuie să îndeplinească minimal următoarele cerințe:

- Va oferi posibilitatea prezentării datelor în formate variate (de exemplu tabele, tabele pivot, grafice, texte derulante);
- Va oferi funcționalități de navigare ghidată pentru utilizatorii finali, cu posibilități multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât și pentru grafice;
- Va permite combinarea rezultatelor obținute de pe platforme diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
- Va permite salvarea rapoartelor în formate diferite (Excel, PDF, Word, HTML);
- Va oferi posibilitatea definirii de tablouri de bord și a includerii rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
- Va permite tuturor utilizatorilor modificarea tablourilor de bord sau a rapoartelor, de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
- Va facilita accesul la informație printr-un nivel de metadate care să ascundă utilizatorilor finali complexitatea structurilor fizice de date;
- Nivelul de metadate expus utilizatorilor va fi comun la nivelul tuturor modulelor sistemului de raportare și analiză;
- Utilizatorii își vor putea crea singuri propriile rapoarte (analize ad-hoc) fără să fie nevoiți să cunoască structurile fizice de date pe care le accesează;
- Va permite accesarea datelor atât de pe platforme relaționale, cât și multidimensionale sau foi de calcul;
- Va permite integrarea cu LDAP, oferind în același timp capabilități proprii de definire a rolurilor pentru restricționarea accesului la rapoarte;
- Interacțiunea utilizatorilor finali cu aplicația se va face într-o interfață de tip web, fără a necesita instalarea de componente software suplimentare pe calculatoarele utilizatorilor;
- Va expune o interfață de administrare atât a drepturilor de acces la diferite zone cât și a drepturilor de acces pe diferite tipuri de acțiuni;
- Va fi scalabilă și va dispune de mecanisme de clustering a componentelor, astfel încât să poată fi adăugate ulterior resurse hardware suplimentare;
- Va oferi posibilitatea prezentării simultane a aceleiași informații în formate diferite, printr-o singură execuție a interogării: de exemplu tabel + grafic;
- Va permite facilități avansate de formatare a rapoartelor;
- Va oferi posibilitatea de a salva, organiza și partaja rapoartele cu alți utilizatori;
- Va oferi capabilități de drill-down (navigare în adâncime) pe diferite nivele de agregate;
- Generarea interogărilor către bazele de date va ține seama de specificul bazei de date accesate;
- Va permite acces la surse de date multiple, în mod transparent pentru utilizatorul final;
- Accesul utilizatorului final se va face dintr-o singură interfață web din care să aibă acces la toate componentele de analiză și raportare;

- Din punctul de vedere al arhitecturii sistemului de raportare, toate componentele sale vor fi strâns integrate, vor face parte dintr-un mediu unitar de lucru și vor împărtăși un sistem de securitate comun;
- Va oferi utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât și în aplicația de analiza și raportare;
- Va dispune de mecanisme de alertare pentru utilizatorii finali
- Va oferi utilizatorilor finali posibilitatea subscrierii la alertele definite.
- Rapoartele analitice să poată fi construite pe un număr variabil de interogări analitice. Instrumentul de business intelligence nu trebuie să limiteze numărul de astfel de interogări.
- Să asigure posibilitatea de writeback (scriere) în baza de date din aplicația de raportare;
- Este necesar ca aplicația de raportare să poată afișa anumite valori indentificate ca și critice, să semnalizeze depășirea unor praguri ale acestor valori, să semnalizeze apariția unor evenimente. Astfel, va oferi utilizatorilor posibilitatea de formatare condiționată a valorilor prin setarea unor praguri, pentru a evidenția valorile excepționale.
- Să nu necesite replicarea datelor pe un server separat, ci să folosească capabilitățile bazei de date sursă.
- Mediul de lucru pentru utilizatorii finali sau alți dezvoltatori de rapoarte/analize să fie în mediu web pur, interacțiunea cu sistemul să se realizeze prin operațiuni de tip „point and click” și „drag and drop” (să nu necesite cunoștințe de programare din partea utilizatorilor)
- Să ofere posibilitatea definirii de rapoarte în lantuite, datele din raportul copil fiind filtrate pe baza rezultatelor din raportul părinte.
- Să permită tuturor utilizatorilor crearea sau modificarea de rapoarte, analize ad-hoc și tablouri de bord, acordarea drepturilor specifice (consultare, creare de obiecte etc.) urmând a fi făcută de către administratorul platformei.
- Să ofere cel puțin algoritmi analitici de tipul regresie sau clusterizare accesibili utilizatorilor din interfața platformei.
- Să permită detectarea de paternuri /relații prin selecția datelor dintr-o vizualizare, selectare care să realizeze automat evidențierea datelor corelate din toate vizualizarile existente în pagină.
- Să ofere posibilitatea de combina seturi de date multiple și de definire a cheilor de legătură în interfața web
- Să ofere posibilitatea de modifica manual dimensiunilor obiectelor afișate
- Să ofere posibilitatea de dimensiona automat obiectele afișate astfel încât să utilizeze tot ecranul
- Să permită folosirea datelor externe imediat ce au fost încărcate, fără a solicita activități de modelare a datelor
- Posibilitatea de a efectua transformări primare la încărcarea datelor
- Posibilitatea de a combina datele din fișiere externe cu date modelate în ariile de subiecte din platforma analitică

- Posibilitatea de a crea rapoarte analitice pe dispozitive mobile
- Sa permita crearea de snapshoturi ale vizualizatorilor create astfel incat sa permita partajarea rezultatelor analitice cu ceilalti utilizatori ai sistemului, prin parcurgerea ordonata a activitatilor de interpretare a datelor
- Sa permita definirea de marimi calculate prin aplicarea unor functii matematice predefinite asupra marimilor existente
- Sa permita crearea automata a unor reprezentari sugestive pentru informatiile selectate de utilizator si sa permita utilizatorului alegerea tipului de vizualizare din paleta de obiecte disponibile
- Sa permita utilizarea proactiva a functionalitatilor de tip Machine Learning pentru identificarea anuntor informatii relevante (grupari de date, trenduri etc)
- Sa permita utilizarea algoritmilor de tip Machine Learning in procesarea unor fluxuri de date. Configurarea algoritmilor trebuia facuta in mod simplu fara a necesita scriere de cod
- Sa permita afisarea pe harta a informatiilor, oferind suport pentru filtrarea informatiilor dupa criterii geospatiale prin selectarea pe harta a ariei geografice de interes
- Sa ofere posibilitatea de partajare a continutului analizelor efectuate, intr-un mod securizat, cu alti membrii ai echipei de lucru, alte departamente etc

3.8.5. Componenta de interoperabilitate

Componenta de interoperabilitate isi propune sa implementeze o platforma unica in schimbul de informatii intre diferite sisteme existente dar si viitoare la nivelul institutiilor publice. Platforma va utiliza tehnologii moderne, standarde deschise (servicii web, JSON/XML), cozi de mesaje), va implementa schimburi de date sincrone si asincrone, asigurand un management complet al ciclului de viata al serviciilor web. Platforma nu isi propune sa stocheze volume mari de date, scopul fiind acela de hub de schimb de informatii, dar functie de specificul fiecarui sistem anumite seturi de date vor putea fi sincronizate la nivelul acestei platforme. Platforma isi propune sa fie flexibila in modul in care componente de integrare vor fi dezvoltate si implementate, permitand ansamblarea componentelor SOA sub forma de aplicatii compozite. De asemenea, in vederea standardizarii definirii aplicatiilor SOA, se va folosi un limbaj standard de definirea a fluxurilor de business BPEL (Business Process Execution Language) si va permite reprezentarea acestora folosind BPMN (Business Process Model and Notation).

In acest sens, aceasta componenta va trebui sa urmareasca programul promovat la nivelul comunitatii europene si anume: ISA 2 (Interoperability Solution for European Public Administration, Business and Citizens).

Acest demers se defineste ca un cadrul de lucru ce defineste cateva principii ce guverneaza acest program:

- Only once, ce definește conceptul de reutilizare și definirea unor servicii specializate cu funcțiuni clar definite ce sunt partajate cu diversi consumatori de servicii
- Open services, ce presupune ca fiecare funcționalitate implementată la nivelul unui sistem informatic să fie definită și ca un serviciu deschis, în acord cu politica de securitate și acces la date
- One-stop-shop, presupune definirea unei interfețe unitare ce oferă un set complet de servicii într-o formă simplificată și coerentă. Într-o exprimare tehnică, aceasta presupune publicarea acestor servicii către consumatori externi sub forma unor cataloage de servicii corespunzător documentate.
- End2End, definește conceptul de consolidare și orchestrare unitară a diverselor funcțiuni unitare care vin să definească un proces de business complet, astfel, procesul de business va fi încapsulat unitar și ușor de utilizat ulterior (de exemplu, serviciul de aprobare al unei cereri este încapsulat unitar fără a fi nevoie de o cunoaștere în detaliu a procesului de aprobare, persoane, nivel de management, instituții ce sunt implicate în acest proces de aprobare etc)
- Digital by default, recomandă proiectarea fiecărui nou serviciu public sau intern ca serviciu digital, utilizând tehnologii moderne și inovatoare, ce poate fi consumat/accesat de diverse entități interne sau externe (cetățeni, instituții externe etc)
- Cloud ready, flexibilitatea de a beneficia de avantajele conceptului de Cloud (utilizarea de standarde deschise, API driven, scalabilitate, independența de locația de instalare: on-prem, Cloud privat, Cloud public etc)

Astfel, pentru a răspunde cerințelor de funcționalitate și performanță cerute, componenta de interoperabilitate trebuie să ofere următoarele capabilități minime și obligatorii:

- Să fie disponibilă comercial (COTS - Commercial off the Shelf) și să ofere posibilitatea de a rula pe diverse platforme hardware (Windows, Linux)
- Posibilitatea să fie instalată în mediu containerizat (ex: Docker) și să ruleze într-o arhitectură Kubernetes
- Să ofere un instrument de tip CLI prin intermediul căruia să se poată asigura ciclul de viață al aplicațiilor/componentelor software de integrare dezvoltate peste platforma de SOA
- Suport pentru soluții moderne și deschise de integrare conform principiilor și conceptelor arhitecturilor Service Oriented Architecture (SOA) și Event Driven Architecture (EDA);
- Să fie bazată pe standardele deschise de interoperabilitate a aplicațiilor WS-I Basic Profile, WSDL, WS*, XML, SOAP, UDDI, REST;
- Permite comunicații sincrone și asincrone inter-aplicații;
- Soluția va implementa cel puțin următoarele modele de servicii: sincron cerere/răspuns, asincron one-to-one;
- Permite folosirea de canale multiple de notificare pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicații;

- Se integrează cu soluții de tip Service Registry bazate pe standardul deschis Universal Description Discovery and Integration (UDDI);
- Tipurile de mesaje transportate suportate de soluția de tip Service Bus vor fi cel puțin: XML, text, binar, atașament;
- Capabilități extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL) și XQuery;
- Sa ofere conectori la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje (IBM MQ, Oracle AQ, JMS, Apache Kafka), sisteme de fișiere, FTP;
- Posibilitatea de a crea conectori custom, particularizat pe o nevoie de integrare specifica
- Sa ofere conectori la principalele platforme de tip aplicații (SAP, Oracle e-Business Suite, Siebel etc);
- Sa ofere configuratii predefinite cu parametrii optimizati in vederea constuirii de fluxuri de integrare (dimensiune memorie, timeouts, logging, restrictii de dimensiune a payload-ului)
- Servicii de transport cu suport pentru persistența datelor și garantarea livrării datelor;
- Capabilități extinse de transformare și dirijare a datelor bazate pe conținutul transportat;
- Posibilitatea definirii, la momentul execuției, a adreselor de destinație a mesajelor, eventual prin interogarea unei soluții de tip Service Registry;
- Să ofere servicii de securitate atât la nivel transport cât și la nivel de aplicație;
- Gestiunea încărcării livrării mesajelor către serviciile destinație înregistrate la nivelul magistralei de interconectare folosind cozi de mesaje tampon;
- Va include capabilități native de monitorizare cu suport pentru dashboard-uri ce pot afișa informații legate de alertele SLA, parametrii de operare etc.;
- Soluția va asigura suport de înalta disponibilitate prin clusterizare de tip activ-activ sau activ-pasiv;
- Soluția trebuie să permită stoparea temporara a unui nod din cluster pentru mentenanță și suport, sistemul în acest timp fiind disponibil pentru activități normale.
- Suport complet pentru dezvoltarea, testarea, executia, monitorizarea, optimizarea și administrarea proceselor de flux;
- Modelarea declarativă a proceselor de afaceri utilizând BPEL / BPMN cu ajutorul mediului de dezvoltare integrat al sistemului;
- Suport pentru standarde de larga răspândire cum ar fi: XML, web services, JMS, J2EE, SMTP, HTTPS;
- Oferă șabloane predefinite de dirijare a activităților către utilizatorii cu roluri specifice la nivelul aplicatiilor precum și interfete grafice de lucru cu fluxurile automatizate;
- Trimitere automata de notificări de initiere de activități, termene limita, stadiu de executie, finalizare și să trateze automat acest tip de notificări primite de la sisteme externe;
- Va permite colectarea permanentă de statistici de executie - timpi de executie, frecvență de aparitie evenimente, stări fluxuri - pentru procesele instalate;

- Modul integrat de stocare și evaluare a regulilor de business, externe proceselor modelate, pe care personalul non-tehnic le va putea accesa și modifica ulterior;
- Modulul de reguli de business trebuie să ofere un editor de reguli precum și funcționalități avansate de discovery, guvernanta, versionare, trasabilitate și stocarea într-un mod centralizat
- Posibilitatea de a defini reguli de business în limbaj natural, descriptiv în vederea definirii unei reguli de business, fără a fi nevoie de cunoștințe de programare
- Să ofere mecanisme avansate de caching, ce asigură persistența componentelor în memorie, pentru creșterea performanței rularii proceselor de integrare și îmbunătățirea accesului la date
- Suport pentru includerea sub-proceselor apelate dintr-un proces principal în tranzacția fluxului initiator;
- Facilități de activare a auditării fluxurilor;
- Monitorizarea activității la nivelul proceselor, cu capacități de colectare informații și raportare grafică;
- Monitorizarea în timp real a indicatorilor de performanță (KPI). Definirea de alerte și acțiuni în cazul în care indicatorii de performanță nu ating anumite praguri valorice;

3.8.6. Componenta de API management

Soluția de Management API va oferi o interfață vizuală pentru a configura politici complexe de securitate pentru protecția API-urilor și serviciilor web. De asemenea va pune la dispoziție instrumente integrate de testare și monitorizare care să asigure un management continuu al întregului ciclu de viață a serviciilor API.

Soluția propusă va oferi un mediu API securizat - unul care protejează toate etapele ciclului de viață API, inclusiv partea de furnizare (construcția, implementarea și gestionarea traficului API), cât și partea de consum - descoperirea, achiziția și consumul de către dezvoltatorii de aplicații și alte API consumatori.

Va facilita schimbul de date cu acuratețe, în mod eficient și în condiții de siguranță între diferite sisteme informatice (atât din cadrul autorității contractante cât și din cadrul altor instituții cu care există sau vor exista protocoale de colaborare) conform proceselor de lucru operaționale specifice instituțiilor implicate.

Platforma trebuie să fie o aplicație software de tip COTS cu licențiere perpetuă sau sub forma de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție.

Soluția trebuie să permită implementare ca software de sine stătător, appliance software, implementare în mediu virtual, și implementare în containere cum ar fi Docker.

Soluția va trebui să ofere și:

- posibilitatea de a aplica versiuni noi/ patch-uri de la distanță
- management centralizat al tuturor nodurilor din cluster într-o singură pagină de administrare
- scripting în linie de comandă pentru politici
- suport pentru disaster recovery out-of-the-box
- monitorizare și alertare centralizată

Totodată, având în vedere că dezvoltatorii software sunt adesea rugați să facă aplicațiile mai colaborative, incluzând funcții sociale și de mesagerie, soluția oferită va trebui să dispună de o componentă pentru crearea unui modul pentru mesajele directe de la utilizator la utilizator sau de la utilizator la grup în aplicațiile dezvoltate cu doar câteva linii de cod.

Portal pentru dezvoltatori (Portalul DEV_API)

Această soluție trebuie să le permită proprietarilor de API să controleze modul în care sunt publicate API-urile, le permite consumatorilor să descopere ce servicii sunt disponibile și ajută echipele de operațiuni să monitorizeze performanța API-urilor prin integrarea cu instrumente de monitorizare API de nivel enterprise.

Portalul API trebuie să simplifice descoperirea API pentru dezvoltatori și să le ofere acces la datele terțelor instituții care vor publica servicii API pentru a crea aplicații rapid. Relațiile cu dezvoltatorii, partenerii și terții să fie ușor de gestionat prin oferirea de funcționalități de publicare documentații de folosire a API-urilor, configurare drepturi de acces, posibilitatea de a publica instrumente educaționale, inclusiv aplicații demo, API Explorer și generarea de cod pentru serviciile API publicate în portal.

Portalul API va trebui să utilizeze o arhitectură containerizată pentru a ușura implementarea, migrarea și upgrade-ul în viitor. Componentele portalului să fie implementate în containerele Docker, facilitând schimbarea/înlocuirea containerelor pe măsură ce se lansează noi funcționalități ale acestei componente.

Această componentă va trebui să pună la dispoziție nativ și un server de email propriu (SMTP) care să poată fi configurat independent față de serverul de email al beneficiarului.

De asemenea, soluția trebuie să:

- suporte instalarea și configurarea pe o bază de date (ex : MySQL sau PostgreSQL)
- permită crearea de utilizatori, conturi, organizații
- permită configurarea de abonamente la nivel de API sau de conturi de dezvoltator
- permită crearea de mai mulți utilizatori pentru un singur cont de dezvoltator
- pună la dispoziție un flux de lucru pentru înregistrarea unui dezvoltator software nou pentru accesul la serviciile API oferite.
- permită crearea de utilizatori de tipul publisher care permite organizațiilor terțe să publice și să administreze propriile servicii API expuse

- suporte adăugarea de câmpuri custom cerute la înregistrarea unui utilizator nou
- pună la dispoziție o zonă de forum de discuții între dezvoltatorii de software înregistrați în sistem
- permită generarea de cod automat client-side în JavaScript, node, Python, Ruby, PHP, Objective C, Java pentru serviciile puse la dispoziția dezvoltatorilor
- ofere un API Explorer
- permită expunerea unei baze de date prin REST API
- pună la dispoziție o zonă de administrare a cheilor API care să permită: suspendarea/revocarea cheilor API, crearea unui certificat sau token (în plus față de cheia API generată)
- permită posibilitatea de a defini preturi pentru abonamente lunare alocate dezvoltatorilor precum și urmărirea și facturarea lor
- ofere controale RBAC pentru utilizatori de tipul autor, editor și publisher

Raportări portal

Soluția va oferi rapoarte pentru cel puțin următoarele informații:

- utilizarea API-ului de către dezvoltator individual
- utilizarea API-ului de către grupul de dezvoltatori
- utilizarea API-ului de către anumiți clienți dezvoltatori
- erori de rutare API
- depășire limite de utilizare API
- disponibilitate API
- utilizarea API în raport cu cota
- timpilor de răspuns API
- latență API backend

Soluția trebuie să aibă abilitatea de a genera rapoarte în mai multe formate (cel puțin CSV, PDF și HTML)

Securizare Acces

Următoarele cerințe tehnice trebuie acoperite de soluția propusă:

- Soluția trebuie să realizeze conversia XML-JSON direct fără a fi nevoie de scheme separate pentru XML și JSON. Transformarea XML-JSON trebuie să fie bidirecțională, XML-JSON și JSON-XML.
- Să ofere control asupra performanțelor apelurilor API:
 - o configurare „throttling” și „rate limit”
 - o priorizare de trafic
 - o limitare acces API pe utilizator, orar și adresă IP
 - o rutare trafic în funcție de regiune geografică, adresă IP și timp de răspuns

- Să ofere funcționalități de cluster păstrând funcționalitățile de securitate precum și politicile de performanță definite la nivelul tuturor nodurilor prin replicare automată (limite interogări, protecție la atacuri, firewall xml)
- Să ofere suport pentru diverși algoritmi de criptare: 3DES , AES, SHA, RSA
- Să suporte algoritm de criptare curba eliptica
- Soluția trebuie să detecteze automat atașamentele SOAP;
- Soluția trebuie să permită definirea și detectarea de atașamente neașteptate sau incompatibile cu cerințele definite;
- Soluția trebuie să detecteze cererile XML cu un număr foarte mare de attribute ceea ce indică un atac la nivel de conținut.
- Să ofere mecanisme SSO end-to-end pe toate dispozitivele precum și integrare nativă cu soluția de SSO web/browser-based oferită.
- Să asigure suport pentru menținerea corespondenței între sesiunea de front-end și cea de backend.
- Să asigure capabilități de WS/API firewall și funcții de control acces pe baza de politici de acces de tip RBAC;
- Să poată inspecta conținutul apelurilor folosind XML Schemas, XPath JSON Schemas, JSON Path, expresii regulate și comparații de stringuri
- Să permită următoarele metode de autentificare:
 - o HTTP Basic;
 - o WS-Security
 - o Security Assertion Markup Language (SAML);
 - o ticket Kerberos;
 - o token OAuth.
- Să ofere mecanisme de securitate pentru echipamente Mobile și IoT prin OAuth (client și server side) și OpenID Connect.
- Să ofere suport pentru notificări către end-user prin Email, Apple Push Notification Service și Android alerts.
- Să permită un management complex al serviciilor API oferite prin:
 - o Versionare și rollback
 - o Orchestrare
 - o Suport pentru crearea de politici ramificate și politici globale
 - o Validarea politicilor create în real-time
 - o Aplicarea oricăror modificări de politici real-time fără necesitatea repornirii vreunei componente
 - o Automatizarea migrărilor serviciilor API pe toate nodurile clusterului

De asemenea, soluția trebuie:

- să limiteze mărimea documentului XML incluzând sau nu dimensiunea atașamentului;
- să detecteze vulnerabilități de genul SQL-injection sau XPATH-injections;
- să poată limita numărul de mesaje pe o perioadă de timp: pe secundă, pe minut, pe oră și pe zi;
- să poată limita numărul de conexiuni concurente către un anumit serviciu web expus;

- să poată preveni atacuri de tip “replay”: mesaj autentic cu credențiale valide repetat de foarte multe ori;
- să aibă posibilitatea ștergerii, înlocuirii, criptării sau mascării de date confidențiale;
- soluția trebuie să monitorizeze tranzacțiile în timp real și să permită vizualizarea statisticilor pe perioade de timp.;
- să poată cripta și decripta mesaje XML;
- să suporte WS-Security și XML Encryption;
- să valideze semnătura pentru a determina dacă un mesaj este de încredere;
- să valideze certificatele pe baza unei liste de certificate revocate;
- să poată bloca accesul de la o lista de IP-uri sau subnet-uri;
- să poată permite accesul pe baza unei liste de adrese IP sau subnet;
- să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse nu sunt disponibile;
- să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse au o performanță deteriorată, sub nivelul unei limite pentru: timp de răspuns și număr de reîncercări;
- să permită logarea evenimentelor la nivel de servicii, client și tranzacții;
- să ofere următoarele opțiuni de logging:
 - o fișier log local;
 - o server Syslog;
 - o bază de date;
 - o trap SNMP;
- să permită posibilitatea separării evenimentelor de securitate de cele care privesc tranzacțiile.
- Trebuie să ofere capabilități suplimentare pentru a proteja amenințările aplicațiilor web conform cerințelor de mai jos descrise de OWASP:
- Trebuie să ofere acces deplin la toate cererile web și conținutul de răspuns și context pentru a permite inspecția și protecția în timpul execuției.
- Să poată cere autentificare puternică sau multifactorială prin protocoale securizate pentru a proteja împotriva atacurilor de forță brută folosind politici simple sau sofisticate de limitare a ratei de interogări sau politici de throughput.
- Să poată detecta și proteja împotriva atacurilor bazate pe sesiune, controlând atributele de securitate ale cookie-urilor, folosind semnături digitale și criptare sau urmărirea și maparea, și politici de impunere a identificărilor de sesiune sticky trimiși.
- Să poată impune prin politici criptare în repaus sau în tranzit și să poată fi configurat conform PCI-DSS - îndeplinind nevoile industriilor reglementate, cum ar fi sectorul financiar, asistența medicală și sectorul public.
- Să protejeze împotriva execuției de cod de la distanță și a atacurilor de denial of services (DoS).
- Să ofere mecanisme de control al accesului proprietare și conform standardelor din industrie, pentru a se asigura că resursele protejate pot fi accesate numai de utilizatori și aplicații autentificați și autorizați, folosind politici de securitate centralizate.

- Trebuie să permită o implementare ușoară și sigură în DMZ și să fie conformă cu certificarea Common Criteria pentru profilurile Enterprise Security Management, Policy Management și Enterprise Security Management, Access Control.
- Să ofere protecție maximă împotriva atacurilor pentru servicii, API-uri și aplicații și să le permită clienților să detecteze, să răspundă și să blocheze atacurile folosind politici de securitate centralizate ca firewall la nivel de aplicație.
- Să ofere niveluri de monitorizare definibile, permițând un nivel adecvat de raportare pe baza cerințelor beneficiarului.
- Trebuie să permită integrarea cu scanere de viruși și să protejeze împotriva amenințărilor la nivel de mesaj prin validarea traficului împotriva metadatelor la nivel de aplicație, cum ar fi schemele XML și schemele JSON .
- Să ofere capabilități de reverse proxy web:
 - o Memorare în cache
 - o Throttling/shaping
 - o Comprimare
 - o Terminare SSL
 - o Rutare dinamică/echilibrare de încărcare inteligentă
 - o Rescrierea adreselor URL
 - o Manipulare antet
 - o Manipulare parametri
 - o Manipulare cookie

Pentru a asigura o integrare completă a soluției de API management în cadrul arhitecturii proiectului, componenta va fi extinsă cu funcționalități avansate de orchestrare și automatizare a proceselor prin API-uri. Această extindere are rolul de a transforma componenta de API Management dintr-un simplu mecanism de publicare și securizare a serviciilor într-un instrument unitar de guvernare, orchestrare și execuție automată a fluxurilor de lucru.

Orchestrarea API-urilor in workflows

Soluția va permite integrarea nativă a API-urilor în fluxuri de lucru complexe, configurabile printr-o interfață vizuală, asigurând:

- posibilitatea de a corela apeluri API cu procese interne sau interinstituționale;
- definirea de condiții, ramificări și execuții paralele pentru apelurile API;
- reutilizarea serviciilor expuse sub formă de componente modulare în diferite scenarii operaționale;
- integrarea cu formulare electronice (workflow forms) care vor declanșa procese automatizate pe baza datelor introduse de utilizatori.

Formulare integrate în Workflows

Soluția va pune la dispoziție mecanisme pentru crearea și utilizarea formularelor electronice

integrate în fluxurile de lucru. Aceste formulare vor permite:

- introducerea de date direct de către utilizatori finali sau funcționari, în vederea declanșării sau completării unui proces automatizat;
- validarea datelor prin reguli predefinite și transmiterea acestora către API-uri interne sau externe;
- generarea de documente și rapoarte pe baza datelor introduse, cu trasabilitate completă;
- integrarea formularelor în portaluri interne, aplicații web sau sisteme externe prin API.

Surse, Trigger-e și Evenimente

Soluția va include mecanisme de tip event-driven architecture, care vor oferi:

- configurarea de surse de date și sisteme externe ce emit evenimente către platformă;
- definirea de trigger-e pentru inițierea automată a fluxurilor de lucru în funcție de condiții predefinite (de exemplu: depășirea unei cote de utilizare API, erori de rutare, primirea unui mesaj extern);
- gestionarea unitară a evenimentelor generate în timp real, cu posibilitatea de a corela și filtra aceste evenimente pentru a iniția acțiuni automate.

Automatizarea proceselor interinstituționale

În context guvernamental, unde schimbul de date între instituții este critic, soluția va permite:

- crearea de procese automate interinstituționale pe baza API-urilor expuse de fiecare entitate;
- trasabilitate completă asupra fiecărei tranzacții, cu înregistrarea detaliată a evenimentelor și generarea de rapoarte pentru audit și conformitate;
- reducerea timpilor de răspuns prin eliminarea operațiunilor manuale redundante și orchestrarea automată a schimburilor de date.

Suport multi-limbaj de programare

Pentru a sprijini o gamă variată de dezvoltatori și instituții, soluția va asigura suport nativ pentru generarea și consumul de cod scris în mai multe limbaje de programare, inclusiv, dar fără a se limita la: Node.js, Deno, Python, PHP, Java, C# etc. Astfel, consumatorii de API-uri vor putea integra rapid serviciile expuse în aplicații diverse, reducând timpul de dezvoltare și facilitând interoperabilitatea între platforme. Cerințe obligatorii:

- posibilitatea de selectare a versiunii de runtime pentru limbaje precum PHP (minimum 5.6, 7.4, 8.2, 8.3) și Java (minimum 8, 11, 17, 21), pentru a garanta compatibilitatea

- aplicațiilor existente cu cele noi;
- suport pentru utilizarea librăriilor și pachetelor externe, prin intermediul managerilor de pachete specifici fiecărui limbaj (Composer pentru PHP, Maven/Gradle pentru Java, pip pentru Python, npm pentru Node.js);
 - mecanisme de sandboxing și izolare a execuțiilor, care să asigure rularea sigură a librăriilor externe și protecția mediului de producție.

Suport pentru limbaje de scripting și administrare

Soluția va asigura:

- Execuție scripturi Bash și Shell: pentru integrarea rapidă a scripturilor existente utilizate în procesele de administrare Linux/Unix;
- Suport PowerShell: pentru medii Windows, cu posibilitatea de a rula cmdlet-uri și scripturi complexe de administrare a sistemelor;
- Execuție comenzi prin SSH: pentru conectarea securizată la servere și echipamente externe, permițând automatizarea sarcinilor de mentenanță sau colectare de date;
- Management variabile de mediu și secrete: integrare cu Vault pentru stocarea și utilizarea în siguranță a credențialelor, cheilor SSH și altor date sensibile;
- Logare și audit detaliat: fiecare execuție de script (Bash, PowerShell sau SSH) va fi înregistrată, cu trasabilitate completă pentru conformitate și audit.

Funcționalități suplimentare

- integrarea cu mecanismele de securitate definite în secțiunea precedentă (inclusiv RBAC, autentificare multiplă și criptare end-to-end);
- posibilitatea de definire și configurare a proceselor automatizate prin interfață vizuală și/sau scripting;
- suport pentru integrarea cu notificări, sisteme de alertare și instrumente de monitorizare existente;
- planificarea execuțiilor (cron-like): posibilitatea de a rula scripturi la intervale regulate sau pe baza unor condiții/triggere;
- execuții paralele și izolate: rularea simultană a mai multor scripturi cu izolare completă a mediului;
- bibliotecă de scripturi reutilizabile: un repository centralizat de scripturi validate ce pot fi reutilizate în fluxuri de lucru diferite;
- capacitatea de a scala și replica fluxurile de lucru în medii containerizate și distribuite.

3.8.7. Platforma pentru administrarea identității utilizatorilor

Soluția va cuprinde o platformă de gestiune a identității utilizatorilor în cadrul sistemelor și aplicațiile din cadrul instituției, asigurând administrarea centralizată a rolurilor și

permisiunilor utilizatorilor, provizionarea identitatii si a conturilor de utilizator in aplicatii. Solutia trebuie sa fie un instrument disponibil commercial (COTS- Commercial off the Shelf) si sa ofere posibilitatea de a rula pe diverse platforme hardware, pe sistemele de operare majore existente pe piata (Windows, Linux), precum si posibilitatea de a rula intr-o infrastructura Kubernetes. Componenta de management centralizat a identitatii utilizatorilor trebuie sa indeplineasca urmatoarele cerinte functionale:

- Automatizeaza procesul de acordare si eliminare a conturilor, drepturilor de acces si a rolurilor de aplicatie catre utilizatori in sistemele si aplicatiile din cadrul institutiei;
- Stocheaza informatii despre profilul utilizatorilor precum si conturile, permisiunile acestora in raport cu functia pe care o au in cadrul institutiei;
- Asigura sincronizarea si reconcilierea automata a informatiilor de identitate utilizatori intre sisteme;
- Garanteaza eliminarea conturilor de acces, a drepturilor si permisiunilor utilizatorilor in sistemele si aplicatiile interne atunci cand angajatul paraseste institutia;
- Propaga si sincronizeaza automat modificarile aparute in profilul utilizatorilor in sistemele gestionate;
- Oferă o interfata unica de tip self-service pentru utilizatori prin care acestia pot solicita conturi si permisiuni in aplicatii si sisteme;
- Faciliteaza dezvoltarea de fluxuri de acordare si aprobare conturi in sistemele si aplicatiile interne;
- Faciliteaza integrarea cu sistemele existente prin intermediul de conectori specifici fiecarui sistem in parte;
- Oferă capabilitati de monitorizare si auditare.

Pentru indeplinirea acestor cerinte functionale platforma trebuie sa fie o solutie robusta, performanta si flexibila care sa permita administratorilor sa gestioneze centralizat politicile de acces, fluxurile de aprobare si propagare a conturilor si permisiunilor in aplicatiile si sistemele institutiei, oferind in acelasi timp capabilitati de auditare si raportare asupra activitatilor efectuate in cadrul platformei.

Componenta de management centralizat a identitatii utilizatorilor

Componenta de management centralizat a identitatii utilizatorilor trebuie sa includa un portal prin intermediul caruia utilizatorii pot sa solicite accesul la aplicatii, sisteme, roluri si permisiuni. Portalul trebuie sa includa instrumente de tip wizard prin intermediul caruia se pot realiza cereri de acces, utilizatorul avand la dispozitie instrumente personalizate in functie de pozitia pe care acesta o indeplineste in cadrul institutiei. Pentru a creste eficienta operatiilor de administrare, componenta trebuie sa includa mecanisme care sa permita provizionarea simultana de conturi si drepturi de acces pentru mai multi utilizatori. Utilizatorii vor putea sa isi modifice datele personale de profil, sa delege catre alte persoane din cadrul institutiei activitatea de aprobare a cererilor de acces. Rolurile si drepturile de acces in aplicatiile si sistemele institutiei vor fi gestionate printr-un catalog centralizat,

gestionat de către administratorul platformei.

Componenta de management centralizat a identității utilizatorilor trebuie să permită definirea de politici de aprobare care să 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 a identității utilizatorilor trebuie să ofere posibilitatea de a defini politici asociate parolilor 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 a identității utilizatorilor trebuie să ofere posibilitatea de a defini în mod grafic atribute asociate utilizatorilor, rolurilor, precum și tipul de date al atributelor (ex: număr sir de caractere, numeric, lista de valori, tip date). 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 rularilor.

Componenta de management centralizat a 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 și parametri în determinarea intervalului de atestare informații precum gradul de confidentialitate 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 baza de reguli definite de către administrator. Platforma trebuie să fie capabilă să trimită notificări automate

catre 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 a 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 baza de protocoale și formate de date diferite.

Componenta de management a 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 adaptori standard pentru baze de date relationale, 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, SMS;
- 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 redirectionată către alți administratori în funcție de politicile de aprobare definite;
- Trebuie să permită definirea de fluxuri ad-hoc pentru a solicita informații suplimentare;
- Interfetele definite în cadrul fluxurilor de aprobare să poată fi dezvoltate pe baza limbajului 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

evidentiindu-se actorii participanti, intervalul de timp si datele pe baza carora au fost luate deciziile pe fluxul de aprobare.

Solutia trebuie sa includa in mod standard o lista de rapoarte predefinite:

- Raport politici de acces asociate rolurilor, raport politici de acces asociate aplicatiilor din institutie;
- Rapoarte de atestare utilizatori, roluri, permisiuni de aplicatie, aplicatii institutiei precum si rapoarte pentru lista de atestari efectuate si drepturi si conturi eliminate in urma procesului de certificare;
- Raport lista conturi orfane pe aplicatie;
- Raport cereri de acces in aplicatii institutiei;
- Raport istoric permisiuni de acces utilizatori;
- Rapoarte asociate parolelor utilizatorilor (ex: parole expirate);
- Raport istoric profil utilizatori;
- Raport utilizatori stersi, dezactivati;
- 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 sa ofere posibilitatea de a exporta rapoartele generate in formate diverse, minim PDF si HTML. Generarea de rapoarte se va realiza la cererea administratorilor sau automat la o data si un interval de timp predefinit, livrarea rapoartelor se va realiza pe email, server FTP, HTTP.

Componenta de control acces

Solutia trebuie sa includa un sistem centralizat de management a accesului la aplicatii si sa ofere functionalitati de single sign-on, autentificare, autorizare, administrare centralizata, managementul agentilor de autorizare si a politicilor de acces, management in timp real a sesiunilor de aplicatii si audit.

Solutia trebuie sa fie un instrument disponibil commercial (COTS- Commercial off the Shelf) si sa ofere posibilitatea de a rula pe diverse platforme hardware, pe sistemele de operare majore existente pe piata (Windows, Linux), precum si posibilitatea de a rula intr-o infrastructura Kubernetes.

Rolul acestui sistem este de crestere a securitatii prin politici globale de securitate si eliminarea riscurilor potentiale, prevenirea accesului neautorizat la sisteme si aplicatiile institutiei, simplificarea operatiilor de administrare prin reducerea si automatizarea numarului de operatiuni administrative.

Componenta de control acces va identifica utilizatorul la inceputul sesiunii de lucru prin redirectarea catre un ecran de autentificare. Ca si mekansime de autentificare, solutia va suporta minim urmatoarele:

- utilizator si 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 precum și activitățile 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, componența va permite filtrarea autentificării și autorizării pe baza unor reguli avansate utilizând diverse criterii: adresa IP, dispozitivul folosit, tipul de browser folosit, interval orar.

Componența 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.

Componența trebuie să ofere capacități de grupare politici de acces pe zonă 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.

Componența 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 cauta, 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 capacități 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 bază 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.

Componența 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 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 2 furnizori de identitate;
- permite accesul la resursele protejate pe baza de politici de acces la nivel de atribute despre profilul utilizatorilor

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

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

- Rapoarte asociate procesului de autentificare grupate pe sistem, adresă 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 profilelor de utilizatori într-un director de tip LDAP și să ofere posibilitatea de a rula pe diverse platforme hardware și sisteme de operare.

Administrarea și editarea profilelor 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. Profilele utilizatorilor trebuie să poată fi extinse prin adăugare de noi atribute pentru a asigura compatibilitatea sistemului cu module suplimentare.

Componenta de stocare centralizată a profilelor 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 mare în definirea regulilor de acces.

Soluția oferă mecanisme de unificare mai mult 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 capacitatea 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. Profilele de utilizator vor putea fi extinse prin adăugarea de noi atribute, acestea fiind administrate și editate prin intermediul unor profile de utilizatori.

Soluția va oferi mecanisme de extindere a funcționalităților standard utilizând plug-in-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 profile și parole de utilizatori).

3.8.8. Componenta de securizare a accesului privilegiat

Această componentă are rolul de a proteja, gestiona și monitoriza accesul privilegiat la resursele critice ale sistemului PNI. 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.

Platforma trebuie să fie o aplicație software disponibilă comercial (COTS) cu licențiere perpetuă sau sub formă de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție.

Această componentă trebuie să îndeplinească următoarele cerințe de bază:

- Soluția trebuie să aibă posibilitatea de a oferi acces pe baza 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 să 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.

- Solutia trebuie sa permită definirea de politici de acces individualizate pentru sisteme, in functie de rolul acestora.
- Soluția trebuie să asigure suplimentarea controalele native furnizate de sistemul de operare pentru Fișiere și Directoare (atat pentru sisteme Windows cat si Linux/Unix), astfel încât să asigure cel puțin controlul operațiilor de: read, write, execute, create, delete, rename, chown și chmod asupra fișierelor și directoarelor.
- Solutia trebuie sa detina o certificare de securitate emisa de o institutie independenta recunoscuta international - Common Criteria sau echivalent.
- Solutia trebuie sa ofere posibilitatea eliminarii conturilor administrative comune prin implementarea functionalitatilor de delegare a sarcinilor administrative, administratorii avand drepturi doar la componentele necesare indeplinirii sarcinilor.
- Solutia trebuie sa ofere politici predefinite care sa fie in conformitate cu bunele practici de securitate.
- Solutia trebuie sa permită definirea de politici pentru implementarea unei functionalitati de tip firewall in functie de porturi, adresa sursa, tipul conectarii precum si timp. Aceasta functionalitate trebuie oferita atât pentru conexiunile egress cat si pentru cele ingress.
- Solutia trebuie sa permită definirea de politici de securitate ce pot fi distribuite pe grupuri de servere, indiferent de domeniul din care acestea fac parte
- Solutia trebuie sa ofere posibilitatea administrarii si definirii de politici intr-un mod centralizat, indiferent de sistemul de operare care ruleaza pe sisteme.
- Solutia trebuie sa suporte definirea de roluri, astfel încât pe baza grupurilor din care face parte utilizatorul, sa i se permită accesul la diferite functionalitati.
- Solutia trebuie sa suporte criptarea datelor transmise prin retea si a datelor aplicatiei
- Solutia trebuie sa ofere functionalitati de administrare a parolelor conturilor partajate si privilegiate.
- Solutia trebuie sa permită accesul utilizatorilor la parolele conturilor privilegiate pe baza de reguli de access. Regulile de acces trebuie sa poată fi create si modificate de către administratorul solutiei.
- Solutia trebuie sa ofere posibilitatea integrarii cu aplicatii dezvoltate in-house in vederea schimbarii parolelor.
- Solutia trebuie sa ofere suport pentru a putea extrage parolele din sistem, folosind linia de comanda si 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.
- Solutia trebuie sa permită utilizatorilor folosirea conturilor inregistrate in sistem, fără ca acestia sa poată vedea parola prin folosirea unei metode de tip login automat.
- Solutia trebuie sa suporte cel puțin protocolul RDP, SSH si Telnet pentru loginul automat.
- Solutia trebuie sa ofere posibilitatea autentificarii utilizatorului in mod automat pentru sesiunile SSH, Telnet, RDP prin folosirea interfetei web, intreaga sesiune fiind

inregistrata si stocata. Solutia trebuie sa puna la dispozitie optiunea de a vizualiza din interfata web sesiunile inregistrate.

- Solutia trebuie sa extraga comenzile rulate in cadrul sesiunilor SSH si Telnet si sa le ataseze inregistrarii sesiunii. Pentru fiecare sesiune, inregistrarea cat si lista comenzilor executate trebuie sa poata fi vizualizate in interfata web.
- Pentru conturile cu un grad mare de risc, solutia trebuie sa ofere posibilitatea definirii unui proces de aprobare, astfel incat inaintea folosirii contului, utilizatorul sa ceara aprobarea unei alte persoane. Accessul la cont sa se permita numai dupa obtinerea aprobarii.

3.8.9. Monitorizare date, sisteme și aplicații

Având în vedere complexitatea tehnică și funcțională a sistemului PNI , precum și importanța acestuia, devine esențială necesitatea implementării unei soluții de management de aplicații care să elimine discontinuitatea serviciilor oferite de IT către zona funcțională, unificând în acest fel cele două componente.

Platforma pentru monitorizarea performanței infrastructurii va conlucra pentru 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.

Platforma trebuie să fie o aplicație software sau o suită de aplicații integrate disponibile comercial (COTS) cu licențiere perpetuă sau sub forma de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție.

Platforma trebuie să asigure următoarele funcționalități minimale:

- Monitorizarea unificată a aplicațiilor, bazelor de date, infrastructurii hardware și software
- Generare de alerte bazate pe reguli prestabilite pentru fiecare tehnologie în parte
- Integrarea cu sistemul LDAP, cu definirea de roluri tehnologice și de securitate pentru acces diferențiat
- Platforma trebuie să fie capabilă să:
 - ofere tablouri de bord intuitive, asigurând astfel o învățare ușoară și rapidă a soluției;
 - ofere panouri de control predefinite pentru:
 - o Administrarea soluției
 - o Monitorizarea bazelor de date
 - o Monitorizarea sistemelor de operare
 - o Monitorizarea LDAP
 - o Monitorizarea infrastructurilor de virtualizare și a sistemelor hibride
 - o Monitorizarea containerelor
- Să ofere posibilitatea definirii de panouri de control personalizate;

- Să furnizeze o paletă foarte largă de șabloane predefinite pentru monitorizarea elementelor de infrastructură, pentru generarea de rapoarte, precum și posibilitatea construirii de rapoarte personalizate;
 - Să permită generarea automată de rapoarte la intervale predefinite și transmiterea acestora prin e-mail către utilizatori predefiniți;
 - Să furnizeze mecanisme de notificare prin care să transmită alerte prin email și SMS atunci când anumite praguri critice sunt depășite.
 - Platforma trebuie să asigure monitorizarea infrastructurii hardware și software:
- ✓ **Monitorizarea sistemului de virtualizare - platforma trebuie să realizeze:**
- identificarea și diagnosticarea problemelor de performanță la nivelul infrastructurii de virtualizare.
 - monitorizarea la nivel de sistem de operare Windows/Linux/Unix.
 - monitorizare pentru tehnologii de virtualizare multiple, incluzând cel puțin: VMware vSphere, Microsoft Hyper-V și Citrix
 - analiza a proceselor active pentru a determina care dintre acestea afectează performanțele mașinilor virtuale și care mașini virtuale nu utilizează eficient resursele.
 - să includă o interfață predefinită de prezentare în timp real în format tabelar și grafic a metricilor (parametrilor de funcționare) a infrastructurii de virtualizare care să conțină date intuitive, cu panouri de control dedicate care să prezinte o imagine de ansamblu și de detaliu a infrastructurii de virtualizare.
 - monitorizarea metricilor de performanță pentru fiecare mașină virtuală - cel puțin încărcare CPU, memorie, disc, interfață de rețea să asigure declanșarea de acțiuni automate complexe, ca de exemplu: re-configurare rețea sau re-alocare resurse mașini virtuale pe baza datelor detectate astfel încât să asigure remedierea automată a problemelor de performanță;
 - monitorizarea în detaliu a soluțiilor de containerizare și clusterizare a containerelor - cel puțin Docker, Kubernetes/ Google Kubernetes și să asigure declanșarea de acțiuni automate complexe, ca de exemplu: reconfigurare cluster, alocare resurse suplimentare, repornire/oprire container pe baza datelor detectate astfel încât să asigure remedierea automată a problemelor de performanță;
 - monitorizarea apariției unui anumit text în fișiere de jurnal (log) și să asigure declanșarea de acțiuni automate complexe, ca de exemplu: re-configurare rețea sau re-alocare resurse mașini virtuale pe baza datelor detectate în fișierele jurnal (log);
 - determinarea în mod automat a performanței "normală" de funcționare a componentelor de infrastructură monitorizate și să determine modele de funcționare normală bazate pe oră, zi, săptămână etc. De asemenea, soluția trebuie să asigure capacitatea de a genera alarme / evenimente în cazul depășirii valorilor normale de funcționare;
 - identificarea configurației hardware și software a serverelor și să detecteze automat orice modificare a configurației acestora (modificare configurație hardware, instalare / dezinstalare software etc) cu generarea automată a unei alerte;

- distribuirea automată, de la distanță de patch-uri de securitate, update-uri de sisteme de operare precum și de noi aplicații sau noi versiuni ale aplicațiilor specifice de business;
- ✓ **Monitorizarea sistemelor de operare**
 - Platforma trebuie să permită monitorizarea sistemelor de operare care stau la baza aplicațiilor, bazelor de date și dispozitivelor de rețea din infrastructura IT. În acest sens, va permite colectarea parametrilor de funcționare la nivel de CPU, memorie, intrări/ieșiri, tendințe de utilizare a spațiului de stocare, precum și a proceselor care rulează pe fiecare server / mașină virtuală. Toate aceste date vor fi agregate cu datele legate de diverse evenimente, date de monitorizare a bazelor de date și infrastructurii de virtualizare pentru furnizarea unei monitorizări globale a performanței sistemului;
 - Platforma trebuie să ofere o perspectivă similară (model unificat) a colecțiilor de resurse monitorizate indiferent de sistemul de operare monitorizat;
 - Platforma trebuie să asigure capabilități de diagnosticare grafică afișând metrici în timp real și oferind posibilitatea de a naviga la metrici conexe efectuând click pe reprezentările grafice (drill-down).
 - Platforma trebuie să asigure:
 - monitorizarea conținutului fișierelor log și să genereze alarme atunci când identifică anumite expresii definite;
 - monitorizarea timpului de răspuns la accesarea diferitelor URL-uri;
 - identificarea blocajelor la nivelul sistemelor de operare prin monitorizarea fluctuațiilor la nivel de procese;
 - prezentarea parametrilor de funcționare (CPU, memorie rețea, utilizare disc) în timp real pentru un număr configurabil de sisteme, astfel încât să ofere o imagine de ansamblu asupra stării de funcționare a infrastructurii IT la nivel de sistem de operare, cu afișarea alarmelor pe diferite niveluri de severitate;
- ✓ **Monitorizarea LDAP**
 - Platforma trebuie să detecteze, diagnosticheze și să rezolve problemele de performanță, disponibilitate și replicare la nivelul LDAP atât în medii fizice cât și virtuale;
 - Platforma trebuie să dispună de un panou de control dedicat ce prezintă o imagine de ansamblu a infrastructurii LDAP (numărul de incidente de tip normal, avertisment, critic, fatal) la nivel de forest, domeniu, site, controler de domeniu;
 - Soluția trebuie să includă o serie de rapoarte cu informații referitoare la disponibilitatea și performanțele LDAP, printre care:
 - Rapoarte referitoare la alarmele LDAP
 - Rapoarte de utilizare, precum și rapoarte de sumar și de detaliu ale resurselor hardware pentru controlerul de domeniu
 - Soluția trebuie să includă o interfață de prezentare în timp real în format tabelar și grafic a metricilor (parametrilor de funcționare) la nivel de controler de domeniu - nivelul de consumare al resurselor (CPU, memorie, spațiu disc, rețea) precum și un

clasament al serverelor controler de domeniu pe tip de resursă consumată (CPU, memorie, rețea, spațiu disc) la nivel de site;

- Soluția trebuie să includă o interfață de administrare a regulilor ce condiționează severitatea incidentelor la nivelul LDAP cu posibilitatea sortării acestora după gradul de severitate, stare activă/inactivă.

✓ **Monitorizarea rețelei**

- Platforma trebuie să monitorizeze funcționarea și disponibilitatea dispozitivelor de rețea;
- Platforma trebuie să asigure următoarele funcționalități:
 - Să fie capabilă să colecteze informații despre tranzacțiile echipamentelor de rețea prin intermediul ICMP (Internet Control Message Protocol);
 - Să poată afișa atât informații privind disponibilitatea dispozitivelor de rețea, cât și performanța acestora;
 - Să permită adăugarea/modificarea/eliminarea manuală a dispozitivelor și locațiilor de rețea și configurarea parametrilor de colectare pentru acestea;
 - Să permită configurarea intervalului la care se efectuează colectarea datelor;
 - Să permită verificarea rapidă a disponibilității unui dispozitiv, fără a necesita colectarea de date despre performanța acestuia;
 - Să permită configurări avansate pentru colectarea de date, cum ar fi numărul și mărimea pachetelor de ping, sau timpul maxim de așteptare pentru Trace Route;
 - Să poată colecta și afișa date de disponibilitate, timp de răspuns și pachete pierdute referitoare la performanța echipamentelor de rețea.

✓ **Monitorizarea bazelor de date**

- Platforma trebuie să poată monitoriza platforme eterogene de baze de date, ajutând astfel la reducerea costurilor administrative și la îmbunătățirea nivelului serviciilor. Trebuie să poată monitoriza cel puțin următoarele soluții de baze de date: Cassandra, DB2, MongoDB, Microsoft SQL Server, MySQL, Oracle (inclusiv RAC), PostgreSQL.
- Platforma trebuie să asigure următoarele capabilități:
 - Să ofere interfețe unitare pentru toate platformele de baze de date;
 - Să poată monitoriza baze de date instalate fie pe medii fizice, fie pe medii virtuale;
 - Să monitorizeze componentele bazelor de date pentru a asigura funcționarea acestora în limitele capacității resurselor;
 - Să ofere o vizualizare de ansamblu a stării de sănătate a tuturor instanțelor bazelor de date;
 - Să descopere când se produc degradări ale performanței execuției de fraze SQL;
 - Să declanșeze alarme atunci când anumite valori de referință sunt încălcate;
 - Să poată colecta date fără necesitatea instalării unui agent local, ci prin agenți la distanță, asigurând astfel un consum minim de resurse suplimentare;

- Să dispună de un mecanism de eliminare a alarmelor false prin impunerea de praguri adaptive, să poată fi programate perioade de oprire și mentenanță, în care generarea de alarme va fi suprimată.

3.8.10. Soluție de disaster recovery

La nivelul sistemului PNI se va implementa o soluție de disaster recovery care să faciliteze procesul de recuperare a componentelor software și a datelor stocate în cazul unui dezastru. Acesta soluție va automatiza și gestiona procesele esențiale necesare pentru a restabili funcționalitatea operațională a sistemului PNI din cadrul Cloud-ului Privat Guvernamental în Centrul de Date STS din Cristian, Jud. Brașov după evenimente neprevăzute precum întreruperi de curent, erori umane, atacuri cibernetice, sau dezastre naturale.

Soluția trebuie să fie o aplicație software disponibilă comercial (COTS) cu licențiere perpetuă sau sub forma de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție.

Cerințe tehnice

Soluția va include o funcție de replicare a mașinilor virtuale către sisteme ce folosesc aceeași platformă de virtualizare:

- replicarea trebuie să fie posibilă atât sincron cât și asincron și trebuie să poată fi definită la nivel de mașină virtuală, cu granularitate până la nivel de disc virtual, disc fizic prezentat mașinii virtuale;
- funcția trebuie să fie prezentă la nivelul interfeței unificate de management a soluției HCI, fără a fi necesară o altă interfață pentru administrarea soluției de replicare;
- în cazul detectării unor latențe mari, datorate unor probleme de conectivitate între centrele de date, soluția de replicare trebuie să poată comuta automat din modul sincron în modul asincron, pentru a nu impacta performanța mașinilor virtuale replicate;
- funcția de replicare va realiza jurnalizarea tuturor operațiunilor de scriere, astfel încât să fie posibilă restaurarea datelor la momente de timp predefinite sau definibile de către utilizator, cu o granularitate la nivel de secundă;
- replicarea la distanță a mașinilor virtuale trebuie să utilizeze capabilități de deduplicare și compresie a datelor transmise pentru a eficientiza transferul acestora de la un centru de date la altul;
- replicarea la distanță a mașinilor virtuale trebuie să se poată realiza în diverse arhitecturi: local, cascadă, un centru de date către mai multe (cel puțin unul la patru), mai multe centre de date către unul (cel puțin patru la unul), combinații ale acestora;
- automatizează procesul de failover și failback al mașinilor, grupurilor de mașini virtuale (din același punct de consistență) între centrele de date;

- funcția de replicare trebuie să fie licențiată (dacă este cazul) indiferent de numărul mașinilor virtuale care vor fi create pe infrastructura HCI propusă.

Soluția de disaster recovery propusă va dispune de următoarele funcționalități:

- Asigură protecția sistemelor virtualizate și fizice, la nivel de imagine, a sistemului de operare, a fișierelor, integrat cu aplicațiile ce rulează pe aceste sisteme, prin politici de protecție flexibile și distincte.
- Include suport pentru protecția atât a workload-urilor tradiționale (inclusiv Oracle, Exchange, SQL, SAP HANA) cât și pentru sisteme de fișiere, containere Kubernetes și medii virtuale VMware, Hyper-V, Red Hat Virtualization, oVirt, Oracle VM.
- Soluția trebuie să poată susține nativ protecția stațiilor de lucru tip MS Windows, Linux.
- Soluția trebuie să protejeze sisteme de operare de tipul Microsoft Windows, Linux CentOS, Debian, Red Hat, SuSE, Ubuntu, Oracle Linux, AIX, HP-UX și Solaris.
- Soluția trebuie să protejeze prin module dedicate aplicații ca Microsoft Exchange, Microsoft SQL, Microsoft SharePoint, Oracle, SAP, SAP HANA, DB2, Informix, MySQL, PostgreSQL și Sybase.
- Soluția va permite protecția oricăror tipuri de baze de date și aplicații, chiar și a celor nespecificate în matricea de complianță, prin mecanisme native de salvare direct către appliance-urile hardware, software dedicate stocării datelor protejate, utilizând capabilitățile de deduplicare și compresie la sursă.
- Soluția va permite definirea și rularea unor rutine ca parte a procesului de protecție a unei aplicații, rutine ce vor rula înainte sau imediat după desfășurarea procesului de salvare a datelor în funcție de cerințele specifice aplicației din mediul de producție.
- Soluția va oferi posibilitatea ca cererile de restaurare operațională să se facă dintr-un set de date complet, tip full backup set, indiferent de politicile de protecție definite și fără transfer de date adițional între aplicația de salvare a datelor și echipamentul dedicat stocării datelor deduplicate.
- Susține o deduplicare a datelor, la sursă sau destinație, utilizând un mecanism global de segmentare variabilă a fiecărui proces de protecție indiferent de rețea sau protocolul de transfer utilizat.
- Soluția propusă trebuie realizeze monitorizarea tuturor componentelor soluției, într-o singură interfață grafică ce va permite personalizarea informațiilor în funcție de cerințele administratorului integrând parametrii de stare a sistemelor și aplicațiilor din producție.
- Soluția trebuie să ofere posibilitatea de a scoate rapoarte combinate, în format grafic, cu informații preluate de la sistemele sursă până la cele de destinație a proceselor de salvare pentru un client, o imagine de sistem sau pentru protecția unei aplicații.
- Soluția va permite protecția unui număr nelimitat de mașini virtuale și de aplicații ce rulează pe sistemele licențiate conform matricei de compatibilități a producătorului.
- Licențierea soluției de salvare și replicare a datelor de producție trebuie să includă

un minim de 20 de procesoare fizice cu posibilitatea extinderii ulterioare.

- Licențierea soluției va fi independentă de cantitatea de date protejate, salvate, de numărul mașinilor virtuale.

3.8.11. Componenta SIEM

Componenta pentru Managementul Incidentelor de Securitate (SIEM) trebuie să îndeplinească următoarele cerințe minime:

- să fie o aplicație software sau o suită de aplicații de la același producător disponibile comercial (COTS) cu licențiere perpetuă sau sub forma de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție;
- toate funcționalitățile oferite de ofertant trebuie confirmate prin citate și/sau extrase din documentația producătorului disponibilă public (se transmite documentația tehnică în cadrul Propunerii Tehnice). În caz de neconcordanță între documentația producătorului și ofertă primează documentația producătorului;
- să fie oferită ca appliance hardware sau software, cu funcțiile interne securizate de producător;
- Soluția trebuie să ofere capabilități de monitorizare real-time a device-urilor de securitate, switch-uri și routere de rețea, sisteme Windows și Unix/Linux, servere de aplicații, servere de baze de date și soluții de stocare
- Soluția trebuie să identifice atacuri în timpul colectării datelor
- Soluția trebuie să ofere posibilitatea colectării de log-uri, iar arhitectura de stocare trebuie să suporte stocarea datelor atât online cât și arhivat pentru investigații
- Soluția trebuie să ofere posibilitatea colectării de evenimente din segmente de rețea separate la nivel de firewall sau locație geografică
- Soluția trebuie să ofere monitorizarea traficului de rețea prin captura acestuia în mod continuu și prin monitorizarea unor metadate de tip flow
- Soluția trebuie să poată stoca log-urile colectate la nivelul fiecărei locații geografice atât online cât și arhivat în locația geografică de unde acestea au fost colectate
- Soluția trebuie să ofere prin intermediul unei console centrale vizibilitate unificată asupra întregii infrastructuri de comunicații prin agregarea datelor primite pe baza traficului de rețea și loguri de la diferite sisteme, precum și detecția rapidă a incidentelor de securitate și a utilizării incorecte a resurselor de rețea
- Soluția trebuie să permită crearea incidentelor de securitate atât manual cât și automat
- Soluția trebuie să ofere o interfață de vizualizare a alertelor și incidentelor de securitate
- Soluția trebuie să ofere posibilitatea criptării transmisiei datelor
- Soluția trebuie să garanteze integritatea informațiilor colectate
- Soluția trebuie să aibă opțiunea de a adăuga componente fără a fi nevoie de înlocuirea hardware-ului existent, a software-ului sau a licențelor
- Soluția trebuie să ofere posibilitatea de a rula query-uri în timp real pentru detecția anomaliilor

- Soluția trebuie să ofere posibilitatea raportării și investigării pe datele stocate
- Soluția trebuie să ofere posibilitatea instalării componentelor în mediu virtual sau fizic
- Soluția trebuie să includă licențele necesare atât pentru sistemele de operare, cât și pentru aplicațiile specifice
- Soluția trebuie să colecteze datele în format brut cu performanțe ridicate de analiză în timp real
- Interfața web a soluției trebuie să suporte cel puțin următoarele opțiuni de investigare detaliată: drill-down, interogare pe o informație specifică, filtre și căutări
- Soluția trebuie să ofere posibilitatea de a salva profile pentru vizualizarea log-urilor și pentru scopuri de investigații
- Soluția trebuie să ofere cel puțin configurarea următoarelor intervale de timp pentru realizarea investigațiilor: ultima, ora, ultimele 24 ore, ultimele 2 zile și interval de timp personalizat
- Soluția trebuie să ofere capabilități de corelare de bază în timp real
- Soluția trebuie să ofere capabilități de investigare detaliată direct din pagina de sumarizare a evenimentelor
- Soluția trebuie să ofere posibilitatea creării și administrării regulilor de corelare direct din interfața web, fără a fi nevoie de unelte terțe adiționale
- Soluția trebuie să ofere capabilități de alertare pentru regulile de corelare folosind cel puțin: SMTP și Syslog
- Soluția trebuie să ofere posibilitatea rulării de scripturi în momentul identificării unei alerte
- Soluția trebuie să ofere posibilitatea de a modifica criticitatea alertelor generate
- Soluția trebuie să ofere o interfață pentru construcția de reguli pentru rapoarte, diagrame, alerte și, corelări, suficient de flexibilă și fără a fi nevoie de limbaje de scripting complexe
- Soluția trebuie să ofere suport pentru descărcarea și instalarea actualizărilor aplicației direct din consola web sau din linia de comandă
- Soluția trebuie să permită crearea de tablouri de bord personalizate
- Soluția trebuie să ofere posibilitatea investigării detaliată (drill-down) direct din tablourile de bord
- Soluția trebuie să ofere acces pe bază de roluri
- Soluția trebuie să permită autentificare prin Active Directory sau Pluggable Authentication Modules (PAM)
- Soluția trebuie să ofere interfață web cu suport HTML5
- Soluția trebuie să ofere posibilitatea de a crea parsere personalizate pentru sursele de evenimente ce nu sunt suportate standard
- Soluția trebuie să ofere posibilitatea monitorizării surselor de evenimente pentru cazul în care sursa nu mai trimite evenimente sau se închide
- Soluția trebuie să ofere posibilitatea colectării log-urilor fără agent, agentul fiind folosit numai în cazurile în care colectarea fără agent nu este posibilă pentru sursa de evenimente

- Soluția trebuie să ofere posibilitatea de secretizare a informațiilor din evenimentele colectate
- Soluția trebuie să ofere funcționalități de auditare ale sistemului
- Soluția trebuie să ofere posibilitatea alertării utilizatorilor în cazul identificării unui incident de securitate
- Soluția trebuie să ofere conectivitate externă cu serviciile de cloud ale furnizorilor pentru descărcarea de informații adiționale: APT, definiții Botnet, rețele malițioase, zero-day/compromitere, rapoarte suplimentare, parsere noi, reguli pentru rapoarte și diagrame
- Soluția trebuie să permită introducerea în analiză a informațiilor ce provin de la alte tipuri de tehnologii cum ar fi web-proxy, IDS/IPS, firewall sau NAC
- Soluția trebuie să includă informații GeolP în scopuri de investigații
- Soluția trebuie să ofere funcționalități de raportare. Rapoartele trebuie să includă cel puțin accesul bazat pe roluri: read&write, read only, no access
- Soluția trebuie să suporte expresii regulate (RegEx) pentru crearea rapoartelor
- Soluția trebuie să ofere cel puțin următoarele opțiuni la afișarea rapoartelor: tabular, area, bar, column, line, pie, spline
- Soluția trebuie să ofere opțiunea de a programa rularea rapoartelor: ad-hoc, ora de ora, zilnic, săptămânal, lunar
- Soluția trebuie să permită export-ul rapoartelor cel puțin în format PDF și CSV
- Soluția trebuie să ofere rapoarte, reguli și diagrame predefinite. Personalizarea rapoartelor, regulilor și diagramelor trebuie să fie posibilă
- Soluția trebuie să ofere posibilitatea de a configura Identity Feed pentru a adăuga domenii Active Directory, stații și utilizatori pentru log-uri și sesiuni non-Windows
- Soluția trebuie să ofere posibilitatea de a configura liste pentru obținerea de informații contextuale despre stații, utilizatori sau adrese IP
- Soluția trebuie să fie capabilă să automatizeze și să orchestreze răspunsul și mitigarea pentru incidentele de securitate
- Soluția trebuie să dispună de mecanisme complet automate de prelucrare a incidentelor de securitate, mecanisme capabile să fie declanșate automat sau manual la intervenția utilizatorului
- Soluția trebuie să fie capabilă să identifice utilizarea incorectă a conturilor cu privilegii de administrare
- Soluția trebuie să fie capabilă să identifice schimbarea credențialelor de acces și a privilegiilor de acces
- Soluția trebuie să fie capabilă să identifice login-urile administrative neuzuale în funcție de locație, timp sau durată.
- Soluția trebuie să fie capabilă să identifice accesul utilizatorilor de administrare cu credențialele compromise
- Soluția trebuie să fie capabilă să identifice și să clasifice incidentele de securitate, inclusiv faza atacului și riscul acestuia

- Soluția trebuie să fie capabilă să identifice traficul generat de Botnet, DDoS, scanări de vulnerabilitate, bitcoin, tunelare http/dns, command and control, exfiltrare, remote administration tools
- Soluția trebuie să fie capabilă de identificare a atacurilor pe baza de IOC introduse în sistem folosind STIX
- Soluția trebuie să fie capabilă de identificare a atacurilor de tip “Remote Execution of Procedure Call”
- Soluția trebuie să fie capabilă de detectie a atacurilor necunoscute pentru care nu exista semnături specifice
- Soluția trebuie să fie capabilă de gestionare a informațiilor de trafic atât din mediul virtual cât și din mediul fizic
- Soluția trebuie să dispună de un tool de management a cazurilor pentru incidentele de securitate procesate cu posibilitatea de adăugare de note și fișiere de către utilizatori
- Soluția trebuie să fie capabilă să folosească feed-uri de securitate comerciale și open source configurabile de către utilizator
- Soluția trebuie să ofere posibilitatea de a limita evenimentele vizibile de către un utilizator în funcție de rolul acestuia
- Soluția trebuie să ofere posibilitatea de instala componente de tip interfață de acces la nivelul fiecărei locații pentru a simplifica investigarea și raportarea evenimentelor colectate în locația respectivă fără a fi necesar transferul acestora între locații
- Soluția trebuie să ofere posibilitatea de a aplica reguli de corelare separate la nivelul datelor colectate în fiecare locație geografică
- Soluția trebuie să ofere posibilitatea de a aplica configurații diferite pentru componentele aflate în diferite locații geografice
- Soluția trebuie să ofere posibilitatea de a executa rapoarte la nivelul unei locații geografice utilizând un motor local
- Componenta SIEM trebuie să fie licențiată pentru 50GB de loguri procesate pe zi.

3.8.12. Soluție concentrator VPN

Soluția concentrator VPN va facilita conectarea mediului de producție al sistemului PNI din Cloud-ul Privat Guvernamental la mediul de disaster recovery din Centrul de Date STS din Cristian, Jud. Brașov prin utilizarea unei soluții avansate de Virtual Private Network (VPN) ce va oferi un nivel înalt de securitate și control.

Concentratorul VPN va oferi capacitatea de a cripta integral traficul de date între cele 2 medii (producție și disaster recovery), asigurând astfel confidențialitatea informațiilor transferate, această caracteristică esențială consolidând infrastructura digitală a Autorității pentru Digitalizarea României, asigurând un nivel suplimentar de securitate a datelor.

Soluția va dispune de funcționalitatea de monitorizare a traficului și auditare a activității utilizatorilor, aceste aspecte contribuind la întărirea controlului și transparenței în ceea ce privește utilizarea rețelei.

Soluția trebuie să fie o aplicație software disponibilă comercial (COTS) cu licențiere perpetuă sau sub forma de subscripție valabilă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție.

Concentratorul VPN va permite definirea următoarelor roluri pentru utilizatori:

- Administratori soluție ce vor beneficia de minim următoarele funcționalități:
 - o Gestionează utilizatorii și accesul acestora în cadrul modulului VPN
 - o Monitorizează activitatea utilizatorilor VPN pentru a asigura securitatea și conformitatea cu politicile instituționale
- Utilizatori soluție ce vor beneficia de minim următoarele funcționalități:
 - o Beneficiază de acces securizat la rețea prin intermediul serviciilor VPN
 - o Utilizează interfețe prietenoase pentru a accesa și utiliza serviciile VPN fără dificultăți

Accesul utilizatorilor soluției se realizează pe baza unor permisiuni, generate de către administrator. Astfel, pot fi create de către administrator tipuri de utilizatori cu diverse nivele de acces, prin intermediul planului de control oferit în cadrul soluției.

Specificații funcționale minime:

- Soluția va permite asigurarea unei integrări fluente cu soluții de tip Single Sign-On, oferind utilizatorilor o modalitate sigură și eficientă de a accesa, folosind minim următoarele protocoale de tip SSO: SAML, LDAP, SWA, OAuth și OpenID Connect;
- Soluția va dispune de propriul mecanism de autentificare pentru instituțiile ce nu dispun de opțiunea de Single sign-on (SSO) și va oferi unui sistem de autentificare dedicat, asigurând același grad ridicat de securitate, în ceea ce privește stocarea credențialelor;
- Soluția va dispune de mecanisme de Multi-Factor Authentication (MFA) și Time-based one-time password (TOTP): metode robuste de autentificare cu factori multipli și TOTP, sporind nivelul de securitate pentru autentificare;
- Soluția va permite înregistrarea și gestionarea utilizatorilor: funcționalități complete pentru înregistrarea și gestionarea utilizatorilor, facilitând administrarea acceselor și atribuirea de roluri, fiind integrată și sincronizarea cu sisteme de tip LDAP;
- Soluția va dispune de mecanisme de control granular bazat pe roluri (RBAC): sistem avansat de control al accesului bazat pe roluri, oferind administratorilor posibilitatea de a defini permisiuni specifice pentru fiecare utilizator;
- Soluția va permite utilizarea de credențiale temporare, nereutilizabile, pentru situații în care se impune un nivel sporit de securitate, oferire de credențiale temporare sau nereutilizabile;
- Soluția va permite verificare autentificării și verificarea utilizatorilor la distanță: auditul dispozitivelor care solicită acces în rețeaua instituției constă în evaluarea respectării criteriilor predefinite de securitate și stabilitate, înainte de a le permite

conectarea, precum și gestionarea accesului utilizatorilor la rețea indiferent de tipul de dispozitiv folosit, fie el un PC, laptop, smartphone sau tabletă;

- Soluția va dispune de autoritate de certificare internă proprie pentru utilizatorii la distanță. Aceasta va fi asigurată prin intermediul unei singure console de management a echipamentelor și certificatelor
- Soluția va permite stocarea istoricului detaliat al atributelor tuturor dispozitivelor conectate la rețea: componenta de autentificare și verificare utilizatori la distanță va oferi inclusiv informații despre tipurile de utilizatori, oferind detalii despre aplicațiile instalate și configurarea firewall-ului, precum și a activității acestora din punct de vedere al autentificării și autorizării;
- Soluția va permite configurarea de politici de acces pentru utilizatori la distanță: posibilitatea de a segmenta și controla accesul în rețea în conformitate cu grupurile de securitate și de a partaja informații despre aceste grupuri cu componenta echipamentelor firewall;
- Soluția va permite scalabilitatea componentei de autentificare și verificare utilizatori la distanță: arhitectura oferită va putea asigura gestionarea de la zeci de utilizatori la mii de utilizatori, fără a necesita modificări la instalarea inițială, ci doar prin adăugarea de noi mașini cu roluri dedicate;
- Soluția va asigura funcționalitatea de asigurare a Change of Authorization - CoA: componenta pentru autentificarea și verificarea utilizatori la distanță va oferi posibilitatea de a modifica autorizarea pentru utilizatori direct la echipamentele la care aceștia s-au conectat;
- Soluția va permite integrarea cu alte dispozitive de securitate a componentei destinate autentificării și verificării utilizatori la distanță. Soluția va permite astfel blocarea automată a accesului în rețea în situația detectării unei amenințări de securitate.

Specificații tehnice minime:

- Soluția va beneficia de suport pentru WireGuard și OpenVPN, suportul pentru aceste protocoale moderne permițând implementarea și gestionarea simultană a mai multor rețele VPN;
- Soluția va dispune de multiple protocoale de criptare, permițând administratorilor să aleagă nivelul optim de securitate în funcție de nevoile specifice, pe baza minim următoarelor protocoale: ChaCha20, Poly1305, AES și HMAC;
- Soluția va permite criptarea post-cuantică, oferind o soluție robustă împotriva amenințărilor viitoare;
- Ca și mecanism de protecție suplimentar, soluția va trebui să permită ca semnarea criptografică a imaginilor software să fie urmată de implementarea lansării controlate în execuție (secure boot), prin verificarea că imaginea semnată criptografic este executată exclusiv pe platforma hardware destinată, inclusiv cel puțin un chip TPM instalat în fabrică pentru identificare unică și autentică a platformei hardware;
- Soluția va permite utilizarea protocoalelor de comunicație UDP și TCP pentru acoperirea nevoilor specifice ale utilizatorilor;

- Soluția va permite un nivel de performanță ridicat, asigurând utilizatorilor o experiență de înaltă calitate, cu o viteză de transfer de cel puțin 1000 Mbps și un ping de maxim 0,5 ms;
- Soluția va permite asignarea și gestionarea mai multor adrese IP pe fiecare server VPN, facilitând distribuirea utilizatorilor între mai multe gateway-uri care pot fi localizate în diverse regiuni;
- Din punct de vedere al implementării, soluția va permite instalarea în regim on-premise, în cloud, sub formă de SaaS, în mod managed și SaaS managed;
- Soluția va oferi suport pentru multi-cloud, permițând gestionarea infrastructurii în minim următoarele medii de cloud: Azure, AWS, Google, dar și în sisteme de cloud-uri private on-premise;
- Soluția va dispune de aplicații native pentru sistemele de operare minim următoarele sisteme de operare: Windows, Linux, Mac, routere, IOS și Android. Sistemul va oferi și posibilitatea de utilizare fără a fi necesară instalarea unui client prin oferirea serviciului de VPN direct în browser;
- Soluția va dispune de mecanisme pentru automatizarea și integrarea platformei cu alte sisteme și procese cu ajutorul API-urilor și token-urilor;
- Soluția va permite update-ul fără downtime atât pentru componentele platformei de gestionare, cât și pentru actualizarea serverelor de VPN în vederea asigurării continuității serviciilor oferite administratorilor și utilizatorilor;
- Soluția va dispune de mecanisme de criptare a datelor interne în tranzit și at rest pentru protejarea informațiilor stocate;
- Soluția va permite filtrarea/blocarea domeniilor URL și adreselor IPv4/IPv6 la nivel de firewall sau de conexiune VPN pentru a controla accesul la resurse;
- Va dispune de capabilități de advanced logging pentru a permite monitorizarea detaliată a activității utilizatorilor și a evenimentelor de securitate;
- Va permite monitorizarea avansată a traficului TCP și UDP pentru oferirea de informații detaliate despre utilizarea rețelei;
- Va permite atribuirea traficului către utilizatori pentru a oferi un nivel granular asupra serviciilor;
- Soluția va dispune de un sistem propriu de alertare asupra evenimentelor critice de rețea, inclusiv opțiuni pentru integrare cu următoarele tipuri de platforme: Slack, SMS, e-mail și sisteme de ticketing pentru a notifica rapid administratorii despre evenimentele critice;
- Soluția va permite blocarea accesului și securizarea dispozitivelor, inclusiv opțiunea de killswitch pentru a preveni accesul neautorizat în cazul căderii VPN-ului;
- Soluția va permite split tunneling pentru a da posibilitatea administratorilor să direcționeze selectiv traficul prin VPN sau prin conexiuni normale.

3.9. SERVICII

Ofertantul va include la nivelul propunerii tehnice descrierea tuturor serviciilor următoare, menționând cel puțin următoarele informații:

- modelele de formulare care trebuie să fie utilizate pentru fiecare livrabil în parte;

- descrierea conținutului fiecărui livrabil;
- metodologiile după care se vor realiza fiecare dintre serviciile solicitate în timpul desfășurării proiectului.

3.9.1. Serviciile de livrare și instalare 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

3.9.1.1. Realizarea Documentației de instalare

Împreună cu Beneficiarul se va agree de comun acord 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 Contractantului;
- 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 care 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, banere de login, descriere interfețe, etc), dacă este cazul.

3.9.1.2. Instalarea echipamentelor în site

Pentru fiecare site se vor efectua următoarele operații:

- Transportul echipamentelor de către Contractant 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.5/6, Fibră optică etc.) furnizate de către ofertant;
- Interconectarea noilor echipamente cu sistemul de comunicații existent, dacă 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 agreată.

3.9.1.3. Configurarea echipamentelor

Toate echipamentele vor fi configurate de către Contractant conform soluției tehnice agreeate cu Beneficiarul în urma workshop-urilor comune.

Planul de adresare IP pentru testarea echipamentelor instalate va fi pus la dispoziția Contractantului de către Beneficiar, iar acesta din urmă va configura adresele IP de producție pe echipamentele respective, după efectuarea tuturor testelor de verificare.

Responsabilitatea Contractantului 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 cunoștință Contractantului și agreeate 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.

3.9.2. Serviciile de livrare și instalare componente software

Pentru asigurarea livrării cu succes a infrastructurii software ale sistemului, trebuie să fie realizată toată infrastructura sistemului. Pentru fiecare mediu în parte vor trebui să fie instalate, conform arhitecturii, produsele furnizate, în modul de disponibilitate solicitat cu toate componentele necesare (inclusiv sisteme de operare).

Vor trebui astfel asigurate cel puțin următoarele activități:

- Finalizarea arhitecturii componentelor software;
- Instalarea componentelor software;
- Configurarea sistemului software;
- Integrarea componentelor software;
- Testarea soluției.

3.9.3. Serviciile de pre-analiză privind interoperabilitatea inter-instituțională

Aceste servicii vor acoperi următoarele activități:

- **Transpunerea normelor de referință pentru realizarea interoperabilității în cerințe de business** pentru a ușura etapa de analiză și proiectare a sistemului informatic PNI (Platforma Națională de Interoperabilitate).
- **Propunerea de norme subsecvente de aplicare a NRRI.** Serviciile vor acoperi modalitatea detaliată prin care PNI va implementa procesele tehnice stabilite prin Normele de referință pentru realizarea interoperabilității (NRRI) în domeniul tehnologiei informației și comunicațiilor, pentru asigurarea schimbului de date între sistemele informatice deținute de participanții la schimbul de date și pentru îmbunătățirea colaborării și a prestării comune a serviciilor publice. Se vor realiza procedurile necesare pentru toate procesele prevăzute în legea interoperabilității și NRRI și modul în care ele se vor implementa tehnic în PNI (ex: procedura de conectare și participare la platforma națională de interoperabilitate și a schimbului de date).
- Stabilirea datelor necesare asigurării interoperabilității sistemelor publice pentru furnizarea serviciilor publice care trebuie puse la dispoziția sistemului informatic PNI de către autoritățile și instituțiile publice sau private conform NRRI.
- Alinierea proceselor operaționale pentru furnizarea acelorași servicii publice de către instituții diferite.
- În colaborare cu administratorii registrelor de bază, stabilirea categoriilor de date care sunt partajate de fiecare autoritate și instituție publică și acordarea drepturilor de acces celorlalte autorități și instituții publice, persoane juridice de drept privat, respectiv persoane care exercită profesii libere reglementate, pentru fiecare categorie de date.
- Stabilirea nivelului semantic pentru schimbul de date.
- Redactarea draft-urilor de contracte schimb de date ce vor fi semnate de către furnizorii și beneficiarii seturilor de date prin intermediul sistemului informatic PNI. Acestea vor fi validate cu departamentul juridic al ADR și cu instituțiile ce dețin registre de bază. Cerințe funcționale pentru precompletarea informațiilor acestor contracte și întocmirea lor în mod automat prin intermediul sistemului informatic PNI.

- Realizarea analizei necesare pentru măsurarea consumului de date prin PNI și realizarea documentației necesare pentru billing.

Conform Legii 242/2020 privind schimbul de date între sistemele informatice și crearea Platformei naționale de interoperabilitate, art 13, alin (1) și (4): Schimbul de date între autoritățile și instituțiile publice, pe de o parte, și utilizatorii persoane juridice de drept privat sau persoanele care exercită profesii libere reglementate, pe de altă parte, are loc în bază contractuală.

Contractul de schimb de date se încheie între autoritatea care administrează Platforma Națională de Interoperabilitate și persoana juridică de drept privat, respectiv persoane care exercită profesii libere reglementate și care dețin sisteme informatice, și este cu titlu oneros.

Costurile de operare a platformei vor fi stabilite de administratorul Platformei Naționale de Interoperabilitate și vor depinde de costurile operaționale ale administratorilor registrelor de bază consultate, respectiv ale administratorului Platformei Naționale de Interoperabilitate.

Un procent de 80% din veniturile realizate de administratorul Platformei Naționale de Interoperabilitate vor fi vărsate administratorilor registrelor de bază, iar administratorul Platformei Naționale de Interoperabilitate va reține un procent de 20% din venituri pentru mentenanța, în urma unei analize a costurilor realizate de MCID.

Procedurile administrative pentru punerea în practică a mecanismului de plăți revin Autorității pentru Digitalizarea României, în calitate de administrator al platformei, care va publica și modelul de contract folosit pentru schimbul de date prin PNI.

3.9.4. Serviciile de implementare sistem

Pentru asigurarea implementării sistemului vor trebui asigurate cel puțin următoarele categorii mari de activități:

- Servicii de analiză a sistemului;
- Servicii de modelare/proiectare a sistemului:
 - o Proiectarea modelului sistemului de date;
 - o Definirea serviciilor aferente noului flux funcțional de sistem;
 - o Definirea principalelor funcționalități de sistem folosind modele entitate - asociere sau UML2.0;
 - o Proiectarea componentelor și arhitectura de sistem;
- Dezvoltarea softului de aplicație:
 - o Instalarea și configurarea produselor COTS;
 - o Dezvoltarea componentelor de software;

- Integrarea componentelor software;
- Testarea soluției software;
- Configurarea sistemului software;
- Obținerea acordului final din partea beneficiarului proiectului;

Se vor avea în vedere minim servicii pentru interconectarea sistemului ADR cu:

- proiectul - ROeID;
- portalul Single Digital Gateway - proiectul PDURO;
- Registrele de baza existente și mature conectate și expuse în conformitate cu procedurile publicate în registrul registrelor.
- Ghiseul.ro pentru achitarea eventualelor taxe pentru interconectare sau schimbul de date.
- ONRC și ANAF în vederea extragerii datelor unice ale CUI-ului introdus de utilizatorul inițial care va dori utilizarea datelor din registrul de baza.
- 5 instituții care vor folosi registrele de baza (ex: MAI, ONRC, MMJS etc.).

3.9.4.1. Servicii de analiză

Rolul principal al serviciilor de analiză este de a înțelege corect nevoile utilizatorilor înainte de proiectarea și implementarea unui sistem care să le îndeplinească, prin clarificarea și detalierea cerințelor formulate în prezenta documentație.

Echipa de analiză a Prestatorului trebuie să analizeze cerințele împreună cu membrii echipei de proiect din partea ADR pentru a înțelege corect cerințele utilizatorilor înainte de proiectarea și dezvoltarea platformei.

În cadrul fazei de analiză este foarte posibil ca anumite cerințe formulate inițial în prezentul caiet de sarcini să se transforme prin detalieri, de asemenea este posibil ca noi cerințe să fie identificate, nefiind observate inițial. În această situație, se va ține cont de rezolvarea neajunsurilor identificate și atingerea beneficiilor anticipate, de obiectivele generale și specifice ale achiziției, astfel încât să se ajungă la un rezultat constructiv.

În vederea implementării platformei, Prestatorul trebuie să execute activități de analiză care să asigure premisele unei implementări eficiente.

Beneficiarul va acorda tot sprijinul necesar pentru înțelegerea cât mai bună și completă a contextului în care va fi implementată platforma.

Analiza se va efectua la sediul Beneficiarului (sau prin ședințe ONLINE) și va avea ca finalitate un pachet de specificații tehnice agreeat de comun acord cu acesta. Serviciile de analiză vor acoperi cel puțin următoarele aspecte:

- analiza contextului existent;
- înțelegerea structurii organizatorice a Beneficiarului;

- analiza situației din momentul de față din cadrul instituției Beneficiarului prin ședințe de analiză, chestionare etc. Se vor identifica și documenta procesele operaționale care vor fi impactate prin implementarea soluției în cadrul contractului;
- definirea cerințelor informaționale pentru sistem. Se va contura astfel, imaginea sistemului informatic prin stabilirea proceselor operaționale care să precizeze succesiunea activităților, participanții și momentul intervenției acestora, locația sau contextul, modalitatea de intervenție, informația procesată și resursele utilizate. Pentru prezentarea proceselor operaționale se vor utiliza instrumente de modelare a proceselor și activităților în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent);
- integrarea cu sistemele informatice identificate în cadrul etapei de analiză necesare fluxurilor descrise în cadrul caietului de sarcini;

3.9.4.2. Servicii de modelare/proiectare a sistemului

În vederea implementării contractului, Prestatorul va trebui să execute următoarele activități care să asigure premisele unei implementări eficiente:

- proiectarea modelului sistemului de date;
- definirea serviciilor aferente noului flux funcțional de sistem;
- definirea principalelor funcționalități de sistem folosind modele entitate - asociere sau UML sau echivalent ;
- proiectarea componentelor și arhitectura de sistem;

Proiectarea sistemului dorit, constă în detalierea la nivel tehnic a cerințelor și specificațiilor rezultate din activitatea de analiză pentru toate nivelurile și componentele sistemului care va fi realizat, astfel:

- arhitectura de sistem - va prezenta cel puțin următoarele niveluri: hardware, comunicații, componente software instalate, arhitectură logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate și caracteristicile funcționale și non-funcționale ale acestora;
- scenarii (cazuri) de utilizare - din care să reiasă modul de utilizare a sistemului informatic adaptat din perspectiva utilizatorului final, modul în care utilizatorii interacționează cu sistemul, în corespondență directă cu activitățile menționate în cadrul proceselor operaționale ale acestor utilizatori. Scenariile de utilizare trebuie să cuprindă și interacțiunile cu sistemele externe, astfel încât să fie evidențiat exact modul în care este fructificată o integrare la nivel de sistem informatic.
- integrările la nivel de componentă software - pentru fiecare interacțiune se va specifica sistemul sursă/destinație, modalitatea de implementare, canal de comunicare, setul și structura de date transferate, reguli specifice de validare etc.;
- rapoarte ce vor fi realizate în cadrul sistemului - vor fi descrise rapoartele noi, care sunt informațiile conținute, care sunt criteriile de filtrare dacă este cazul și tipul de livrare al acestora (timp real, la cererea utilizatorului sau automatizate la un anumit moment de timp programat apriori).

Documentul/documentele de specificații, rezultate în urma activităților de analiză și

proiectare, vor descrie soluția în detaliu, vor conține informații privind toate funcționalitățile necesare și vor sta la baza stabilirii și realizării testelor pentru recepția livrabililor.

În urma activităților de analiză și proiectare, pentru a se obține un sistem adaptat final operațional se vor desfășura activități de dezvoltare, configurare, testare și punere în producție.

3.9.4.3. Dezvoltarea softului de aplicație

Pentru implementarea contractului, în urma analizei și proiectării sistemului, se vor realiza cel puțin următoarele acțiuni:

- o Instalarea și configurarea produselor COTS;
- o Dezvoltarea componentelor de software;
- o Integrarea componentelor software;
- o Testarea internă a soluției software;
- o Configurarea sistemului software;

Toate dezvoltările trebuie să asigure compatibilitatea sistemului cu specificațiile de interfațare ale acestuia cu sistemele externe. Testarea internă se va face pentru a se asigura că funcționalitățile individuale funcționează conform documentației de analiză.

Dezvoltarea, configurarea și testarea internă se vor face folosind o metodologie de dezvoltare validată în timp bazată pe standarde/bune practici internaționale. Prestatorul va folosi instrumente specifice de dezvoltare, configurare și testare compatibile conform cerințelor caietului de sarcini.

În cadrul propunerii tehnice ofertantul trebuie să prezinte:

- metodologia detaliată în baza căreia vor fi desfășurate activitățile de dezvoltare și testare internă, demonstrând integrarea acestor proceduri cu procedurile de analiză și proiectare;
- instrumentele utilizate în desfășurarea activităților de implementare și testare internă;
- detalierea livrabililor aferente prestării activităților de implementare și testare internă.

3.9.5. Testarea și asigurarea calității sistemului

Este necesar ca Prestatorul 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.

3.9.5.1. Testarea

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

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

Contractantul trebuie să precizeze toate instrumentele de testare (aplicații, scripturi, etc.), destinate a fi utilizate în timpul procedurilor de testare. Contractantul trebuie să pună la dispoziție instrumentele de testare. Toate rezultatele testelor trebuie înregistrate și furnizate Beneficiarului după fiecare test.

Toate componentele HW/SW necesare testării vor fi descrise de Contractant 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 testare

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. Contractantul va oferi toate instrumentele de testare, în cazul utilizării instrumentelor automate pentru testele de acceptață operațională.

Coordonarea testelor

Planul de testare însoțit de specificațiile de testare va fi propus de Contractant și agreat de Beneficiar cu 10 zile înainte de execuția efectivă a testelor. Testele vor fi coordonate de către Beneficiar/Utilizatori, care vor controla faptul că mediul de testare e conform cu cerințele, vor monitoriza efectuarea testelor și se vor asigura de aplicarea procedurilor de management al testării.

3.9.5.2. Asigurarea Calității Serviciilor

- Contractantul trebuie să prezinte un plan pentru Asigurarea Calității acceptabil pentru Beneficiar, ca parte a planului de proiect;
- Contractantul 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;
- Contractantul va elabora procedurile standard de operare pentru toate aplicațiile livrate, cu instrucțiuni detaliate pentru sprijinirea angajaților în diferite procese de lucru;
- Contractantul va pune la dispoziție manuale, documentații, proceduri complete privind concepția, implementarea și administrarea în integralitate a sistemului informatic;

Contractantul 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.

3.9.6. Instruire utilizatori

În cadrul proiectului se va asigura instruirea diferențiată a următoarelor categorii de beneficiari, astfel:

- administratorii și personalul de întreținere a sistemului informatic de la ADR. Pentru această categorie, proiectul va asigura instruirea a 10 persoane de la ADR;
- O echipă desemnată de ADR va fi instruită de furnizorul soluției informatice conform legislației în vigoare pentru asigurarea Nivelului 1 de suport pentru utilizatorii sistemului propus (15 utilizatori).

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 pentru conștientizarea securității;
- cursuri de securitate pentru administratori.

Sesiunile de instruire vor fi realizate de furnizorul soluției informatice. De asemenea, furnizorul soluției informatice va elabora și pune la dispoziția beneficiarului manuale de utilizare și administrare soluție și sistem și suport de curs în limba română, pentru toate categoriile de utilizatori ai sistemului. Planul de instruire va fi propus de Contractant și agreeat de Beneficiar cu 10 zile înainte de începerea efectivă a instruirii.

La terminarea cursului, cursanții din categoriile administrator de sistem vor primi de la furnizor certificate de instruire individuale. Certificarea se va face diferențiat pentru cele două categorii.

Sistemul va fi operat, administrat și gestionat de către următoarele categorii de utilizatori, având rolurile menționate mai jos:

- **Personalul operațional.** Această categorie de utilizatori este responsabilă de operaționalizarea sistemului.
 - o cursul va avea o durată de minim 5 zile (8 ore /zi)
 - o cursul va fi dimensionat pentru 15 utilizatori
 - o cursul va fi susținut în limba română
 - o curricula va acoperi toate aspectele necesare utilizării în bune condiții a sistemului.
- **Administratori sistem integrat** - cursuri specifice soluției integrate oferite.
 - o cursul va avea o durată de minim 5 zile (8 ore /zi)
 - o cursul va fi dimensionat pentru 10 utilizatori
 - o cursul va fi susținut în limba română.
 - o curricula va acoperi toate aspectele necesare utilizării în bune condiții a sistemului.
 - o curricula va acoperi toate aspectele de securitate cibernetică a sistemului informatic.

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 materiale de curs pentru toți participanții. La sfârșitul cursului participanții vor completa formulare pentru evaluarea serviciilor de training.

Se va organiza și o sesiune de tip workshop cu furnizorii registrelor de baza care vor fi conectați la PNI. Workshop-ul va avea o durată de 8 ore și se va desfășura în limba română într-o locație amenajată pentru acest tip de activitate de către Furnizor. Se va asigura spațiu, echipamente, catering pt minim 40 de persoane pentru workshop.

3.9.7. Punere în producție

Ofertanții trebuie să prezinte planul care va fi utilizat la trecerea în producție a

sistemului. Contractantul va transmite spre aprobare planul de punere în producție cu cel puțin 15 zile lucrătoare înaintea de începerea activității.

Planul prezentat trebuie să țină cont de legăturile logice între subsisteme astfel încât să se asigure o trecere în producție coerentă și cu impact minim în derularea activităților operaționale ale Beneficiarului.

Pentru aprobare raportului de punere în producție, Beneficiarul se va asigura că Prestatorul a efectuat cu succes următoarele activități cu rezultatele lor respectiv:

- toate componentele software de bază necesar 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 implementarea sistemului.

Raportul aprobat de punere în producție a Platformei Naționale de Interoperabilitate marchează finalizarea perioadei de execuție a contractului. Acest document atestă faptul că platforma a fost instalată, configurată și testată conform cerințelor tehnice prevăzute în contract și este operațional în condiții normale de utilizare. Raportul include detalii privind funcționalitățile implementate, eventualele observații identificate în faza de testare, precum și confirmarea faptului că toate componentele platformei sunt funcționale și livrate conform specificațiilor.

4. RESURSE

Atât Prestatorul, cât și Beneficiarul trebuie să asigure cadrul profesional adecvat desfășurării proiectului în bune condiții. Fiecare va pune la dispoziție toți specialiștii necesari pentru îndeplinirea scopului și obiectivelor proiectului.

În calitate de beneficiar al proiectului, ADR, înțelege că pentru bunul mers al acestuia trebuie să pună la dispoziție toate resursele necesare îndeplinirii contractului.

În acest sens, pentru buna desfășurare a fazelor proiectului, dar și pentru exploatarea curentă a acestuia după implementare, beneficiarul va asigura capacitatea operațională și administrativă necesară. Astfel, pe lângă resursele financiare, va asigura și resursele materiale necesare pentru buna implementare a proiectului. Din aceste resurse materiale deținute și utilizate pentru buna implementare a proiectului amintim:

- sediul Beneficiarului, precum și dotările necesare pentru întâlnirile echipei de proiect

și desfășurării activităților acestora;

- baza logistica: mobilier (birouri, scaune, dulapuri pentru o parte din membrii echipei) și echipamente IT;
- mijloace de comunicație;
- site-ul Beneficiarului, pentru o comunicare și promovare eficientă și completă a rezultatelor proiectului.

Prestatorul are obligația de a propune spre mobilizare o echipă formată din experți calificați pentru realizarea activităților prevăzute în caietul de sarcini și va fi responsabil pentru activitatea experților și pentru obținerea rezultatelor contractului. Experții propuși vor avea calificarea și experiența profesională necesare pentru acoperirea cu succes a tuturor activităților indicate în caietul de sarcini. Astfel, Prestatorul va pune la dispoziția autorității contractante o echipă formată din personal cheie cu competențe și experiență dovedite, capabil să ducă la bun sfârșit cu succes sarcinile definite prin prezentul caiet de sarcini, astfel ca, în final, să contribuie la îndeplinirea obiectivului general și a obiectivului specific ale proiectului, în condițiile respectării cerințelor de calitate și a termenelor stabilite și încadrarea în bugetul prevăzut.

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 cheie care au obligația de a îndeplini următoarele cerințe minime și obligatorii:

Nr.crt.	Tip Expert	Nr. Experți
Experți cheie		
1	Expert manager de proiect	1
2	Expert team leader software	1
3	Expert coordonator analiză de business	1
4	Expert arhitect sistem informatic	1
5	Expert baze de date	1
6	Expert administrarea identității utilizatorilor	1
7	Expert securitate	1
8	Expert testare securitate	1
9	Expert interoperabilitate	1
10	Expert infrastructura hardware și procesare	1
11	Expert testare software	1
Experți non-cheie		
12	Expert analist	2
13	Expert dezvoltator software	3
14	Expert DMS	1
15	Expert portal	1
16	Expert BI (Business Intelligence)	1
17	Expert suport tehnic	1

Nr.crt.	Tip Expert	Nr. Experți
18	Expert instruire	1

Ofertantul va îndeplini următoarele condiții minime pentru echipa de proiect:

4.1. Experți cheie

4.1.1. Expert manager de proiect

Pentru expertul manager de proiect se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind metodologia de management de proiect pe care Prestatorul o va utiliza în cadrul proiectului, dovedite prin prezentarea a cel puțin unei diplome sau certificări recunoscută la nivel național sau internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de manager de proiect

Responsabilități în cadrul Contractului:

- Este punct unic de contact în relația cu Beneficiarul și va avea între atribuțiile sale conducerea unică a echipei de proiect;
- Planifică activitatea echipei de proiect;
- Stabilește cerințele de management al proiectului;
- Monitorizează implementarea proiectului;
- Elaborează planul revizuit de activități și urmărește respectarea termenelor proiectului;
- Elaborează rapoartele de progres lunare ce vor fi înaintate spre aprobare beneficiarului;
- Supraveghează îndeplinirea de către prestator a obligațiilor asumate în conformitate cu contractul semnat.

4.1.2. Expert team leader software

Pentru expertul team leader software se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe în domeniul dezvoltării de software, dovedite prin prezentarea a cel puțin unei diplome sau certificări recunoscută la nivel național sau internațional
- Deținerea de competențe privind realizarea arhitecturilor software, dovedite prin prezentarea a cel puțin unei diplome sau certificări recunoscută la nivel național sau internațional
- Deținerea de competențe privind metodologiile de tip Scrum Agile în dezvoltare produse software, dovedite prin prezentarea a cel puțin unei diplome sau certificări recunoscută la nivel național sau internațional
- Deținerea de competențe în tehnologie de cloud Microsoft Azure privind

administrarea, proiectarea, migrarea și optimizarea resurselor, managementul identității, protecția platformei, securitatea datelor și aplicațiilor precum și implementarea practicilor și proceselor DevOps, dovedite prin deținerea a cel puțin unei diplome sau certificări recunoscute la nivel național sau internațional

- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de team leader echipă dezvoltare

Responsabilități în cadrul Contractului:

- Gestionează implementarea sistemului;
- Coordonează întreaga echipă tehnică, cu alocarea sarcinilor pe fiecare membru al echipei;
- Menține și aplică managementul riscurilor și procedurile de asigurare a calității;
- Asigură resurse pentru executarea serviciilor de implementare cuprinse în specificațiile tehnice;
- Întocmește toate rapoartele tehnice necesare conform cerințelor proiectului și/sau alte rapoarte cerute de către managerul de proiect;
- Validează specificațiile de business în vederea extragerii specificațiilor tehnice și gestionează relația cu clientul;
- Coordonează echipa în toate fazele de dezvoltare ale sistemului ținând cont și de specificul mediului cloud Microsoft Azure;
- Elaborează specificații tehnice de design și arhitectură software;
- Asigură managementul produselor software (roadmap dezvoltări, planificarea release-urilor, integrarea produsului în arhitectura IT a beneficiarului).

4.1.3. Expert coordonator analiză de business

Pentru expertul coordonator analiză de business se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de cunoștințe în domeniul analizei de business, dovedite prin prezentarea unei diplome/ certificări recunoscută la nivel național/internațional, (de tip CBAP sau echivalent)
- Deținerea de cunoștințe în modelarea și documentarea proceselor de business, dovedite prin prezentarea unei diplome sau certificări recunoscută la nivel național sau internațional, (de tip UML, BPMN sau echivalent)
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de analist de business;

Responsabilități în cadrul Contractului:

- Analizează, planifică și monitorizează cerințele funcționale și non-funcționale;
- Realizează documentele de analiză și a specificațiilor;
- Coordonează activitățile de analiză de business;
- Analizează, definește procesele de business și elaborează specificațiile detaliate ale

- proceselor;
- Analizează și interpretează cerințele;
 - Identifică problemele din rândul proceselor, inițiază acțiuni de îmbunătățire a proceselor;
 - Participă la definirea scenariilor de testare;
 - Participă la structurarea procesului de instruire.

4.1.4. Expert arhitect sistem informatic

Pentru expertul arhitect sistem informatic se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe în domeniul arhitecturilor complexe de tip Enterprise în contextul sistemelor informatice, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/internațional
- Deținerea de cunoștințe în domeniul proiectării și implementării de arhitecturi software orientate pe servicii, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/internațional
- Deținerea de cunoștințe privind metodologii de dezvoltare software bazate pe principii de dezvoltare iterativă, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Deținerea de competențe în dezvoltare de aplicații sau baze de date, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Deținerea de competențe în tehnologia de cloud Microsoft Azure, dovedite prin deținerea a cel puțin unei diplome sau certificări recunoscute la nivel național sau internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de arhitect sistem informatic.

Responsabilități în cadrul Contractului:

- Coordonează activitatea de proiectare și definire a arhitecturii sistemului respectând standardele în domeniu și ținând cont și de specificul mediului cloud Microsoft Azure în ceea ce privește procesarea stocarea, comunicațiile, înalta disponibilitate și securitatea în cloud;
- Documentează și păstrează informații și/sau modele ale arhitecturii de sistem și ale structurilor de date. Se ocupă de actualizarea și modificarea acestor informații pe parcursul derulării activităților;
- Asigură suport pentru testare, implementare /utilizare corectă a sistemului informatic.

4.1.5. Expert baze de date

Pentru expertul baze de date se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe în tehnologia de baze de date ofertată privind administrarea, optimizarea, asigurarea înaltei disponibilități și asigurarea securității bazei de date, dovedite prin prezentarea unei diplome/certificări a producătorului în tehnologia bazei de date ofertate, recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert baze de date

Responsabilități în cadrul Contractului:

- Configurarea bazelor de date pentru a obține performanțe maxime în raport cu cerințele sistemului;
- Strategia de backup pentru bazele de date;
- Realizează managementul performanței bazelor de date, diagnosticarea potențialelor probleme prin urmărirea logurilor de sistem;
- Este responsabil cu menținerea integrității și securității bazelor de date;
- Monitorizează îndeplinirea indicatorilor de performanță specifici bazelor de date.

4.1.6. Expert administrarea identității utilizatorilor

Pentru expertul administrarea identității utilizatorilor se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind administrarea soluțiilor de management al identităților electronice, dovedite prin prezentarea unei diplome/certificări recunoscute la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert administrarea identității utilizatorilor

Responsabilități în cadrul Contractului:

- Analiza infrastructurii existente de autentificare/autorizare și a cerințelor de securitate la nivel de identitate;
- Integrarea sistemelor cu soluții de identitate;
- Configurarea de protocoale de autentificare;
- Definirea și aplicarea politicilor de autentificare, autorizare și audit;
- Asigurarea interoperabilității între componente on-premises;
- Elaborarea și menținerea documentației tehnice aferente configurărilor și fluxurilor de identitate.

4.1.7. Expert securitate

Pentru expertul securitate se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind analiza, corelarea și investigarea evenimentelor de

securitate, crearea de reguli complexe și optimizarea performanțelor pentru sisteme de tip SIEM (Security Information and Event Management), dovedite prin prezentarea unei diplome certificări recunoscute la nivel național / internațional

- Deținerea de competențe în domeniul protecției cibernetice, incluzând detectarea, analiza și răspunsul la incidente de securitate, analiza traficului de rețea, investigarea artefactelor digitale și gestionarea amenințărilor, dovedite printr-o diplomă/certificare obținută în urma promovării unui examen practic de analiză proactivă a amenințărilor cibernetice
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert securitate

Responsabilități în cadrul Contractului:

- Proiectarea, implementarea și configurarea platformei SIEM, asigurând integrarea corectă a surselor de loguri și evenimente din infrastructura IT;
- Administrarea și optimizarea performanței sistemului SIEM, incluzând gestionarea fluxurilor de date, a stocării și a resurselor hardware/software;
- Dezvoltarea regulilor de corelare, alerte și rapoarte personalizate pentru detectarea anomaliilor și a incidentelor de securitate;
- Colaborează cu expertul de testare securitate pentru remedierea vulnerabilităților și îmbunătățirea controalelor de securitate.

4.1.8. Expert testare securitate

Pentru expertul testare securitate se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de cunoștințe privind testarea de securitate a infrastructurilor de rețea din punct de vedere al securității informației, dovedite printr-o diplomă/certificare obținută în urma promovării unui examen practic de penetrare efectivă a unui sistem informatic
- Deținerea de competențe privind procesul de analiză a vulnerabilităților și interpretarea rezultatelor obținute în urma procesului de testare de securitate efectuat conform unei metodologii recunoscute în domeniu, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Deținerea de competențe privind testele de penetrare a infrastructurilor de tip cloud din punct de vedere al securității informației, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Deținerea de competențe privind auditarea de securitate a sistemelor informatice, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert testare securitate

Responsabilități în cadrul Contractului:

- Stabilirea și elaborarea planului de testare, precum și a scenariilor de atac;
- Identificarea sistemelor și serviciilor de rețea active pentru evaluarea vulnerabilităților care derivă din configurațiile nesecurizate, lipsa actualizărilor de securitate, lipsa sau ineficiența mecanismelor de criptare;
- Realizează scanarea de vulnerabilități a sistemului de cloud ;
- Realizează testele de penetrare a sistemului de tip cloud pentru a identifica și elimina orice vulnerabilități înainte de a fi dat în producție;
- Asigură suport pentru configurarea din punct de vedere al securității a sistemului de cloud;
- Elaborarea Raportului de testare de securitate;
- Acordă suport pentru înțelegerea deplină a problemelor identificate și alegerea măsurilor/metodelor aplicabile pentru remedierea acestora, în scopul minimizării riscurilor de securitate informatică asociate problemelor și vulnerabilităților descoperite;
- Oferă feedback sub forma de recomandări, rezerve etc. pentru orice modificări a arhitecturii;
- Păstrează înregistrări ale tuturor actualizărilor și/sau modificărilor aduse arhitecturii de Cloud și ale informațiilor privind comunicațiile și echipamentele de securitate;
- Participă la analiza detaliată a tuturor aspectelor sau propunerilor ce pot avea un impact semnificativ asupra platformei de Cloud.

4.1.9. Expert interoperabilitate

Pentru expertul interoperabilitate se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind componenta de interoperabilitate, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert interoperabilitate

Responsabilități în cadrul Contractului:

- Transpunerea în funcționalități a cerințelor documentate în etapele de analiză și proiectare;
- Participarea la activitățile de instalare și dezvoltare/configurare a componentei de interoperabilitate;
- Testarea funcționării soluției instalate și configurate, la nivelul sistemului, cu setul de date de test acordat cu Beneficiarul astfel încât să fie acoperite cerințele specifice de sistem;
- Asigurarea expertizei în domeniul tehnic cu privire la componenta de interoperabilitate, 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.

4.1.10. Expert infrastructură hardware și procesare

Pentru expertul infrastructură hardware și procesare se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind design, instalare, configurare și management soluții de virtualizare, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/ internațional
- Deținerea de competențe privind soluții de procesare și stocare, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/ internațional
- Deținerea de competențe privind configurarea și administrarea soluțiilor de backup și recuperare, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/ internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert infrastructură și procesare

Responsabilități în cadrul Contractului:

- Evaluează configurarea infrastructurii hardware;
- Documentează instalarea și configurarea infrastructurii;
- Este responsabil de instalarea și configurarea soluției de backup și recuperare date, de asigurarea administrării, monitorizării și disponibilității sistemelor de back-up și recuperare în parametrii normali;
- Asigură elaborarea documentațiilor tehnice de utilizare și administrare a infrastructurii și, după caz, participă la sesiunile de instruire a utilizatorilor;
- Participă la sesiunile de testare a sistemului;
- Documentează activitățile efectuate în sensul celor de mai sus.

4.1.11. Expert testare software

Pentru expertul testare software se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind testarea funcționalității sistemelor informatice, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem

informatic în care a avut responsabilități specifice rolului de expert testare software

Responsabilități în cadrul Contractului:

- Este responsabil de asigurarea testării funcționalităților dezvoltate și implementate conform metodologiei de testare agreeate cu Beneficiarul;
- Realizează documentele de testare și specificații ale scenariilor de test;
- Acordă suport utilizatorilor pentru testarea funcțională;
- Planifică activitățile de testare;
- Elaborează planurile, scenariile și cazurile de test;
- Este responsabil de întocmirea și livrarea rapoartelor de testare;
- Realizează testele de acceptanță specifice;
- Coordonează activitățile de testare la nivelul echipei de testare a Prestatorului;
- Este responsabil de asigurarea funcționării corecte a sistemului din punct de vedere al respectării cerințelor, consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor.

Pentru demonstrarea îndeplinirii cerințelor pentru experții cheie se vor depune următoarele documente:

- CV-ul datat și semnat;
- copii conform cu originalul după diplomele/certificările/atestările relevante în raport cu cerințele din prezenta documentație;
- în vederea respectării principiul recunoașterii reciproce, precizăm că, pentru personalul nerezident, se permite prezentarea certificărilor/ autorizărilor corespunzătoare emise în țara de rezidență;
- documente relevante din care să reiasă îndeplinirea cerințelor de experiență profesională specifică, solicitate prin prezenta documentație - îndeplinirea cerințelor se face prin prezentarea de certificate/ documente cum ar fi: contracte, recomandări, procese verbale, documente constatatoare sau orice alte documente doveditoare;
- pentru experții care nu sunt angajați ai ofertantului, se vor prezenta declarații de disponibilitate (Formularul - Declarație de disponibilitate) dateate și semnate de titular;
- prestatorul va putea utiliza în echipă și alți experți fiind responsabil de componența echipelor de experți și profilul generic al acestora;
- prestatorul va asigura personalul administrativ și suport (backstopping) necesar echipei sale;
- fiecare dintre persoanele propuse trebuie să îndeplinească integral toate cerințele minime aferente expertului (profilului de persoană) pentru care au fost nominalizate. Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.

Ofertanții vor transmite documentele solicitate în caietul de sarcini care certifică îndeplinirea cerințelor minime de calificare, pentru experții cheie. Totodată, ofertanții vor prezenta împreună cu documentele solicitate, un tabel în cuprinsul căruia se va detalia

modalitate de îndeplinire a cerințelor minime de calificare, prin indicarea în clar a documentelor suport care probează îndeplinirea cerințelor (exemplu: pentru cerințele privind Studiile/ Calificările educaționale se va indica documentul în clar care probează îndeplinirea cerințelor minime).

4.2. *Experți non-cheie*

4.2.1. *Expert analist*

Pentru expertul analist se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind analiza de business, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert analist

Responsabilități în cadrul Contractului:

- Analizează, planifică și monitorizează cerințele funcționale și non-funcționale;
- Realizează documentele de analiză și a specificațiilor;
- Analizează, definește procesele de business și elaborează specificațiile detaliate ale proceselor;
- Analizează și interpretează cerințele;
- Identifică problemele din rândul proceselor, inițiază acțiuni de îmbunătățire a proceselor;
- Participă la definirea scenariilor de testare.

4.2.2. *Expert dezvoltare software*

Pentru expertul dezvoltare software se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind dezvoltarea de software, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Deținerea de competențe privind dezvoltarea aplicațiilor cu seturi de date relaționale, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert dezvoltare software

Responsabilități în cadrul Contractului:

- Este responsabil de dezvoltarea de aplicații software;
- Este responsabil de elaborarea, testarea și întreținerea aplicațiilor software;
- Întocmește documentația tehnică;
- Asigură suport tehnic.

4.2.3. Expert DMS

Pentru expertul DMS se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe de specialitate în ceea ce privește implementarea soluției de management de documente ofertată (modelare, configurare, personalizare, integrare), dovedită prin prezentarea unei diplome/certificări recunoscută la nivel național/ internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert DMS

Responsabilități în cadrul Contractului:

- Participă la etapa de analiză și proiectare pentru definirea atât a cerințelor de arhitectură de ansamblu cât și la nivel de modul constituent privind componenta de management a documentelor;
- Realizează configurările/dezvoltările necesare în cadrul componentei de management a documentelor, procedează la definirea rapoartelor asociate acestei componente și participă la implementarea cerințelor privind sincronizarea și migrarea datelor, inclusiv cele de interoperabilitate;
- Asigură elaborarea documentațiilor tehnice de utilizare și administrare a componentei de management a documentelor și, după caz, participă la sesiunile de instruire a utilizatorilor.
- Participă la sesiunile de testare unitară a sistemului și efectuează testările la nivelul componentei de management a documentelor;
- Documentează activitățile efectuate în sensul celor de mai sus.

4.2.4. Expert Portal

Pentru expertul portal se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind soluții de tip portal dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert portal

Responsabilități în cadrul Contractului:

- Este responsabil de dezvoltarea și implementarea soluției de tip portal pe baza documentelor de analiză, specificații funcționale, specificații tehnice, arhitectură sistem;
- Este responsabil de testarea unitară a soluției de tip portal (internă);
- Acordă suport utilizatorilor cheie pentru testarea funcțională;
- Este responsabil de rezolvarea disfuncționalităților (bug-uri).

4.2.5. Expert BI (Business Intelligence)

Pentru expertul BI se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de cunoștințe privind implementarea soluțiilor de business intelligence, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert BI (Business Intelligence)

Responsabilități în cadrul Contractului:

- Este responsabil de crearea modelelor de date/metadate pentru analiză și raportare;
- Realizează activitățile de proiectare, dezvoltare și implementare a soluției de analiză și raportare.

4.2.6. Expert suport tehnic

Pentru expertul suport tehnic se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe privind managementul sistemelor IT dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert suport tehnic

Responsabilități în cadrul Contractului:

- Este responsabil de asigurarea analizei, planificarea, administrarea, rezolvarea, monitorizarea progresului, prioritizarea cererilor de suport;
- Este responsabil de asigurarea rezolvării cererilor de suport sau escaladarea acestora la un nivel superior pentru rezolvare;
- Identifică problemele și propune soluții pentru problemele identificate;
- Efectuează verificări periodice ale funcționării sistemului.

4.2.7. Expert instruire

Pentru expertul instruire se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- Studii superioare absolvite cu diplomă de licență (sau echivalent)
- Deținerea de competențe în domeniul formării și dezvoltării competențelor profesionale, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional
- Experiență specifică - participarea în minim 1 proiect de implementare sistem

informatic în care a avut responsabilități specifice rolului de expert instruire

Responsabilități în cadrul Contractului:

- Întocmește planul de instruire;
- Coordonează instruirea conform planului de instruire;
- Coordonează activitatea de instruire a administratorilor și operatorilor care vor acorda suport utilizatorilor finali.

Pentru experții non-cheie nu se solicită documente justificative care dovedesc calificarea și experiența acestora, în cuprinsul propunerii tehnice. Aceste documente se prezintă la momentul în care vor interveni în implementarea viitorului contract.

În cuprinsul propunerii tehnice, ofertanții vor descrie momentul în care vor interveni experți non-cheie în executarea viitorului contract, precum și modul în care operatorul economic, care va îndeplini calitatea de ofertant, și-a asigurat accesul la serviciile acestora (fie prin resurse proprii, caz în care vor fi prezentate persoanele în cauză, fie prin externalizare, situație în care se vor descrie aranjamentele contractuale realizate în vederea obținerii serviciilor respective). Astfel, după intrarea în vigoare a contractului, Prestatorul, la momentul intervenției experților non-cheie, va înainta documentele suport prin care se va justifica îndeplinirea cerințelor la nivelul echipei de experți non-cheie, individual, pentru fiecare expert non-cheie în parte.

Pentru demonstrarea îndeplinirii cerințelor pentru experții non-cheie se vor depune la momentul intervenției experților următoarele documente:

- CV-ul datat și semnat;
- copii conform cu originalul după diplomele/certificările/atestările relevante în raport cu cerințele din prezenta documentație;
- în vederea respectării principiul recunoașterii reciproce, precizăm că, pentru personalul nerezident, se permite prezentarea certificărilor/ autorizărilor corespunzătoare emise în țara de rezidență;
- documente relevante din care să reiasă îndeplinirea cerințelor de experiență profesională specifică, solicitate prin prezenta documentație - îndeplinirea cerințelor se face prin prezentarea de certificate/ documente cum ar fi: contracte, recomandări, procese verbale, documente constatatoare sau orice alte documente doveditoare;
- fiecare dintre persoanele propuse trebuie să îndeplinească integral toate cerințele minime aferente expertului (profilului de persoană) pentru care au fost nominalizate. Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.

Pe parcursul derulării contractului de achiziție publică, modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează conform prevederilor art. 162 din Anexa 1 (Normele metodologice) la HG nr. 395/2016.

Astfel, înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului

se realizează numai cu acceptul autorității contractante, și nu reprezintă o modificare substanțială, așa cum este aceasta definită în art. 221 din Legea 98/2016, decât în următoarele situații:

- a. noul personal de specialitate nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin criteriile de calificare/selecție prevăzute în cadrul documentației de atribuire;
- b. noul personal de specialitate nominalizat pentru îndeplinirea contractului nu obține cel puțin același punctaj ca personalul propus la momentul aplicării factorilor de evaluare.

În situațiile prevăzute anterior, contractantul are obligația de a transmite pentru noul personal documentele solicitate prin documentația de atribuire fie în vederea demonstrării îndeplinirii criteriilor de calificare/selecție stabilite, fie în vederea calculării punctajului aferent factorilor de evaluare.

Se vor avea în vedere și prevederile din Contract, anexă la prezenta documentație.

4.3. Resurse materiale

În calitate de solicitant al investiției ADR 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 ADR sau într-o locație desemnată de ADR.

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 ADR resursele materiale descrise în secțiunea de componente hardware 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, enumerăm:

Instituția	Adresa de implementare	Resurse materiale puse la dispoziție de către instituție
ADR	Sediul ADR sau locația desemnată de ADR	• Sediul propriu situat în București

Instituția	Adresa de implementare	Resurse materiale puse la dispoziție de către instituție
		- Calculatoarele membrilor echipei de proiect implicat, împreună cu echipamentele periferice alocate fiecărui calculator în parte (imprimante, scanere, etc.) - Dotările permanente ale ADR - mobilier, linii de comunicații, etc.
STS	Unul din centrele de date al Cloud-ului Privat Guvernamental Centrul de Date STS din Cristian, Jud. Brașov	Centre de date

5. GARANȚIE ȘI SUSTENABILITATE

5.1. Garanția sistemului

Pentru dezvoltările realizate în cadrul proiectului se va acorda garanție și suport tehnic pe o perioadă de 60 de luni de la data acceptanței finale, prin intermediul acestor servicii asigurându-se funcționarea corespunzătoare a tuturor funcționalităților existente la data acceptanței finale a sistemului informatic.

Pentru componentele software de tip software standard, pe parcursul unei perioade de 36 de luni de la data acceptanței finale a sistemului informatic se vor asigura cel puțin următoarele: upgrade-uri, update-uri de securitate, instalarea de patch-uri disponibile. De asemenea, pentru aceste componente, pe lângă cele 36 de luni de garanție acordate începând cu data acceptanței finale, se va acorda suport tehnic și pe toată durata implementării proiectului.

Pentru componentele hardware se va asigura SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, 24 ore timp de remediere), pe o perioadă de 3 (trei) ani acordați începând cu data acceptanței finale, care să garanteze diagnosticarea echipamentului/modulului defect și înlocuirea acestuia, fără costuri suplimentare pentru beneficiar; Suportul soluțiilor software de infrastructura care rulează pe echipamentele hardware trebuie să fie pe o perioadă de 3 (trei) ani acordați începând cu data acceptanței finale, acoperind dreptul de a face update -uri software ori de câte ori este necesar. Pe toată durata garanției, se va asigura accesul direct al personalului beneficiarului la site-ul

producătorului pentru descărcarea de update-uri software și deschidere de cazuri de suport în caz de bug-uri sau alte probleme, inclusiv pentru defecțiuni hardware ale echipamentelor.

Pe întreaga perioadă de garanție prestatorul va asigura funcționarea conform specificațiilor tehnice și funcționale agreeate în documentele de analiză de business, de arhitectură, de specificații funcționale elaborate pentru dezvoltarea și implementarea sistemului, va presta servicii de suport, iar această activitate va fi monitorizată de către managerul de proiect.

Pe perioada de garanție se vor asigura prevenirea și remedierea defecțiunilor și anomaliilor apărute.

Serviciul de suport tehnic va avea scopul de a oferi utilizatorilor finali un punct unic de contact pentru toate solicitările de intervenții, 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).

În perioada de garanție se vor presta cel puțin următoarele activități:

- consiliere și suport telefonic prin serviciul Help-desk;
- rezolvarea bug-urilor care nu au fost identificate în timpul implementării și/sau care apar în faza de producție; remedierea software se va face cu precădere de la distanță;
- întreținerea și buna funcționare a sistemului furnizat în parametrii agreeați (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- actualizări software la locația de instalare a beneficiarului sau de la distanță, inclusiv instalarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- reconfigurări ale resurselor hardware virtuale și software la nivelul inițial solicitat în cazul în care erorile apărute nu sunt datorate beneficiarului;
- consiliere și suport tehnic pentru posibilități de extindere a soluției existente;
- actualizarea manualelor de utilizare și altor documente în urma efectuării corecțiilor;
- toate incidentele vor fi gestionate prin intermediul aplicației software de gestionare a tichetelor pusă la dispoziție de către prestator.

Pe timpul derulării garanției, se vor presta următoarele intervenții:

- în condițiile apariției unei erori în funcționarea resurselor hardware virtuale sau 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, în caz de necesitate, a actualizărilor de software, remedierea în locația beneficiarului;
- actualizările de software pot face referire, dar nu limitativ, la: compilarea pe un suport magnetic 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 și pentru asigurarea bunei funcționări a produselor oferite, 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 Prestator, cu toate informațiile care descriu intervențiile respective.

Timpii de rezolvare sunt definiți în funcție de gravitatea incidentului apărut:

Nivel Criticitate	Timp de răspuns	Timp soluționare temporară	Timp soluționare finală
Critic	Maxim 4 ore	12 ore	24 ore
Mediu	Maxim 4 ore	24 ore	48 ore
Minor	Maxim 4 ore	48 ore	96 ore

Tipurile incidentelor:

- Critic: una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate, iar impactul acestui incident duce la imposibilitatea utilizării sistemului.
- Mediu: impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor funcționalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.
- Minor: impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.

Timpii de mai sus sunt calculați din momentul în care Prestatorul a fost înștiințat de apariția problemelor.

Datele și orele de înregistrare ce vor fi folosite pentru calcularea SLA-ului vor fi următoarele:

- În cazul utilizării telefonului: Data și ora de înregistrare = data și ora la care s-a încheiat convorbirea telefonică.
- În cazul utilizării e-mail-ului: Data și ora de înregistrare = data și ora la care se recepționează email-ul, reprezentând data și ora din server-ul de e-mail-uri (în cazul primirii de informații de către furnizor, respectiv data și ora la care furnizorul a trimis e-mail-ul, reprezentând data din server-ul de e-mail - în cazul transmiterii de informații de către furnizor).

La sfârșitul fiecărui caz deschis, Prestatorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului și o va include în recomandarea finală.

Prestatorul va garanta că SLA-ul mai sus menționat se bazează pe servicii de suport pentru soluția software furnizată în cadrul acestui contract. Timpii de răspuns și timpii de remediere asigurați de către Prestator pe perioada furnizării serviciilor sunt calculați conform priorității

fiecărei solicitări. Calcularea acestora se va realiza în programul de lucru de Luni până Vineri, în intervalul orar 8:30 - 17:30, cu excepția sărbătorilor legale.

Definițiile, descrise mai jos, se vor aplica la Service Level Agreement:

- Timp de Răspuns: Timpul scurs de la contactul inițial dintre beneficiar și HELPDESK și răspunsul primit de la echipa de suport tehnic a Prestatorului către Beneficiar. Această acțiune se va desfășura prin intermediul telefonului/e-mail;
- 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, dacă este posibil;
- SLA: Service Level Agreement identifică funcționalitățile și definește procesele care implică livrarea de către Prestator a diferitelor servicii de suport către Beneficiar;
- Suport: Telefonul de suport tehnic, asistență web și e-mail oferite de Prestator 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 Prestatorului care oferă asistență pentru componentele soluției informatice furnizate.

5.2. Sustenabilitate

Finalizarea proiectului de față, prin realizarea activităților prevăzute și îndeplinirea obiectivelor propuse, contribuie la soluționarea pe termen lung a problemelor cu care se confruntă ADR. După finalizarea implementării, rezultatele proiectului vor fi menținute prin activitățile specifice desfășurate în cadrul ADR, prin personalul propriu.

Se precizează ca proiectul reprezintă o inițiativă independentă din punct de vedere financiar, tehnic și al resurselor umane, implementarea să nefiind condiționată de alte activități desfășurate de instituții în perioada de referință.

5.2.1. Sustenabilitatea din punctul de vedere al asigurării capacității tehnice

Soluția tehnică trebuie să fie dimensionată pentru a asigura scalabilitatea software și hardware a aplicației pentru o perioadă de minimum 5 ani după implementarea proiectului, iar solicitantul va alocă resurse tehnice (spații, accesul la rețeaua internă proprie de date și accesul la Internet) pentru desfășurarea optimă a procesului de implementare a sistemului.

De asemenea, sustenabilitatea tehnică a proiectului va fi asigurată prin activitățile de mentenanță care vizează administrarea echipamentelor de calcul necesare bunei funcționări a soluției software implementate, asigurarea suportului tehnic intern și extern, ceea ce se va face de către furnizorii de echipamente hardware care vor asigura asistența tehnică pe o perioadă specificată în contractul de achiziție.

În ceea ce privește sistemul software, asistența tehnică va fi prevăzută în contract pentru o perioadă de minim 3 ani din momentul în care începe executarea obligațiilor contractuale, urmând ca pentru următorii ani serviciile de mentenanță și suport să fie subcontractate.

5.2.2. Sustenabilitatea din punctul de vedere al resurselor umane

Resursele umane alocate proiectului sunt suficiente atât din punct de vedere numeric cât și din punct de vedere al experienței. În situația apariției fluctuației de personal, se va desfășura instruirea noilor angajați de către personalul pregătit în cadrul proiectului. Persoanele implicate în proiect au experiența în domeniul implementării de proiecte.

Echipa va fi alcătuită din specialiști cu pregătire în diverse domenii aferente activităților desfășurate, asigurând astfel interdisciplinaritatea necesară realizării unui astfel de proiect.

5.2.3. Sustenabilitatea financiară a proiectului

Sustenabilitatea financiară reprezintă capacitatea financiară a ADR de a asigura operarea și mentenanța investiției pentru o perioadă de cel puțin 5 ani după implementarea proiectului.

Suținerea financiară se va realiza prin alocarea de fonduri de la bugetul ADR.

6. LOCUL ȘI DURATA CONTRACTULUI

6.1. Locul desfășurării activităților

Din punct de vedere tehnic, arhitectura sistemului PNI va include un mediu de producție ce va fi găzduit în Cloud-ul Privat Guvernamental și două medii ce vor fi găzduite în Centrul de Date STS din Cristian, Jud. Brașov: unul de testare-dezvoltare și unul de disaster recovery.

Echipamentele hardware vor fi instalate în cadrul Centrului de Date STS din Cristian, Jud. Brașov.

Activitățile necesare în vederea prestării serviciilor se pot desfășura la sediul ADR și la sediul Prestatorului sau în alte locații.

Având în vedere natura activităților, activitățile ce fac obiectul contractului se vor desfășura în principal în regim de telemuncă, dar Autoritatea Contractantă își rezervă dreptul de a solicita prezența experților Contractantului la sediul ei, atunci când consideră că este necesar.

6.2. Durata prestării serviciilor

Durata contractului este de maxim 24 de luni de la data semnării acestuia de către ambele părți, cu respectarea următoarelor termene pentru activitățile principale ale contractului:

- servicii de livrare și implementare a infrastructurii hardware- maxim luna 6, finalizate cu proces verbal de recepție cantitativă și calitativă;
- servicii de livrare și instalare componente software- maxim luna 15, finalizate cu proces verbal de recepție cantitativă și calitativă;
- Serviciile de pre-analiză privind interoperabilitatea inter-instituțională - maxim luna 8, finalizate cu proces verbal de recepție a raportului (documentului) de pre-analiză
- servicii de analiză a sistemului - maxim luna 9, finalizate cu proces verbal de recepție a raportului (documentului) de analiză;
- servicii de modelare/proiectare a sistemului - maxim luna 11, finalizate cu proces verbal de recepție a documentației tehnice aferentă activității de proiectare a platformei;
- servicii dezvoltare software - maxim luna 22, finalizate cu proces verbal de recepție ca rezultat al activității de dezvoltare și configurare;
- servicii de testare a platformei, inclusiv teste de securitate - maxim luna 23, finalizate cu proces verbal de recepție a raportului de testarea funcționalităților platformei;
- servicii de instruire - maxim luna 24, finalizate cu proces verbal de recepție a raportului de instruire a personalului;
- servicii de punere în producție - maxim luna 24, finalizate cu proces verbal de recepție a raportului de punere în producție.

Ofertanții pot propune desfășurarea activităților contractului în paralel, fără să depășească termenele limită prezentate mai sus, indicând în metodologia de implementare a contractului modul de abordare propus.

În situația în care ultima zi a termenului maxim de livrare, astfel calculat, este o zi nelucrătoare, se va considera că termenul se încheie la expirarea ultimei ore a următoarei zile lucrătoare.

Termenele de livrare, instalare, configurare, punere în funcțiune hardware și software, dezvoltare, testare, instruire și punere în producție la nivel de servicii include timpul necesar recepției cantitative și calitative a produselor și soluțiilor.

Livrarea produselor și soluțiilor se va putea face parțial, cu acordul prealabil, în scris, al Autorității Contractante. Termenul de livrare, instalare, punere în funcțiune, configurare, testare, operaționalizare și integrare nu trebuie să depășească termenul maxim solicitat de Autoritatea Contractantă.

Contractantul trebuie să asigure, fără nici un cost suplimentar pentru Autoritatea Contractantă, integrarea tuturor produselor livrate, instalate, puse în funcțiune inclusiv prestarea tuturor serviciilor, pe parcursul întregului contract.

Certificarea faptului că produsele au fost furnizate la destinația finală, se va face prin semnarea de primire a produselor și soluțiilor de către reprezentanții autorizați ai Autorității Contractante pe avizele de însoțire a mărfii eliberate de Contractant.

6.3. Opțiuni de suplimentare

Autoritatea contractantă își rezervă dreptul de a achiziționa cantități suplimentare de servicii și/sau produse dacă este îndeplinită una din condițiile enumerate mai jos:

- (i) valoarea atribuită a contractului este mai mică decât valoarea estimată a achiziției iar economiile înregistrate în procesul de atribuire a contractului de achiziție pot fi mobilizate în acest scop;
- (ii) pe parcursul executării contractului, autoritatea contractantă constată că necesarul de servicii/produse de tipul celor ce fac obiectul prezentului contract este mai mare decât cel prevăzut inițial;

În conformitate cu prevederile art. 221. alin. (1) lit. a), autoritatea contractantă își rezervă opțiunea de a achiziționa cantități suplimentare de servicii/produse la prețurile unitare din propunerea financiară detaliată, în limita maximă a economiilor înregistrate la atribuirea contractului de achiziție publică.

Autoritatea contractantă va notifica Contractorului intenția de a-și exercita această opțiune cu minimum 30 de zile înainte, urmând ca modificarea să se reflecte la nivel contractual prin încheierea unui act adițional.

Opțiunea de achiziționare suplimentară nu va fi luată în considerare dacă finanțarea nu este disponibilă sau dacă performanța anterioară a Contractantului este NESATISFĂCĂTOARE sau FOARTE NESATISFĂCĂTOARE.

7. IPOTEZE ȘI RISCURI. MĂSURI DE GESTIONARE A RISCURILOR

7.1. Ipoteze

Ipotezele care pot fi considerate la acest moment sunt următoarele:

- a) buna cooperare între Contractant și Autoritate Contractantă, în special între persoanele desemnate în derularea contractului;
- b) Contractantul va furniza produsele la un înalt nivel de calitate, cel puțin egal cu cel solicitat în prezentul Caiet de Sarcini;
- c) specificațiile produselor solicitate sunt descrise în mod explicit în Caietul de Sarcini;
- d) corelația dintre resursele necesare și rezultatele așteptate este realistă;
- e) începerea activităților se va realiza în perioada preconizată;
- f) nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
- g) toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea activităților vor fi puse la dispoziția Contractantului.

7.2. Riscuri

Pentru a identifica și combate efectele adverse pe care Contractul ar putea să le întâmpine, a fost construită o matrice de risc în vederea observării posibilelor cauze ale riscurilor și pentru a atribui o probabilitate de apariție fiecărui eveniment advers.

Categoriile de riscuri identificate în ceea ce privește implementarea Contractului au fost de natură administrativă, legislativă, organizatorică, contractuală, financiară și managerială.

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, aflate în sfera sa de responsabilitate.

Metodologia de gestiune a riscurilor conduce la identificarea și analizarea acestora, cu impact asupra atingerii obiectivelor, identificarea soluțiilor și reducerea expunerii la pierderi.

Riscurile și măsurile de atenuare a acestora care vor fi luate în considerare pe durata implementării serviciilor, sunt:

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
1.	Prelungirea termenelor procedurilor de achiziție publică	- realizarea și actualizarea permanentă a unui plan de achiziții - analiza permanentă a legislației referitoare la achizițiile publice - un membru al echipei de proiect are rolul de a coordona și realiza derularea achizițiilor publice
2.	Începerea activităților cu întârziere	- realizarea și actualizarea permanentă a unui plan de management - monitorizarea permanentă a respectării termenelor
3	Fluctuații de personal	- selectarea atentă a persoanelor din echipa de proiect - selectarea unei echipe de formate din persoane externe, care vor fi angajate pe toata durata proiectului
4	Modificări legislative care influențează implementarea proiectului	- monitorizarea permanentă a modificărilor legislative - respectarea Contractului de finanțare
5	Indisponibilitatea unor produse/servicii prevăzute în proiect	- plan de achiziții realist, care corespunde ofertei de pe piață - informarea prealabilă privind disponibilitatea de oferte și livrare de servicii și bunuri
6	Calitate necorespunzătoare a produselor/serviciilor	- selecția atentă a furnizorilor de bunuri și servicii, inclusiv pe baza performanțelor dovedite anterior - întocmirea unor documentații de atribuire acoperitoare elaborarea unor clauze stricte în contracte referitor la neîndeplinirea obiectivelor la nivelul de calitate solicitat
7	Modificări în structura organizatorică a Contractantului	- asigurarea flexibilității în planificarea și utilizarea resurselor umane incluse în proiect și posibilitatea suplimentării resurselor alocate în cazul în care riscul se materializează
8	Probleme de comunicare și coordonare între membrii echipei de proiect	- stabilirea și monitorizarea respectării unui circuit de comunicare între membrii echipei de proiect
9	Riscuri politice: - instabilitatea factorului politic poate duce la schimbări legislative și normative; - poate induce instabilitate la	- atenuarea efectelor acestui risc se va efectua asigurând o echipa dedicată implementării acestui proiect, astfel încât deciziile politice să nu influențeze realizarea investiției.

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
	nivel administrativ și decizional prin schimbări în organizarea, funcționarea și/sau conducerea instituțiilor	

Ofertantul va prezenta în cadrul Propunerii tehnice un **Plan de management al riscurilor**. Această secțiune va conține cel puțin următoarele:

- descrierea unor riscuri suplimentare relevante, identificate de Ofertant, care pot afecta execuția contractului, precum și măsurile asociate de răspuns/atenuare a riscurilor astfel identificate, cât și responsabilul alocat;
- recomandări suplimentare de reducere/atenuare/eliminare pentru riscurile identificate de Autoritatea Contractantă, fără afectarea cerințelor Caietului de Sarcini.

8. ATRIBUȚIILE ȘI RESPONSABILITĂȚILE PĂRȚILOR

Atribuțiile și responsabilitățile Părților vor fi guvernate de prevederile prezentului Caiet de Sarcini și ale Contractului care va fi semnat între ADR și operatorul economic desemnat câștigător, în conformitate cu prevederile documentației de atribuire.

În raport cu serviciile/produsele solicitate și cu cerințele stipulate în prezentul Caiet de Sarcini, responsabilitățile și atribuțiile părților sunt:

8.1. Obligațiile principale ale Contractantului

Contractantul are următoarele obligații principale:

- mobilizarea de resurse suficiente și cu expertiză adecvată pentru a asigura gestionarea Contractului, astfel cum este solicitat la nivelul Caietului de Sarcini;
- 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;
- asigurarea unui grad de flexibilitate în planificarea modalității de gestionare a contractului, pe toată durata de derulare a contractului;
- transmiterea datelor de identificare și de contact ale personalului alocat pentru executarea Contractului;
- colaborarea cu personalul Autorității Contractante alocat pentru verificarea produselor livrate și realizarea recepțiilor;
- 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) colaborarea cu personalul Autorității Contractante alocat pentru prestarea serviciilor și furnizarea produselor care fac obiectul Contractului;
- j) completarea unei Declarații de imparțialitate, confidențialitate și privind conflictul de interese de către Personalul desemnat de Contractant, înainte de implicarea în implementarea Contractului;
- k) la livrarea produselor și soluțiilor, Contractantul trebuie să asigure respectarea practicilor de securitate în muncă și de protecție a mediului înconjurător;
- l) Livrările, instalările, configurările, punerile în funcțiune, operaționalizările și integrarea produselor și soluțiilor trebuie să fie în concordanță cu termenele de livrare, instalare, configurare, punere în funcțiune, testare, operaționalizare și integrare prezentate de Contractant în propunerea tehnică;
- m) Contractantul este responsabil să se asigure că pentru toate activitățile cuprinse în propunerea tehnică dispune de toate resursele necesare pentru îndeplinirea Contractului.

Obligațiile principale ale Contractantului se completează cu obligațiile prevăzute în contract.

8.2. Obligațiile principale ale Autorității Contractante

Autoritatea Contractantă are următoarele obligații principale:

- a) desemnarea unei persoane sau a unei echipe pentru monitorizarea Contractului;
- b) punerea la dispoziția Contractantului a tuturor informațiilor disponibile și necesare pentru derularea Contractului în timpul stabilit și la nivelul de calitate și performanță prevăzut în Caietul de Sarcini;
- c) asigurarea accesului în spațiile în care urmează a se realiza prestarea/livrarea, după caz instalarea produselor;
- 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 și produselor care fac obiectul Contractului, respectiv care confirmă prestarea serviciilor/furnizarea produselor potrivit condițiilor de calitate stabilite în Caietul de Sarcini;
 - j) personalul Autorității Contractante va participa la testarea produselor și soluțiilor livrate și va asigura suport în vederea realizării activităților specifice recepției. În acest sens, Autoritatea Contractantă va verifica documentele de acceptanță și de recepție, asigurând semnarea acestora de către reprezentanții Autorității Contractante care au participat la recepție;
 - k) Autoritatea Contractantă se va asigura de respectarea termenelor pentru efectuarea recepțiilor cantitative și calitative, iar după caz, conform clauzelor contractuale, va efectua pe parcursul recepției și alte teste relevante, altele decât cele propuse de Contractant, pentru a se asigura de conformitatea produselor și soluțiilor livrate cu cerințele din prezentul Caiet de Sarcini;
 - l) Autoritatea Contractantă va elibera Contractantului documente constatatoare care să conțină informații referitoare la îndeplinirea obligațiilor contractuale de către acesta, în termenele prevăzute de lege.

Obligațiile principale ale Autorității contractante se completează cu obligațiile prevăzute în contract.

9. DOCUMENTE CE TREBUIE FURNIZATE AUTORITĂȚII CONTRACTANTE

Documentele obligatorii pe care Contractantul trebuie să le livreze Autorității Contractante în cadrul Contractului sunt:

- a) Livrabilele și rapoartele precum și orice alte documente menționate în prezentul Caiet de Sarcini;
- b) Procese verbale de predare-primire
- c) Procese-verbale de acceptanță pentru livrabilele / rapoartele prevăzute în prezentul caiet de sarcini;
- d) Declarații de calitate și conformitate UE a producătorului/ Contractantului întocmite cu respectarea prevederilor art. 4, 5 și 6, din OUG 140/ 2021 privind anumite aspecte referitoare la contractele de vânzare de bunuri, care atestă conformitatea produselor cu legislația aplicabilă conform Blue Guide
https://europa.eu/youreurope/business/productrequirements/compliance/technical-documentation-conformity/index_ro.htm / <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016XC0726%2802%29>. Prin

prezentarea declarației pe propria răspundere a producătorului, autoritatea contractantă se asigură de conformitatea produselor cu toate normele juridice de obținere a marcajului CE, de validitatea comercializării produselor în Zona Economică Europeană și de libera circulație a produselor pe piața europeană. Se certifică astfel că produsele sunt proiectate și fabricate în conformitate cu cerințele de bază ale unei directive a CE, pentru a demonstra și a-i asigura de acest lucru pe toți utilizatorii din țările europene și pentru a fi comercializat în mod legal;

- e) Avizul de expediție a produselor;
- f) Certificate de garanție aferente produselor/soluțiilor livrate emise de Contractant / producător;
- g) Manualele de folosire / operare / mentenanță/documentația tehnică a produselor încorporate în serviciile prestate în limba engleză/română;
- h) Raport privind testarea;
- i) Dosarul de instruire al personalului (Suport de curs, Liste de prezență, Chestionare evaluare instruire, Certificate de participare);
- j) Proces-verbal de acceptanță pentru punerea în producție a platformei implementate;
- k) Rapoarte tehnice;
- l) Procese-verbale de recepție cantitativă și calitativă parțiale/finale pentru serviciile prestate/ produsele livrate;
- m) Factura fiscală.

10. PROCEDURA DE ACCEPTANȚĂ

• Recepția

Recepția serviciilor și a produselor reprezintă procesul prin care un produs sau un livrabil sau un serviciu este acceptat sau respins de către o comisie nominalizată a Autorității Contractante.

Acceptarea/Respingerea se va constata prin emiterea de către Autoritatea Contractantă a documentului denumit „proces verbal de recepție” din care va rezulta ce se acceptă / respinge și criteriile în baza cărora comisia a decis aprobarea/respingerea produsului sau livrabilului sau serviciului.

În cadrul fiecărei etape/fază se va derula cel puțin o recepție sau dacă este cazul mai multe recepții aferente produselor / livrabilelor / serviciilor, iar fiecare astfel de recepție va fi documentată corespunzător.

În cazul în care Autoritatea Contractantă emite un proces verbal de recepție prin care respinge o livrare a prestatorului, atunci Autoritatea Contractantă va enunța în document în clar motivul/motivele pentru care respinge livrarea. Prestatorul are obligația de a reface / înlocui pe cheltuiala proprie și de a solicita o nouă recepție. În cadrul noului proces de recepție Autoritatea Contractantă va putea emite noi observații doar la punctele la care

anterior a emis observații.

Recepția serviciilor prestate și a produselor furnizate se poate realiza în mai multe etape, în funcție de progresul contractului.

Pentru soluțiile și funcționalitățile oferite, 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 de către Autoritatea Contractantă a acestor soluții/funcționalități.

- **Acceptanța Parțială (Provizorie)**

Este data (momentul în timp) la care Autoritatea Contractantă emite către Prestator documentul „proces verbal de acceptanță parțială (provizorie)”.

Procesele verbale de acceptanță parțială (provizorie) vor fi emise în baza proceselor verbale de recepție care au fost aprobate. Documentele vor atesta că prestatorul și-a îndeplinit parțial obligațiile rezultate din caietul de sarcini, respectiv că produsele au fost livrate și serviciile au fost prestate.

Documentul “proces verbal de acceptanță parțială (provizorie)” nu va fi emis dacă un produs sau un livrabil sau un serviciu a fost respins de către Autoritatea Contractantă și ulterior nu a mai fost acceptat/aprobat printr-un nou proces verbal de recepție.

- **Acceptanța Finală**

Este data (momentul în timp) la care Autoritatea Contractantă emite către Prestator documentul „proces verbal de acceptanță finală”. Documentul va fi emis în baza proceselor verbale de acceptanță parțială (provizorie) și reprezintă obținerea acordului final din partea beneficiarului proiectului.

11. MANAGEMENTUL 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.

Pe parcursul derulării Contractului, Autoritatea Contractantă verifică la intervale stabilite și comunicate prin Caietul de Sarcini dacă toate activitățile planificate au fost realizate conform cerințelor.

Atât Ofertantul devenit Contractant, cât și Autoritatea Contractantă vor urmări finalizarea și conformitatea cu scopul contractului a livrabilelor prevăzute în cadrul acestuia, plățile fiind efectuate după recepționarea acestora, conform mențiunilor privind acceptanța/recepția. Monitorizarea contractului se va realiza de către echipa de proiect prin întocmirea rapoartelor pe fiecare din fazele contractului.

METODOLOGIE ȘI PLAN DE LUCRU (DE IMPLEMENTARE)

Ofertanții vor detalia într-o anexă distinctă / anexe distincte **Metodologia și Planul de lucru (de implementare)** ținând cont de informațiile detaliate în prezentul Caiet de Sarcini și de instrucțiunile pentru ofertanți detaliate în secțiunea IV.4.1 Modul de prezentare a Propunerii tehnice, din Anunțul de participare publicat în SEAP.

Metodologia și planul de implementare sunt componente-cheie și obligatorii ale ofertei tehnice. În cadrul ofertei tehnice trebuie prezentate următoarele:

- a) **Metodologia utilizată pentru realizarea serviciilor;**
- b) **Planul de implementare pentru realizarea serviciilor;**
- c) **Personalul utilizat pentru realizarea serviciilor și organizarea acestuia.**

Pentru a demonstra o foarte bună înțelegere a Caietului de Sarcini metodologia și planul de lucru trebuie să fie adaptate cerințelor specifice ale contractului, fiind descurajate abordările de tip copy-paste.

Activitatea de management de proiect trebuie să se desfășoare conform unui cadru (framework) de management de proiect recunoscut internațional de către organisme profesionale specifice de Project Management. Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei proprii de management de proiect pe care o va utiliza în cadrul proiectului.

Implementarea trebuie să acopere următoarele:

- Serviciile de livrare și instalare hardware;
- Serviciile de livrare și instalare software;
- Serviciile de pre-analiză privind interoperabilitatea inter-instituțională;
- Serviciile de analiză;
- Serviciile de modelare/proiectare a sistemului;
- Serviciile de dezvoltarea softului de aplicație;
- Serviciile de testare și asigurare a calitatii sistemului;
- Serviciile de instruire utilizatori;
- Serviciile de punere în producție.

Planul care va fi prezentat împreună cu oferta trebuie să acopere cel puțin toate tipurile de activități menționate mai sus.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice modalitatea în care se va realiza raportarea progresului pentru activitățile din cadrul proiectului.

Ofertantul trebuie să prezinte în cadrul proiectului modalitatea prin care se va realiza comunicarea între participanții la proiect.

Ofertantul va prezenta în cadrul propunerii tehnice modul în care se va gestiona rezolvarea problemelor care pot să apară pe parcursul proiectului. Se va descrie procesul de management al problemelor și formularele care vor fi utilizate pentru managementul problemelor, escaladarea și rezolvarea acestora.

Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanță care va fi utilizat în cadrul proiectului pentru recepțiile/acceptanțele parțiale (provizorii) și recepția/acceptanța finală. Se va prezenta planul împărțit pe etape.

Ofertantul va propune în cadrul ofertei formularele aferente recepțiilor/acceptanțelor parțiale (provizorii) și recepției/acceptanței finale, iar autoritatea contractantă le va aproba înainte de a fi utilizate.

Ofertantul va prezenta în cadrul propunerii tehnice și **modalitatea de tratare a schimbărilor în cadrul proiectului**. Se va prezenta procedura de management al schimbărilor precum și formularele care vor fi utilizate în cadrul acestui proces pe durata proiectului.

Pentru buna desfășurare a activităților și atingerea rezultatelor proiectului, Contractantul va colabora permanent cu echipa de implementare a proiectului.

În termen de **3 zile lucrătoare** de la data începerii contractului, va fi organizată o întâlnire de lucru la care vor participa reprezentanți ai Autorității Contractante (membrii echipei de implementare a proiectului) și ai Contractantului (directorul de proiect și alți experți cheie a căror prezență este considerată necesară de către Contractant).

În cadrul acestei întâlniri vor fi stabilite următoarele:

- principiile de comunicare reciprocă;
- planul de lucru, prin raportare la graficul de desfășurare a activităților
- detaliile privind colaborarea;
- frecvența reuniunilor;
- modelele de procese-verbale;
- modelele de rapoarte privind progresele înregistrate;
- planurile de acțiune în cazul apariției unor probleme;
- alte detalii logistice și organizaționale.

Pentru a demonstra o foarte bună înțelegere a caietului de sarcini metodologia și planul de lucru trebuie să fie adaptate cerințelor specifice ale contractului, fiind descurajate

abordările de tip copy-paste.

În cadrul prezentării abordării sale pentru implementarea proiectului, ofertantul va realiza, pe lângă prezentarea modalității de realizare a fiecărei activități prezentate în graficul Gantt, prezentarea abordării sale în sensul managementului riscurilor asociate activităților de pe calea critică a proiectului (se va face în mod obligatoriu analiza activităților critice și se vor prezenta măsurile pe care prestatorul le va lua pentru a se asigura că fiecare dintre aceste activități nu întârzie și astfel, termenul de finalizare se poate respecta). Analiza activităților critice este obligatorie, lipsa sa fiind motiv de respingere a ofertei.

11.1. METODOLOGIA

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.

În această secțiune trebuie prezentat modul în care ofertantul înțelege:

- obiectivele contractului și sarcinile stabilite prin Caietul de Sarcini;
- modul de abordare ce va fi urmat în livrarea produselor și prestarea serviciilor,
- inclusiv descrierea conceptului utilizat pentru atingerea obiectivelor contractului;
- metodologia de realizare a activităților în scopul obținerii rezultatelor așteptate.

Metodologia trebuie să conțină:

- 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 responsabilitățile stabilite prin Caietul de Sarcini. Activitățile descrise la acest capitol trebuie reprezentate ca durată, la capitolul aferent din planul de implementare și trebuie reflectate în propunerea financiară sub aspect valoric la nivel de etapă și la nivel de pachet de licențe;
- descrierea soluției propriu-zise propuse pentru îndeplinirea obiectivelor stabilite prin Caietul de Sarcini.

11.2. PLANUL DE LUCRU (DE IMPLEMENTARE)

Planul de lucru propus, parte obligatorie a propunerii tehnice, trebuie:

- să demonstreze înțelegerea prevederilor Caietului de Sarcini;
- să demonstreze abilitatea de a transpune prevederile într-un plan de lucru fezabil;

- să demonstreze încadrarea activităților în timp de așa manieră încât să se asigure finalizarea serviciilor în termenul specificat în Caietul de Sarcini.
- să conțină denumirea și durata activităților din cadrul contractului, așa cum vor fi acestea prezentate la capitolul „Metodologie”;
- să conțină succesiunea și interrelaționarea acestor activități. Nu este permisă utilizarea în cadrul graficului Gantt a unor constrângeri de start sau de finalizare având la bază momente de timp arbitrar alese. Toate activitățile, cu excepția primei activități a proiectului, care nu va avea predecesor, vor avea dependențe clar identificate de alte activități;
- să conțină punctele-cheie de control - „jaloanele” proiectului;
- să fie conform cu abordarea și metodologia propusă;
- să conțină resursele materiale și de personal alocate fiecărei activități în raport cu necesitatea atingerii rezultatelor/ livrabililor, cu evidențierea momentelor semnificative ale proiectului și utilizarea resurselor pentru fiecare activitate;
- să fie realizat utilizând un software de planificare a timpului care să permită stabilirea duratelor și a dependențelor și evidențierea căii critice a proiectului, precum și replanificarea automată a activităților în cazul decalării unor termene (fără a fi necesară replanificarea manuală a tuturor activităților care depind de activitatea care a suferit decalaje);
- să conțină toate termenele de transmitere observații și aprobare aparținând autorității contractante pentru fiecare livrabil în parte, termenele de implementarea ale prestatorului pentru observațiile primite de la beneficiar, cât și a tuturor termenelor enumerate la nivelul caietului de sarcini;
- să cuprindă alte activități (dependențe) ale autorității contractante - acele activități ale autorității contractante de care depind activități ale Prestatorului.

11.3. ORGANIZAREA ȘI PERSONALUL

Capitolul din ofertă „Organizarea și personalul” trebuie să conțină:

- structura echipei propuse pentru managementul contractului;
- modul de abordare a activității de raportare cu privire la progresul serviciilor,
- inclusiv documentele finale în raport cu prevederile Caietului de Sarcini;
- descrierea infrastructurii pe care contractorul o utilizează pentru realizarea activităților propuse pentru îndeplinirea obiectului contractului;
- modul de abordare a activităților corespunzătoare îndeplinirii cerințelor privind sănătatea și securitatea în muncă, inclusiv modul în care ofertantul devenit contractant se va asigura că pe parcursul executării contractului obligațiile legale referitoare la condițiile de muncă și protecția muncii sunt respectate (dacă este cazul);
- modul de abordare și gestionare a relației cu subcontractorii, în raport cu activitățile subcontractate (dacă este cazul);

11.4. 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 care apare în procesul de implementare, evitând implicarea acesteia în aspecte de micro management al Contractului.

11.4.1. 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 **3 zile lucrătoare** de la data începerii 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 va pune la dispoziția contractantului datele de care dispune Autoritatea Contractantă necesare desfășurării activităților.

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.

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/planificate 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 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.

11.4.2. *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.

11.5. RAPORTARE

Contractantul este responsabil de elaborarea și transmiterea următoarelor rapoarte către Autoritatea Contractantă:

Nr. crt.	DESCRIERE RAPOARTE
1	Raport Inițial
2	Rapoarte tehnice (anterior convocării oricărei recepții și, implicit anterior emiterii oricărei facturi): - Raport de livrare și instalare hardware - Raport de livrare și instalare software - Raport de pre-analiză privind interoperabilitatea inter-instituțională - Raport de analiza - Raport de modelare/proiectare - Raport de dezvoltare - Raport de testare și asigurare a calității sistemului - Raport de punere în producție - Rapoarte de instruire
3	Alte rapoarte: - Raport trimestrial intermediar de audit intern
4	Raport final

11.5.1. Raportul Inițial

Va fi întocmit în cel mult 7 zile de la demararea contractului. Acest document trebuie să aibă în vedere precizările din Caietul de Sarcini și Propunerea tehnică și să aducă detalierile necesare, structurări sau clarificări unde este cazul.

Raportul va cuprinde planificarea activităților, metodologia utilizată și indicatorii planificați pentru fiecare etapă. Raportul inițial va constitui principalul instrument de lucru și se va face referire la el pe toată perioada de executare a Contractului. Raportul inițial va fi înaintat spre aprobare Autorității Contractante.

11.5.2. Rapoarte tehnice

Anterior convocării oricărei recepții și, implicit anterior emiterii oricărei facturi, Contractantul va elabora un **raport tehnic** în care va preciza cel puțin:

- a) detalii tehnice cu privire la activități derulate și rezultate obținute în termeni cantitativi și calitativi;
- b) detalii referitoare la măsurile întreprinse pentru prevenirea/evitarea conflictului de interese;
- c) dificultățile întâmpinate în cursul implementării activităților și soluțiile propuse pentru a depăși respectivele dificultăți, dacă este cazul;
- d) întârzieri înregistrate, dacă este cazul;
- e) recomandări/propuneri de planificare a activităților pentru perioada următoare, dacă este cazul;
- f) alte informații solicitate de către Autoritatea Contractantă/Organismul Intermediar.

Raportul va avea anexate documente justificative, după caz:

- livrabile realizate în cadrul contractului până la momentul raportării;
- alte documente solicitate de finanțator, prevăzute în instrucțiunile ulterioare.

11.5.3. Alte rapoarte

Contractantul va oferi, pe durata contractului, **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.

Autoritatea Contractantă poate cere Contractantului să elaboreze pe parcursul derulării Contractului și alte rapoarte, în măsura în care acestea sunt legate de buna desfășurare a Contractului. Rapoartele intermediare de audit vor fi transmise până în data de 5 a următoarei perioade pentru care se face raportarea (de ex. Raportul aferent activității din perioada ianuarie-martie se va transmite până pe data de 5 aprilie). În cazul în care data de 5 a lunii respective este o zi nelucrătoare, Prestatorul va anticipa transmiterea raportului trimestrial. De la depunerea rapoartelor inițial și a celor trimestriale Beneficiarul va analiza documentele și va formula observații în termen de 10 zile lucrătoare. Prestatorul va implementa observațiile și comentariile transmise de Beneficiar în termen de maximum 5 zile lucrătoare de la primirea lor, urmând ca aceste rapoarte să fie acceptate în termen de 3 zile lucrătoare de la implementarea observațiilor.

11.5.4. Raportul final

Acest raport trebuie să descrie întreg procesul de execuție și va înlesni evaluarea rezultatelor obținute atât în termeni calitativi, cât și cantitativi.

O versiune preliminară a acestui raport (Proiectul raportului final) trebuie să fie transmisă Beneficiarului cu 10 zile lucrătoare înainte de finalizarea perioadei de execuție a contractului. Versiunea preliminară a acestui raport are ca scop simplificarea și verificarea din timp a raportului final.

Raportul final va cuprinde:

- evaluarea succesului și constrângerilor majore pentru fiecare activitate;
- realizările generale ale Contractului;
- recomandări pentru acțiuni viitoare cu scopul asigurării durabilității activităților, rezultatele așteptate după finalizarea Contractului, precum și măsurile ce trebuie întreprinse de către Beneficiar în acest sens.

De la depunerea versiunii preliminare a raportului final Beneficiarul va analiza documentele și va formula observații în termen de 5 zile lucrătoare, urmând ca Prestatorul să le implementeze în termen de maximum 3 zile lucrătoare de la primirea lor. Prestatorul poate optimiza duratele activităților aflate în sarcina sa, cu respectarea termenelor stabilite de autoritatea competentă pentru aprobare și transmitere observații. Ulterior implementării observațiilor, Prestatorul va preda versiunea finală a raportul final, urmând ca acesta să fie aprobată de către Beneficiar în termen de 3 zile lucrătoare..

11.5.5. Acceptarea livrabilelor sau rapoartelor /recepții în cadrul Contractului

Acceptarea livrabilelor/rapoartelor obținute din derularea Contractului, care nu presupun plăți, dar necesită aprobare din partea autorității contractante se finalizează prin semnarea proceselor-verbale de acceptanță.

Recepția în vederea efectuării plăților parțiale/finale se va efectua pe baza de procese verbale de recepție cantitativă și calitativă parțiale/finale semnate de contractant și reprezentanții autorității contractante. Reprezentantul Contractantului va semna procesele verbale pentru luare la cunoștință și posibilitatea de a prezenta eventuale explicații și/sau observații.

Procesul verbal de recepție parțială atestă îndeplinirea parțială de către Contractor a obligațiilor prevăzute în Caietul de Sarcini, respectiv faptul că serviciile au fost prestate/produsele au fost furnizate corespunzător. Documentul „proces verbal de recepție parțială” nu va fi emis dacă un serviciu/produs au fost respinse de către Autoritatea

Contractantă și ulterior nu a mai fost acceptat/aprobat printr-un nou proces verbal de recepție.

Dreptul Autorității Contractante de a verifica, dacă este necesar, de a respinge serviciile/produsele furnizate, nu va fi limitat sau amânat din cauza faptului că serviciile/produsele au fost verificate de Contractant.

11.5.6. Finalizarea prestării serviciilor/livrării produselor în cadrul Contractului

Autoritatea Contractantă va considera prestarea serviciilor/furnizarea produselor din cadrul Contractului finalizată, 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.

La finalizarea prestării serviciilor/ furnizării produselor, realizarea cantitativă / calitativă a rezultatelor va fi constatată și consemnată de către reprezentanții Autorității Contractante și Ofertantului devenit Contractant în Procesul-verbal de recepție cantitativă și calitativă finală.

11.5.7. 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.

În susținerea acestui demers, în planul de lucru (de implementare) ofertantul va alocă timpuri suficiente de verificare, validare și aprobare din punct de vedere calitativ pentru produsele livrate, serviciile prestate și pentru livrabilele/documentele/rapoartele rezultate, în termen de 10 zile lucrătoare de la predarea acestora, dacă nu se specifică altfel.

Ofertantul va prezenta în cadrul propunerii tehnice o descriere următoarelor proceduri de lucru: Procedura de asistență tehnică, mentenanță și suport, Procedura de livrare, Procedura de recepție/acceptanță parțială (provizorie)/acceptanță finală, Procedura de ședințe, Procedura de control al livrărilor, Procedura de testare a livrabilelor (inclusiv cele de tip software).

11.5.8. Asigurarea calității și Evaluarea performanței contractantului

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.

Contractantul va presta serviciile și va furniza produsele descrise în prezentul Caiet de Sarcini, asigurând un standard de calitate ridicat și va gestiona toate aspectele administrative și de organizare necesare.

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.

În scopul eficientizării modului de derulare a contractului, evitării unor întârzieri în implementare datorate elaborării incomplete și/sau superficiale a livrabilelor, precum și facilitării procesului de aprobare a acestora de către comisia de recepție stabilită la nivelul

Autorității Contractante, se vor utiliza indicatorii de performanță de mai jos:

Nivelul de Calitate a livrabililor proiectului:

INDICATOR	DESCRIEREA INDICATORULUI
Categorie indicator	Tehnic - nivel de calitate
Denumire indicator de performanță	Nivelul de Calitate a rezultatelor/livrabililor contractului
Nivelul de performanță așteptat	Produs / Livrabil predat conform cerințelor stabilite în Caietul de Sarcini
Formula de calcul	Nivelul de acuratețe al livrabililor după “peer review” (sub nivelul de calitate, agreeat conform cerințelor stabilite în Caietul de Sarcini și/sau prezentat în oferta tehnică)
Modalitatea de evaluare	Calificativele vor fi acordate după cum urmează: Foarte satisfăcător (5 PUNCTE) - Livrabilele includ îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini și prezentate în oferta tehnică. Satisfăcător (4 PUNCTE) - Livrabilele includ unele îmbunătățiri și nu includ neconformități/inexactități față de nivelul agreeat. Au fost necesare doar ajustări nemateriale. Acceptabil (3 PUNCTE) - Livrabilele nu includ neconformități/inexactități față de nivelul agreeat 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 agreeat 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) - Produs / Livrabil predat cu mult după încheierea termenelor convenite Livrabilele prezintă neconformități / inexactități majore față de nivelul agreeat, 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
--	--

Termenele de prestare și furnizare:

INDICATOR	DESCRIEREA INDICATORULUI
Categorie indicator	Tehnic - nivel de calitate
Denumire indicator de performanță	Termenele de predare a rezultatelor/livrabilelor contractului
Nivelul de performanță așteptat	Produs / Livrabil predat în termenul agreat
Formula de calcul	Se compară termenele efective de prestare și livrare cu termenele convenite în Graficul aprobat
Modalitatea de evaluare	Calificativele vor fi acordate după cum urmează: Foarte satisfăcător (5 PUNCTE) - Produs / Livrabil predat în termenele convenite. Satisfăcător (4 PUNCTE) - Produs / Livrabil predat imediat după încheierea termenelor convenite însă fără întârzierea activităților din calendarul general al proiectului. Acceptabil (3 PUNCTE) - Produs / Livrabil predat după încheierea termenelor convenite conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate. Nesatisfăcător (2 PUNCTE) - Produs / Livrabil predat cu mult după încheierea termenelor convenite conducând la întârzieri ale activităților din calendarul general al proiectului pentru mai mult de 60 de zile. Foarte nesatisfăcător (1 PUNCT) - Produs / Livrabil predat cu mult după încheierea termenelor convenite conducând la întârzieri majore ale activităților din calendarul general al proiectului pentru mai mult de 90 de zile

11.5.9. Protecția muncii

În baza prevederilor art.51 alin.2) din Legea nr.98/2016, Ofertanții sunt obligați să indice în cadrul ofertei faptul că la elaborarea acesteia au ținut cont de obligațiile referitoare la

condițiile de muncă și protecția muncii, completând și transmițând Declarația privind respectarea legislației privind condițiile de mediu, social și cu privire la relațiile de muncă pe toată durata de îndeplinire a contractului.

Informații privind reglementările în vigoare la nivel național în acest domeniu se pot obține de la Inspekția Muncii sau de pe site-ul:

<http://www.inspectmun.ro/Legislatie/legislatie.html>

<http://www.inspectmun.ro/site/Legislatie/legislatie.html>

Conform prevederilor art.37 alin.2) lit.d) din H.G. nr.395/2016 în cazul în care nu se asigură respectarea reglementărilor obligatorii referitoare la condițiile specifice de muncă și de protecție a muncii, Oferta va fi considerată inacceptabilă.

11.5.10. Cerințe și informații privind respectarea principiului „de a nu prejudicia în mod semnificativ (DNSH)”

Pe toată perioada realizării serviciilor, Contractantul trebuie să se asigure de respectarea principiului „Do No Significant Harm” (DNSH)¹ și că toate serviciile prestate sunt desfășurate într-un mod responsabil, minimizând impactul negativ asupra mediului și societății.

Astfel, în aplicarea principiului DNSH, Contractantul trebuie să respecte următoarele cerințe:

- i. echipamentele utilizate pentru prestarea serviciilor trebuie să îndeplinească cerințele energetice stabilite în conformitate cu Directiva 2009/125/CE¹ pentru servere și stocarea datelor sau computere și servere informatice,
- ii. serviciile prestate trebuie realizate cu respectarea celor mai bune practici privind eficiența energetică a echipamentelor utilizate și gestionarea energiei,
- iii. să evalueze impactul potențial al serviciilor prestate asupra mediului și societății,
- iv. să identifice și implementeze măsuri de reducere a impactului negativ,
- v. să asigure conformitatea cu legislația și reglementările locale și internaționale privind protecția mediului;
- vi. să includă informații privind evaluarea impactului și măsurile adoptate în rapoartele de progres.

Autoritatea Contractantă își rezervă dreptul de a solicita, în orice moment pe perioada derulării contractului informații și evidențe privind modalitatea de aplicare a acestui principiu în prestarea serviciilor aferente contractului.

¹ Directiva 2009/125/CE a Parlamentului European și a Consiliului, din 21 octombrie 2009, de instituire a unui cadru pentru stabilirea cerințelor în materie de proiectare ecologică aplicabile produselor cu impact energetic

În Propunerea Tehnică Ofertantul trebuie să prezinte modalitatea în care se asigură de respectarea principiului DNSH pe toată perioada derulării Contractului.

Ofertantul va prezenta totodată o declarație privind respectarea principiului DNSH.

12. MODALITĂȚI SI CONDIȚII DE PLATĂ

Plata serviciilor prestate se va realiza în mai multe tranșe, pentru livrabilele furnizate în cadrul contractului, în concordanță cu planul de lucru propus și cu oferta financiară. Plata este condiționată de semnarea proceselor-verbale de recepție a serviciilor/produselor și de emiterea proceselor verbale de acceptanță provizorie (parțială).

Modalitatea de plată și termenele aferente sunt prevăzute în Contract, anexă la prezenta documentație.

Autoritatea contractantă va considera serviciile din cadrul contractului de achiziție finalizate în momentul în care:

- toate cerințele cuprinse în caietul de sarcini au fost îndeplinite, respectiv cele asumate prin propunerea tehnică prezentată ca răspuns la acestea;
- rezultatele au fost aprobate de autoritatea contractantă, pe baza cerințelor incluse în contract.

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.

Fiecare factură va avea menționat numărul contractului, datele de emitere și de scadența ale facturii respective.

13. 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 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 responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant 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 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:

- a) Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
- b) Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
- c) Convenția nr. 29 a OIM privind munca forțată;
- d) Convenția nr. 105 a OIM privind abolirea muncii forțate;
- e) Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
- f) Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
- g) Convenția nr. 100 a OIM privind egalitatea remunerației;
- h) Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;
- i) *Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;*
- j) *Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);*
- k) *Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);*
- l) *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.]*
- m) *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.*
- n) *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:*

13.1. 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).

13.2. 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;
- Ordonanța de urgență a Guvernului nr. 155 / 2020 privind unele măsuri pentru elaborarea Planului național de relansare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență (denumită în continuare OUG nr.155/2020);

- Ordonanța de urgență nr. 124/2021 privind stabilirea cadrului instituțional și financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare și reziliență, precum și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență, respectiv normele metodologice de aplicare a prevederilor Ordonanței de urgență a Guvernului nr. 124/2021, cu modificările ulterioare;
- Legea nr. 190/2018 privind măsurile de aplicare a GDPR;
- Instrucțiunile aplicabile pentru contractele finanțate;
- Legislația aplicabilă în vigoare la data semnării contractului de finanțare;
- Reglementările naționale incidente;
- Alte documente/acte normative relevante pentru acest proiect.

13.3. 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 depune DUAE prin care certifică inclusiv faptul că nu se află în conflict de interese în momentul depunerii ofertei și că va informa Autoritatea Contractantă în cazul în care se va afla la un moment dat în situația de conflict de interese, chiar potențial, în timpul îndeplinirii sarcinilor pentru care a fost contractat.

Se vor include în propunerea tehnică informații despre strategia implementată pentru obținerea asigurării că, în legătură cu activitățile și rezultatele incluse în Contractul ce rezultă din această procedură, apariția și materializarea conflictului de interese este prevenit, prin raportare la clauzele contractuale incluse în acest sens în Documentația de atribuire.

13.4. Confidențialitate

Confidențialitatea 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;
- Dezvoltare și testare

13.5. Drepturi de proprietate intelectuală

Toate documentele ce vor fi elaborate în executarea Contractului (Livrabile, studii, analize, rapoarte, planuri, proceduri, metodologii, materiale de instruire și prezentare 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.

Drepturile patrimoniale de autor asupra soluției tehnice create de către Prestator (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, BENEFICIAR (cf. 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 și completarea 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 tuturor operelor create de către contractant sau membrii asocierii, aferente produsului sau serviciului livrat, se transferă către autoritatea contractantă”*.

Înainte de plata facturii finale, Prestatorul va preda Autorității Contractante codul sursă al aplicației.

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.

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 oferite 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.

14. INFORMAȚII SUPLIMENTARE / ADMINISTRATIVE

Limba de lucru este limba română. Toate livrabilele/rapoartele/documentele Contractului vor fi redactate în limba 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 față 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 criteriilor de calificare și selecție 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.

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**. Planul de lucru reprezintă un element de bază al strategiei ofertantului, arată modul în care acesta își va organiza activitatea, motiv pentru care lipsa sa sau a informațiilor solicitate califică oferta ca fiind neconformă și nu poate face obiectul unor completări ulterioare pe durata evaluării ofertelor.

Nu se acceptă doar trimitere către link-uri, ci și documente atașate ofertei, dacă este cazul.

Ofertantul va prezenta la nivelul propunerii tehnice:

- descrierea arhitecturii soluției propuse cu dispunerea produselor software și a modulelor software personalizate pe mașinile virtuale și descrierea componentelor propuse. Prezentarea arhitecturii se va corela cu cerințele caietului de sarcini. Se va detalia lista licențelor oferite, specificând în clar numele licenței de la producător, ediția, producătorul, cantitatea și unitățile de licențiere specifice producătorului (de ex. „User” sau „Processor Core”), precum și corelarea acestora cu cerințele caietului de sarcini. Arhitectura soluției și Lista licențelor trebuie să cuprindă toate licențele propuse de ofertant, în caz contrar oferta va fi declarată neconformă;
- lista echipamentelor hardware specificând în clar identificatorul unic producător (part-number) asociat fiecărui echipament și componenta, numărul de echipamente oferite pentru fiecare tip de echipament, configurația acestora, precum și corelarea acestora cu cerințele caietului de sarcini.

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 cu semnătură electronică extinsă, bazată pe un certificat calificat, eliberat de un furnizor de servicii de certificare acreditat în condițiile legii.

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.

Ofertantul suportă toate cheltuielile datorate elaborării și prezentării ofertei sale.

Nume și prenume		Funcția	Semnătura
Adrian-Gabriel PANCIU	Întocmit	Expert IT Arhitect de sistem - POAT	Panciu Adrian- Gabriel  Digitally signed by Panciu Adrian-Gabriel Date: 2026.02.06 18:27:14 +02'00'
Valeriu-Florian PĂDUREANU	Întocmit	Expert IT Analist de business - POAT	 AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI Padureanu Valeriu-Florian 2026.02.06 18:25:18 +02'00'