CNAIR

Compania Națională de Administrare a Infrastructurii Rutiere

Sistem de tarifare rutiera

12/16/04.01.2024

Aprobat
DIRECTOR GENERAL
Cristian PISTOL

Propun spre aprobare
DIRECTOR DVIC
Lucian CALMUS

CAIET DE SARCINI
pentru
SERVICII DE DEZVOLTARE ŞI IMPLEMENTARE A SOLUŢIEI INFORMATICE, INCLUSIV FURNIZAREA DE ECHIPAMENTE ŞI SOFTWARE DE BAZĂ
In cadrul proiectului
"SISTEM ELECTRONIC DE TARIFARE RUTIERA"
Lot 1 – Sistem informatic centralizat

Cod CPV – 72200000-7 -Servicii de programare si de consultanță software (Rev.2)
Cod CPV – 30210000-4 - Mașini de procesare a datelor (hardware) (Rev.2)
Cod CPV – 30211300-4 – Platforme informatice
Cod CPV – 48820000-2 - Servere (Rev.2)
Cod CPV – 48900000-7 – Diverse pachete software și sisteme informatice
Cod CPV – 72240000-9 – Servicii de analiză și de programare de sisteme

Cuprins

1 INFORMAȚII GENERALE. OBIECTIVELE PROIECTULUI 6
1.1 INFORMAȚII GENERALE 6
1.2 CADRUL LEGAL 7
1.3 CONTEXTUL ȘI OBIECTIVELE PROIECTULUI 8
1.3.1 Contextul proiectului 8
1.3.2 Obiectivele specifice ale proiectului 8
1.3.3 Colectare Electronică a Tarifului de utilizare a infrastructurii rutiere 9
1.3.4 Unități la Bord 10
1.3.5 Dreptul de proprietate 10
1.3.6 Compatibilitatea cu infrastructura IT a clientului 10
1.3.7 Monitorizarea Traficului 11
2 Termeni si definiții 11
3 Situația Existentă 14
3.1 Diagrama sistemului SIEGMCR 15
3.2 Amenajări specifice echipamente 15
3.3 Componente software 15
3.4 Sisteme de virtualizare 16
3.5 Sisteme de automatizare aplicații containerizate 16
3.6 Sisteme de operare 16
3.7 Componente hardware 17
3.8 Licențe perpetue componente software 17
3.9 Volumetrie 18
4 DESCRIEREA TEHNICĂ A PROIECTULUI 19
4.1 PREVEDERI DE SECURITATE 19
4.1.1 Prevederi generale de Securitate 19
4.1.2 Nivelurile de asigurare a încrederii prin mijloace de autentificare 21
4.2 ARHITECTURA TEHNICĂ ȘI FUNCȚIONALĂ 22
4.2.1 Arhitectura funcțională 22
4.2.2 Module necesare realizării sistemului informatic 26
4.2.3 Arhitectura tehnică 35

4.3 CERINȚE TEHNICE PENTRU COMPONENTELE SOFTWARE DE BAZĂ 43

4.3.1 Componenta portal 43

4.3.2 Componenta server de aplicații 48

4.3.3 Componenta server web 49

4.3.4 Componenta de baze de date relationale 49

4.3.5 Componenta de replicare date baze de date relaționale 53

4.3.6 Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics) 55

4.3.7 Componenta Platforma de gestiune fluxuri de date (streaming engine) 57

4.3.8 Componenta de integrare și gateway pentru servicii web 58

4.3.9 Componenta Big Data 61

4.3.10 Componenta de analiză și prognoză 64

4.3.11 Componenta GIS 68

4.3.12 Stocare centralizata profile utilizatori 71

4.3.13 Componenta de gestiune acces utilizatori 72

4.3.14 Componenta de virtualizare și containerizare 73

4.3.15 Componenta de disaster recovery 75

4.3.16 Componenta de analiză și detecție atacuri cibernetice 76

4.3.17 Componenta SIEM 80

4.3.18 Componenta PKI 84

4.3.19 Componenta de monitorizare infrastructură și aplicații 86

4.4 CERINȚE TEHNICE PENTRU COMPONENTELE HARDWARE CENTRALE 87

4.4.1 Echipament server tip 1 87

4.4.2 Echipament server tip 2 98

4.4.3 Echipament stocare tip 1 105

4.4.4 Echipament stocare tip 2 113

4.4.5 Echipament stocare tip 3 120

4.4.6 Switch Distributie 124

4.4.7 Firewall border 126

4.4.8 Switch LAN tip 1 SPINE (2 per site) 131

4.4.9 *Switch LAN tip 2* LEAF 136

4.4.10 Switch LAN tip 3 - MGMT 140
4.4.11 SWITCH Border Gateway(2 per site) 144
4.4.12 Load Balancer 149
4.4.13 Soluție de backup 160
4.4.14 HSM 166
4.4.15 Rack și accesorii 168
4.5 CERINȚE FUNCȚIONALE 169
4.5.1 Funcționalități Modul Nucleu central (core system) 169
4.5.2 Funcționalități modul contravenții 171
4.5.3 Funcționalități servicii web pentru colectare date de la operatorii SETRE 172
4.5.4 Funcționalități servicii web pentru emitere roviniete si peaj 172
4.5.5 Funcționalități aplicație mobila pentru înregistrare si transmitere date privind traseul parcurs de un autovehicul 172
4.5.6 Funcționalități servicii web pentru achiziție roviniete , peaj si mod pre-paid distanta parcursa 173
4.5.7 Managementul utilizatorilor și accesul la sistem 173
4.5.8 Integrarea cu alte sisteme externe 174
4.6 CERINȚE NON-FUNCȚIONALE 174
5 ETAPELE DE IMPLEMENTARE 175
5.1 ANALIZA ȘI PROIECTAREA 175
5.2 DEZVOLTAREA 176
5.3 IMPLEMENTAREA 177
5.4 TESTAREA ȘI ASIGURAREA CALITĂȚII 177
5.5 MIGRAREA DATELOR ISTORICE 178
5.6 PUNEREA ÎN PRODUCȚIE 178
5.7 GRAFICUL DE IMPLEMENTARE 178
6 INSTRUIRE 180
7 DURATA DE EXECUTIE 181
8 GARANȚIA 181
9 METODOLOGIA ȘI PLANUL DE LUCRU 186
9.1 METODOLOGIA 186
9.2 PLANUL DE LUCRU 187

9.3 ORGANIZAREA ŞI PERSONALUL 187
9.3.1 Cerințe privind experții 188
9.3.2 Experții cheie 189
9.3.3 Experții non-cheie 192
10 MANAGEMENTUL CONTRACTULUI 196
10.1 ASPECTE ORGANIZATORICE 196
10.2 FACILITĂȚI OFERITE DE PRESTATOR 197
10.3 METODOLOGIE DE LUCRU ŞI RAPORTARE 198
10.3.1 Metodologia de lucru 198
10.3.2 Cerințe privind raportarea 199
10.3.3 Transmiterea și aprobarea rapoartelor 200
10.3.4 Indicatori de performanță 200
10.4 CONFLICTUL DE INTERESE 201
10.5 DREPTURI DE PROPRIETATE INTELECTUALĂ 202
11 ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI 202
11.1 CONȚINUTUL PROPUNERII TEHNICE 202
11.2 PROPUNEREA FINANCIARĂ 205
12 MODALITĂȚI ŞI CONDIȚII DE PLATĂ 206
13 IPOTEZE ŞI RISCURI 207
13.1 RISCURILE 207
13.2 IPOTEZELE 211
14 ALTE MENȚIUNI 211

1 INFORMAŢII GENERALE. OBIECTIVELE PROIECTULUI

1.1 INFORMAŢII GENERALE

Autoritatea Contractantă este Compania Naţionala de Administrare a Infrastructurii Rutiere (denumita in continuare CNAIR).

Prezentele specificaţii tehnice conţin indicaţiile tehnice minime şi obligatorii care trebuie respectate astfel încât potenţialii ofertanţi să elaboreze propunerea tehnică corespunzător cu necesităţile proiectului.

Caietul de sarcini face parte integrantă din Documentaţia de atribuire pentru achiziţia de servicii de dezvoltare şi implementare a soluţiei informatice, inclusiv furnizarea de echipamente şi software de bază şi constituie ansamblul cerinţelor minime obligatorii pe baza cărora se elaborează Propunerea Tehnică de către fiecare Ofertant.

Cerinţele impuse vor fi considerate ca fiind minime şi obligatorii. în acest sens, orice Propunere Tehnică prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare doar în măsura în care presupune asigurarea unui nivel calitativ superior cerinţelor minime din prezentul Caiet de sarcini. Propunerea Tehnică ce conţine caracteristici inferioare celor prevăzute în Caietul de sarcini va fi considerată neconformă şi va fi respinsă.

Prezentul caiet de sarcini cuprinde regulile de bază care trebuie respectate astfel încât potenţialii ofertanţi să elaboreze propunerea tehnică corespunzător cu necesităţile autorităţii contractante.

Specificaţiile tehnice care indică o anumită origine, sursă, producţie, un produs special, o marcă de fabricaţie sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie sunt menţionate doar pentru identificarea cu uşurinţă a tipului de produs şi nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau anumitor produse. Aceste specificaţii vor fi considerate ca având menţiunea "sau echivalent".

Fără a aduce atingere altor prevederi legale sau dispoziţiilor legale privind liberul acces la informaţiile de interes public ori ale altor acte normative care reglementează activitatea autorităţii contractante, autoritatea contractantă are obligaţia de a nu dezvălui informaţiile din propunerea tehnică, elementele din propunerea financiară şi/sau fundamentări/justificări de preţ/cost transmise de operatorii economici indicate şi dovedite de aceştia ca fiind confidenţiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Caracterul confidenţial se aplică doar asupra datelor/informaţiilor indicate şi dovedite ca fiind date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală.

Operatorii economici vor indica şi dovedi în cuprinsul ofertei care informaţii din propunerea tehnică, elemente din propunerea financiară şi/sau fundamentări/justificări de preţ/cost sunt confidenţiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Informaţiile indicate de operatorii economici din propunerea tehnică, elemente din propunerea financiară şi/sau fundamentări/justificări de preţ/cost ca fiind confidenţiale

trebuie să fie însoțite de dovada care le conferă caracterul de confidențialitate, dovadă ce devine anexă la ofertă.

1.2 CADRUL LEGAL

Prestatorul va desfășura activitățile, realiza și furniza documentele/lucrările specifice Contractului având în vedere toate prevederile legale naționale, europene și internaționale relevante existente la momentul semnării Contractului, precum și cele emise ulterior, pe parcursul derulării Contractului, precum și ansamblul reglementărilor subsecvente, al recomandărilor și practicilor incidente în materie de taxare rutiera, enumerarea următoare nefiind limitativă:

Nr.Crt	Document
1	DIRECTIVA (UE) 2019/520 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 19 martie 2019 privind interoperabilitatea sistemelor de taxare rutieră electronică și facilitarea schimbului transfrontalier de informații cu privire la neplata taxelor rutiere în cadrul Uniunii, cu modificările si completările ulterioare
2	Regulamentul delegat (UE) nr. 203/2020 al Comisiei din 28 noiembrie 2019 privind clasificarea vehiculelor, obligațiile utilizatorilor serviciului european de tarifare rutieră electronică, cerințele privind elementele constitutive de interoperabilitate și criteriile minime de eligibilitate pentru organismele notificate si ale Regulamentului delegat (UE) nr. 204/2020 al Comisiei din 28 noiembrie 2019 privind obligațiile detaliate ale furnizorilor serviciului european de tarifare rutieră electronică, conținutul minim al declarației privind domeniul serviciului european de tarifare rutieră electronică, interfețele electronice și cerințele pentru elementele constitutive de interoperabilitate și de abrogare a Deciziei 2009/750/CE
3	Regulamentul de punere în aplicare (UE) 2020/204 privind obligațiile detaliate ale furnizorilor serviciului european de taxare rutieră electronică, conținutul minim al declarației privind domeniul serviciului european de taxare rutieră electronică, interfețele electronice și cerințele pentru elementele constitutive de interoperabilitate și de abrogare a Deciziei 2009/750/CE
4	Directiva 1999/62/CE din 17 iunie 1999 de aplicare a taxelor la vehiculele grele de marfă pentru utilizarea anumitor infrastructuri, cu modificările si completările ulterioare
5	OG 8/2022 privind interoperabilitatea sistemelor de tarifare rutieră electronică și facilitarea schimbului transfrontalier de informații cu privire la neplata tarifelor rutiere, cu modificările si completările ulterioare
6	OG nr. 15 /2002 privind aplicarea tarifului de utilizare si a tarifului de trecere pe reteaua de drumuri naționale din Romania, cu modificările si completările ulterioare
7	Strategia de Securitate Cibernetica a României

8	OUG nr. 84/2003 pentru înființarea Companiei Naționale de Autostrăzi și Drumuri Naționale din România - S.A. prin reorganizarea Regiei Autonome "Administrația Națională a Drumurilor din România", cu modificările si completările ulterioare;
9	Ordinul SGG – MTI nr. 378/362/2022 pentru aprobarea Procedurii de înregistrare în România a furnizorilor Serviciului european de taxare rutieră electronică
10	OMT nr. 1836/2018 pentru aprobarea unor tarife aplicate de Compania Națională de Administrare a Infrastructurii Rutiere - S.A., cu modificarile si completarile ulterioare;
11	ETSI TS 103 900 V2.0.0 (2022-07) - Intelligent Transportation System (ITS); Vehicular Communications; Basic Set of Applications; Specification of Cooperative Awareness Basic Service;
12	ETSI TS 103 899 V2.0.0 (2022-07) - Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition;
13	ETSI TR 103 576-2 - Intelligent Transport Systems (ITS); Pre-standardization study on ITS architecture; Interoperability among heterogeneous ITS systems and backward compatibility

1.3 CONTEXTUL ȘI OBIECTIVELE PROIECTULUI

1.3.1 Contextul proiectului

Compania Națională de Administrare a Infrastructurii Rutiere – S.A. ca entitate desemnată prin Ordonanța de Urgenta nr. 8/2022 să perceapă tariful rutier în cadrul domeniilor SETRE ce vor fi stabilite pe drumurile de interes național, așa cum sunt prevăzute în Ordonanța Guvernului nr. 43/1997 privind regimul drumurilor, republicată, cu modificările și completările ulterioare, dorește definirea si construcția unui nou sistem informatic integrat având ca scop managementul, gestiunea si controlul tarifului de utilizare a infrastructurii rutiere (pe baza de timp – tip vinieta), cat si pe baza distantei parcurse.

1.3.2 Obiectivele specifice ale proiectului

Având la baza obligativitatea implementării directivei UE 520/2019, Romania, ca si stat membru al UE, trebuie sa își alinieze sistemul de tarifare rutiera in concordanta cu aceasta, scopul fiind in final o mai buna interoperabilitate intre state in direcția transportului rutier. Astfel, noul sistem de tarifare va îngloba atât un mod de tarifare având la baza perioada de utilizare a infrastructurii rutiere (time based) pentru autoturisme, autobuze, autocare si autovehiculele de transport marfa cu masa

totala maxima autorizata (MTMA) ≤ 3,5 tone cat si un mod de tarifare in funcție de distanta parcursa (distance based) pentru autovehiculele de transport marfa cu MTMA> 3,5 tone. Totodată, in cazul autoturismelor, autobuzelor, autocarelor si autovehiculelor de transport marfa cu (MTMA) ≤ 3,5 tone se va aplica si un tarif de trecere (peaj) pentru utilizarea podurilor, tunelurilor si trecătorilor de munte

Noul sistem centralizat de tarifare rutiera va include astfel **funcționalitățile existente** pentru autovehiculele de pana la 3,5 tone inclusiv **migrarea datelor** existente din prezentul sistem centralizat numit Sistem Integrat de Emitere, Gestiune, Monitorizare si Control al Rovinietei - SIEGMCR si va conține si **funcționalitățile specifice** pentru colectarea tarifului de trecere a infrastructurii rutiere pentru autovehiculele cu masa totala de peste 3,5 tone.

Obiectivele specifice sunt:

- **Livrarea de echipamente hardware in 2 centre de date**
- **Instalarea si configurarea echipamentelor hardware in ambele centre de date**
- **Livrarea de componente software**
- **Instalarea componentelor software in ambele centre de date**
- **Analiza, proiectare si dezvoltarea de module software specifice proiectului**
- **Migrarea datelor din vechiul sistem de tarifare pe noul sistem de tarifare**
- **Suport tehnic cu durata de 5 ani pentru toate componentele sistemului**

1.3.3 Colectare Electronică a Tarifului de utilizare a infrastructurii rutiere

Colectarea electronică a tarifului de utilizare a infrastructurii rutiere înseamnă colectarea electronică a tarifului de utilizare relevant stabilit pe baza datelor obținute de la **Unitatea de bord** instalată în vehicul. Plata în sine a tarifului perceput electronic se poate face în numerar, prin transfer bancar sau carduri de plată. Colectarea electronică a tarifului de utilizare se referă la utilizarea generală a Secțiunilor de drum delimitate de către autovehiculele cu o greutate mai mare de 3,5 tone.

Valoarea tarifului de utilizare este calculat ca produsul dintre lungimea distantei parcurse și rata tarifului în euro/km. Tarifele variază în funcție de categoria vehiculului, greutatea totală, numărul de osii și clasa de emisii ale vehiculului și categoria de drum și pot fi, de asemenea, diferențiate în funcție de timp.

În viitor, se pot aplica tarife de utilizare cu mai multe componente, defalcate în tarif de utilizare de infrastructură, costuri de taxe de trafic și taxe de zgomot din trafic. Soluția tehnică trebuie să fie pe deplin pregătită și testată pentru implementarea tarifelor cu mai multe componente.

Distanta parcursă este determinată prin intermediul OBU-urilor, a căror utilizare în vehicul este obligatorie. OBU-urile sunt netransferabile. Obligația de a utiliza OBU nu se aplică vehiculelor scutite de plata taxei conform legislației in vigoare.

În viitor, diferiți algoritmi pot fi utilizați pentru a determina valoarea tarifului de drum parcurs pentru tronsoane diferite. Soluția tehnică a sistemului de tarifare rutiera trebuie să fie complet pregătită și testată pentru a implementa mai mulți algoritmi de determinare a tarifului de utilizare a drumurilor.

Plata tarifului de utilizare se efectuează în Modul Preplătit Taxă și în Modul Post-Taxare.

Soluția tehnică a sistemului de tarifare rutiera trebuie să asigure prelucrarea continuă a datelor de poziție a vehiculelor din OBU pe toate autostrăzile, drumurile naționale de pe teritoriul României. Sistemul de Tarifare Rutiera este o infrastructura de interes național (ICIN) în sensul Legii privind Securitatea Națională.

1.3.4 Unităţi la Bord

Unitățile de bord, serviciile de logistica OBU și Operarea OBU sunt furnizate de către client însuși sau prin terți. **Unitățile de bord nu fac obiectul contractului**. O parte a soluției tehnice a Sistemului de Tarifare Rutiera și obiectul contractului este interfața de comunicație pentru interconectarea on-line a infrastructurii pentru operarea OBU (așa-numitul OBU-proxy) și Sistemul de Tarifare Rutiera precum și integrarea lor în sistem.

În condițiile României, se aplică conceptul de poziție dominantă a Administratorului de Colectare Tarif de utilizare a infrastructurii rutiere, în care evaluarea tranzacțiilor cu taxă este efectuată exclusiv de către administratorul de colectare tarif de utilizare pe baza datelor de localizare de la OBU transmise de furnizorii de servicii de taxare (inclusiv SETRE) sub formă de declarații de taxare.

1.3.5 Dreptul de proprietate

Sistemul de tarifare electronică și toate componentele sale devin proprietatea CNAIR în momentul preluării acestuia în temeiul contractului. Acele componente ale sistemului de taxare rutiera care vor fi livrate continuu pe durata executării contractului devin proprietatea CNAIR în momentul preluării acestora.

1.3.6 Compatibilitatea cu infrastructura IT a clientului

CNAIR deține si operează un sistem informatic pe platforme software Oracle si sisteme de operare Linux, pentru care si-a creat toate competentele necesare. Clientul plănuiește să continue dezvoltarea acestui sistem în viitor. Este in interesul CNAIR sa folosească personalul si resursele materiale existente in favoarea construcției si funcționarii noului sistem de taxare rutiera, fiind avantajos si din punct de vedere economic prin reutilizarea licențelor perpetue achiziționate. Această prevedere nu poate fi interpretată ca limitând sau excluzând o soluție tehnică care utilizează produsele aflate in portofoliul CNAIR într-o măsură mai mică sau nu le utilizează deloc. **Furnizorul va transmite o descriere a gradului de compatibilitate a soluției tehnice propuse cu produsele software aflate in portofoliul CNAIR ca parte a propunerii de soluție tehnică obligatorie.**

1.3.7 Monitorizarea Traficului

Sarcina secundară a sistemului de taxare rutiera este de a asigura monitorizarea traficului tuturor vehiculelor echipate cu OBU pe rețeaua de autostrăzi și drumuri naționale de pe teritoriul României. Conducătorii de vehicule care fac obiectul plății taxelor pentru utilizarea infrastructurii rutiere vor fi obligați să plaseze în vehicul și să aibă permanent OBU în funcțiune atunci când folosesc rețeaua de autostrăzi și drumuri pe teritoriul României.

Obligația CNAIR este de a asigura colectarea și stocarea permanentă și neîntreruptă a datelor din OBU privind localizarea vehiculelor în baza de date proprie și de a pune datele la dispoziția clienților desemnați în scopul controlului și managementului traficului.

2 Termeni si definiții

În sensul acestui document, se aplică termenii și definițiile date în directiva UE 520/2019 precum si cele din standardele ISO/IEC 7498-1:1994, ISO/IEC 10746-2, ISO/IEC 10746-3, ISO 14813-5 și ISO/IEC 15414. ISO și IEC mențin baze de date terminologice pentru utilizare în standardizare la următoarele adrese:

— Platformă de navigare online ISO: disponibilă la https://www.iso.org/obp
— IEC Electropedia: disponibil la http://www.electropedia.org/

SETRE
Serviciul European de Taxare Rutieră Electronică-
Serviciul de tarifare rutieră pus de către un furnizor SETRE la dispoziția unui utilizator SETRE în temeiul unui contract unic în cadrul unuia sau mai multor domenii SETRE
Furnizor SETRE
Furnizor de servicii de tarifare rutieră care, în temeiul unui contract unic, acordă acces la SETRE unui utilizator SETRE, încasează și virează tarifele rutiere către entitățile care le percep, și care este înregistrat în statul membru al Uniunii Europene în care este stabilit;
ALPR
Recunoaștere automată a plăcuței de înmatriculare tehnologie care utilizează recunoașterea optică a caracterelor pe imagini pentru a citi plăcuțele de înmatriculare ale vehiculelor
ITS
Un sistem de transport inteligent (ITS) este o aplicație avansată care își propune să ofere servicii inovatoare legate de diferite moduri de transport și de gestionare a traficului și să permită utilizatorilor să fie mai bine informați și să facă o utilizare mai sigură, mai coordonată și „mai inteligentă" a rețelelor de transport.
DSRC

Comunicația dedicată pe distanță scurtă (DSRC) este o tehnologie de comunicație fără fir concepută pentru a permite automobilelor din sistemul de transport inteligent (ITS) să comunice cu alte automobile sau cu tehnologia infrastructurii. Tehnologia DSRC operează pe banda de 5,9 GHz a spectrului de frecvență radio și este eficientă pe distanțe scurte până la medii.

OBE

Set complet de componente hardware şi software, parte a serviciului de tarifare rutieră electronică, încorporat, instalat sau transportat ca dispozitiv separat la bordul unui vehicul în scopul colectării, stocării, prelucrării, primirii și transmiterii la distanță a datelor

OBU

Unitate de bord (OBU). O unitate de bord este un dispozitiv electronic care este montat în mod normal în sau pe un vehicul sau care, în unele cazuri, poate fi o unitate portabilă. Un OBU poate fi operațional în timp ce un vehicul sau o persoană este mobilă sau staționară. OBU-urile primesc și furnizează date pe unul sau mai multe canale de radiofrecvență (RF). Cu excepția cazurilor în care este exclus în mod specific, operarea OBU este permisă oriunde este permisă funcționarea vehiculului sau trecerea omului.

Artefact

Obiect fizic de material sau informație fizică sau un sistem sau subsistem care este utilizat într-un sistem ITS

Detalii de facturare

Informațiile necesare pentru a determina sau a verifica suma datorată pentru utilizarea unui anumit serviciu

Date de context

Informații definite de perceptorul responsabil de taxă, necesare pentru a stabili taxa datorată pentru circulația unui vehicul pe un anumit domeniu de taxare și pentru a încheia tranzacția de taxare

Colectarea electronică a tarifelor

Perceperea tarifelor prin mijloace electronice

Nota 1 la intrare: Plata efectivă (încasarea taxei) poate avea loc în afara sistemului de tarifare.

Executare

Măsuri sau acțiuni întreprinse pentru a atinge respectarea legilor, reglementărilor sau regulilor

Nota 1 la intrare: În acest context: procesul de respectare obligatorie a unui regim de tarifare.

Interoperabilitate

Capacitatea sistemelor de a face schimb de informații și de a utiliza reciproc informațiile care au fost schimbate

EXEMPLU:

Interoperabilitatea taxării urmărește să permită unui vehicul să circule prin diferite domenii de taxare, având în același timp un singur OBE care operează în baza unui contract cu un furnizor de servicii de taxare.

Echipament de bord

Toate echipamentele necesare la bordul unui vehicul pentru efectuarea funcțiilor de colectare electronică a taxelor (EFC) și a serviciilor de comunicații necesare

Echipamente pe marginea drumului

Echipamente amplasate de-a lungul drumului, fie fixe, fie mobile

Rol

Set de responsabilități

Schema tarifară

Set de reguli pentru a determina tariful datorat pentru un vehicul dintr-un domeniu de tarifare

Tarif

Suma percepută în legătură cu utilizarea unui vehicul într-un domeniu de tarifare

Toll Charger

Entitate care percepe tariful rutier - entitate de drept public sau privat care percepe un tarif rutier pentru circulația vehiculelor într-un domeniu SETRE;

Entitate desemnată să perceapă tariful rutier - entitate de drept public sau privat care este desemnată drept entitate care percepe tariful rutier în cadrul unui viitor domeniu SETRE;

Domeniul de tarifare (Toll domain)

Zonă sau parte a unei rețele rutiere în care se aplică un anumit regim de tarifare

Regim de tarifare (Toll regime)

Set de reguli, inclusiv norme de aplicare, care reglementează colectarea unui tarif de trecere într-un domeniu de tarifare

Schema de tarifare (Toll Scheme)

Viziunea organizatorică a unui regim de taxare, inclusiv actorii și relațiile acestora

Serviciu de tarifare (Toll Service)

Serviciu care permite unui utilizator ca, în baza unui contract unic, să utilizeze un vehicul într-unul sau mai multe domenii de tarifare

Furnizor de servicii de tarifare (Toll Service Provider)

Entitate care pune la dispoziția unui utilizator serviciul de tarifare rutieră în cadrul unuia sau mai multor domenii de tarifare, pentru una sau mai multe clase de vehicule

Serviciu de transport

Serviciu legat de infrastructura de transport care este oferit utilizatorului

Obiect de încredere (trust object)

Obiect informațional care este schimbat între entități pentru a asigura încrederea reciprocă

EXEMPLU:

Semnătura electronică sau un certificat electronic.

3 Situația Existentă

Compania Națională de Infrastructura Rutiera a implementat in anul 2010 un sistem centralizat integrat pentru emiterea si gestiunea rovinietei (forma de plata a taxei de utilizare a infrastructurii rutiere). Sistemul a fost construit având 2 marii arii de funcționare:

- Emiterea rovinietelor prin parteneri si canale diverse
- Controlul plații tarifului de utilizare a infrastructurii rutiere pentru autovehicule ce o utilizează.

Conform legislației actuale, tariful de utilizare a infrastructurii rutiere colectat de către CNAIR in calitate de administrator se aplica numai pe infrastructura de tip autostrada, drum European si drum național

In anul 2015, CNAIR a introdus si primul obiectiv de tip PEAJ (tarif de trecere obiectiv) pentru podul de la Cernavoda. Astfel , acest tip de tarif a fost înglobat in actualul sistem informatic centralizat numit SIEGMCR.

In anul 2020, CNAIR a operat un upgrade al sistemului SIEGMCR atât in partea hardware prin achiziția de hardware nou, precum si upgrade-ul componentelor software, atât cele de tip COTS cat si a celor dezvoltate particular (custom).

Din punct de vedere arhitectural, sistemul SIEGMCR este prezentat in diagrama de mai jos

3.1 Diagrama sistemului SIEGMCR

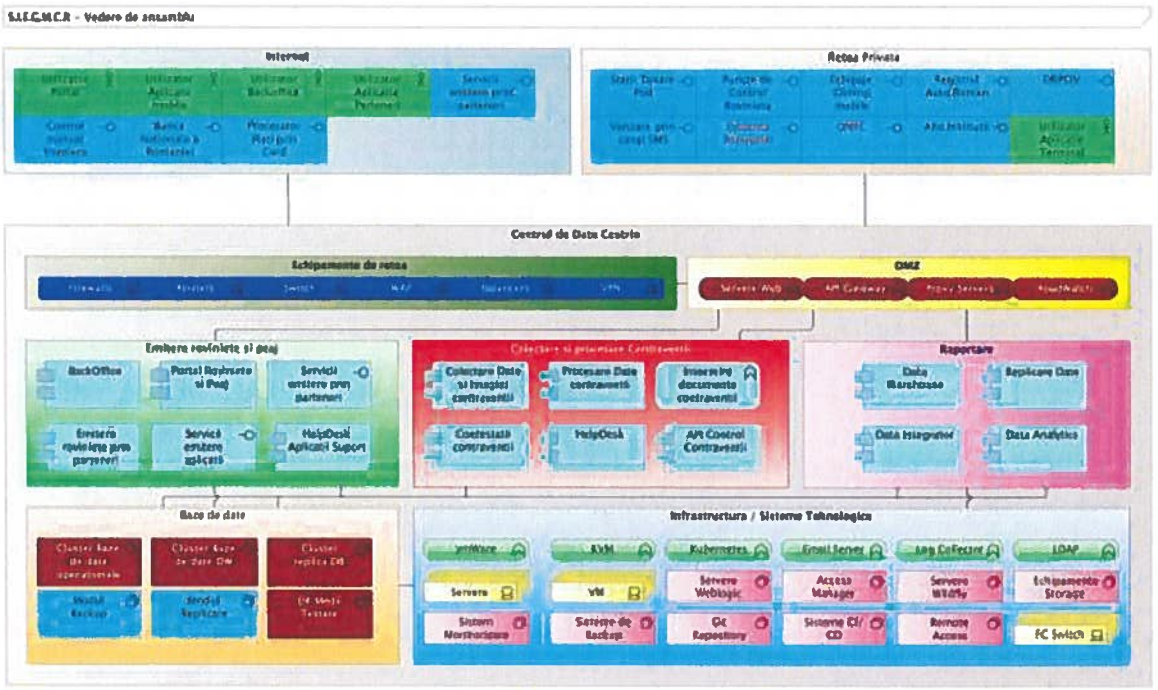


Figura 1 Diagrama sistemului actual "SIEGMCR"

Descrierea modulelor componente ale actualului sistem de tarifare electronica a utilizarii infrastructurii rutiere

3.2 Amenajări specifice echipamente

- Data Center in locația Cestrin
- Locații de control in număr de 110 – dotate corespunzător scopului de colectare si procesare imagini

3.3 Componente software

- modul backoffice (nucleu central) cu următoarele funcționalități:
  - Gestiune nomenclatoare
  - Gestiune parteneri si puncte de lucru
  - Expunere servicii web generice pentru roviniete si peaj
  - Gestiune job-uri programate

  - Gestiune si planificare echipaje de control
  - Gestiune financiara
  - Gestiune categorii auto si a taxei aferente
- Portal emitere roviniete si peaj
- Aplicație mobila pentru achiziție roviniete si peaj
- Aplicație web emitere roviniete pentru parteneri
- Aplicație web pentru colectarea datelor de la punctele de control roviniete si peaj
- Aplicație web pentru prelucrarea datelor legate de contravenții si întocmirea actelor de contravenție
- Servicii de control roviniete si peaj
- Aplicație web pentru gestiunea si operarea punctului de control PEAJ
- Modul de tip data-warehouse
- Modul de raportare
- Modul replicare baze de date
- Modul de captura si procesare imagini la punctele de control
- Modul de transmitere imagini pentru vehiculele depistate fara plata rovinieta catre centrul de date
- API Gateway
- Access management
- Data Integrator
- Data replication
- Modul de tip Business Intelligence
- Clustere de baze de date Oracle
- Modul de backup – mașini virtuale, containere si baze de date
- Servere Email
- Servere DNS
- Servere de timp
- Module specializate pentru persistenta codului sursa si a proceselor de tip CI/CD
- Modul de tip issue management / project management
- Mașini virtuale in număr de 94 (inclusiv medii de testare)

3.4 Sisteme de virtualizare

- vmWare
- KVM

3.5 Sisteme de automatizare aplicații containerizate

- Kubernetes Clusters

3.6 Sisteme de operare

- Oracle Linux
- Redhat Linux
- AlmaLinux
- Ubuntu

3.7 Componente hardware

- Echipamente de tip Server – 28 de bucăți cu procesoare tip x86 aflate in datacenter-ul din locația CESTRIN
- Echipamente de tip server pentru locațiile de control – Servere AxiomTek specializate pentru amplasare in locații cu ambient non-standard tip datacenter – funcție de mărimea locației de control de la 1,2 bucăți la 6
- Camere de luat vederi pentru locațiile de control – Model ARH
- Echipamente de tip storage – 3 bucăți cu spațiul total de stocare de aproximativ 200Tb
- Echipamente de comunicații
  - Switch-uri
  - IPS
  - Balansoare (WAF , Balancers)
  - Firewall
- **Switch-uri de fibra optica**

3.8 Licențe perpetue componente software

Licențe produse de tip COTS

Nr. Crt.	Nume produs	Cantitate	Mod licentiere
1	Oracle Partitioning	24	CPU
2	Oracle Web Tier	8	CPU
3	Oracle Real Application Clusters	24	CPU
4	Oracle Diagnostics Pack	24	CPU
5	Oracle Database Enterprise Edition	24	CPU
6	Oracle Tuning Pack	24	CPU
7	Oracle WebLogic Suite	16	CPU
8	Oracle SOA Suite for Oracle Middleware	16	CPU
9	Oracle Data Integrator Enterprise Edition	8	CPU
10	Oracle Directory Services	4	CPU
11	Oracle Weblogic Suite	40	NUP
12	Oracle Data Integrator Enterprise Edition	50	NUP
13	Oracle SOA Suite for Oracle Middleware	40	NUP
14	Oracle Tuning Pack	50	NUP
15	Oracle Diagnostics Pack	50	NUP
16	Oracle Partitioning	50	NUP
17	Oracle Web Tier	20	NUP

Nr. Crt.	Nume produs	Cantitate	Mod licentiere
18	Oracle Database Enterprise Edition	50	NUP
19	Oracle Business Intelligence Suite Enterprise Edition Plus	55	NUP
20	Oracle Identity and Access Management Suite Plus	300	EMU
21	Oracle Goldengate for Oracle Database	24	CPU
22	Oracle Secure Backup	1	STREAM
23	vmWare ESXI	22	SOCKET
24	vmWare vCenter	1	SITE
25	Subscriptie Oracle Linux Premier Limited	6	Server
26	Subscriptie Oracle Linux Premier support	4	Server
27	Subscriptie Red Hat Enterprise Linux Server, Standard (Physical or Virtual Nodes) (L3 Only)	26	Socket x 2

Nota: Licențele prezentate sunt perpetue si au achiziționate serviciile de suport la zi, cu excepția pozitiilor marcate ca si subscripție

Pentru produsele software dezvoltate personalizat, CNAIR deține dreptul de proprietate intelectuala pentru modulele aferente tarifului de trecere pod. Pentru modulele centrale, servicii emitere rovinieta si control roviniete, dreptul de proprietate intelectuala nu aparține CNAIR.

3.9 Volumetrie

Din punct de vedere volumetrie date, sunt de interes următoarele informații:

- Volumul de storage agregat este de 5Gb/zi
- Traficul din zona internet este de aproximativ 30Mb/s
- Traficul din zona private este de aproximativ 25MB/s
- Volumul de backup este aproximativ de 1,6 TB per săptămâna doar pentru bazele de date si de 12 Tb pentru mașinile virtuale pe săptămâna la care se adaugă backup-ul incremental al datelor aferente modulului de contravenții in cantitate de 40 TB

4 DESCRIEREA TEHNICĂ A PROIECTULUI

4.1 PREVEDERI DE SECURITATE

4.1.1 Prevederi generale de Securitate

În scopul protejării datelor gestionate prin sistemul informatic, se va avea în vedere furnizarea unei soluții care să asigure confidențialitatea, integritatea și disponibilitatea datelor.
Protecția datelor va începe din momentul introducerii informațiilor în sistem și va fi asigurată prin definirea și documentarea nivelurilor de protecție și luarea deciziilor de control al accesului.
Formularea cerințelor de securitate are drept scop definirea cadrului general de securitate prin care să se asigure confidențialitatea, integritatea și disponibilitatea informațiilor stocate, procesate sau transmise prin sistemele de comunicații și informatice, destinate operaționalizării sistemului.
Arhitectura sistemului trebuie să respecte reglementările legale privind protecția datelor cu caracter personal ca și principiu de baza. În acest sens, securitatea datelor prelucrate de sistemul informatic, inclusiv din punct de vedere al comunicațiilor, dintre entitățile participante în sistem trebuie să fie conformă normelor legale.

Sistemul informatic trebuie să asigure mecanisme de protecție împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le gestionează. Soluția de securitate trebuie să asigure securitatea și confidențialitatea datelor cu caracter personal ale cetățenilor existente în bazele de date. Astfel, utilizatorii vor putea accesa numai acele secțiuni și acel conținut care le sunt permise prin apartenența la un profil sau la o macheta de securitate.
Soluția de securitate va fi configurată astfel încât:

- să nu permită persoanelor neautorizate să introducă sau să altereze informațiile din sistem;
- să nu permită persoanelor neautorizate să acceseze sistemul;
- să asigure integritatea și autenticitatea datelor și să permită identificarea sursei datelor inițiale și a persoanelor care au accesat sau au înregistrat aceste date în sistem;
- să asigure trasabilitatea acțiunilor utilizatorilor și operațiunilor efectuate în sistem;
- nu va exista posibilitatea de acces pentru persoanele dintr-un mediu extern la date dintr-un mediu considerat intern;
- informațiile private care se transmit vor fi criptate pana la livrare, astfel încât să nu poată fi interceptate și utilizate;
- informațiile vor putea fi protejate integral și în permanență pentru acces neautorizat;
- grupurile de utilizatori vor putea fi setate pentru diferite niveluri de acces în sistem;
- sistemul va permite controlul complet al accesului utilizatorilor la aplicații și la baza de date prin înregistrarea orei și datei la care a fost executată fiecare tranzacție, precum și identitatea utilizatorului care a initiat-o;

- vor există facilități de generare parole, precum și stabilire de reguli specifice (lungime de parola, timp de expirare parola, numărul maxim de erori tolerate la introducerea parolei după care utilizatorul este automat blocat);
- va oferi posibilitatea de blocare facilă și selectiva a utilizatorilor;
- va asigura securitatea tuturor interfețelor sistemului informatic provenind accesul utilizatorilor neautorizați la sistem;
- nu va permite utilizatorilor obișnuiți accesul la datele din baza de date decât prin intermediul funcțiilor incluse în sistemul informatic (ecrane dedicate);
- in caz de avarii vor există înregistrate suficiente informații de diagnosticare pentru a ajuta la identificarea și soluționarea problemei.

Accesul la date trebuie să se facă doar prin intermediul serviciilor oferite de componentele informatice, pe baza drepturilor deținute de către utilizatori, accesul direct la datele din tabele nefiind permis. De asemenea, accesul trebuie să fie reglementat prin politicile de securitate, aferente fiecărui tip de utilizator.

Sistemul trebuie să includă mecanisme pentru asigurarea următoarelor servicii de securitate:

- confidențialitatea, care asigura ca datele sunt accesibile, vizibile sau disponibile doar utilizatorilor autorizați atât pentru datele stocate cât și pentru cele care tranzitează sistemul;
- integritatea, care asigura nealterarea datelor sau distrugerea acestora de către o acțiune neautorizata;
- disponibilitatea, asigura ca resursele de informații să fie accesibile și utilizabile la cererea personalului autorizat atunci când le sunt necesare;
- autentificarea, este mecanismul prin care un utilizator demonstrează că este autorizat să utilizeze sistemul;
- nonrepudierea, este un serviciu care nu permite unui utilizator participant la introducerea, modificarea sau manipularea datelor prin sistem să decline faptul ca el a fost inițiatorul unei anumite acțiuni. Semnătura digitala este o soluție tehnica utilizata frecvent pentru realizarea serviciului de nonrepudiere.

Pentru asigurarea serviciilor de securitate descrise mai sus, soluția va trebui să ofere funcționalitatea implementată de semnare electronică și marcare temporală prin utilizarea următoarelor servicii criptografice furnizate de o infrastructură cu chei publice:

- semnarea electronică a documentelor de către fiecare utilizator folosind certificate digitale X.509v3, validarea semnăturii electronice și a validității certificatelor utilizate atât prin metode de tip catalog (CRL, RFC 5280), cât și pe baza protocolului OCSP (RFC 2560) în momentul depunerii acestora;
- apelarea funcțiilor de semnătura digitală de către aplicații sau utilizatori diferiți; certificatele digitale și cheile criptografice vor fi emise nominal pentru utilizatorii sistemului de către o autoritate de certificare desemnata, pe baza datelor de identificare ale acestora;
- va asigura semnarea și marcarea temporala a oricărui format de documente, inclusiv PDF și XML, prin utilizarea infrastructurii de chei publice, soluția trebuie să permită folosirea oricăror certificate

digitale calificate conforme cu regulamentul eIDAS, dar prestatorul nu trebuie să furnizeze aceste certificate;

Pentru asigurarea managementului utilizatorilor și accesului la sistem, se vor avea în vedere următoarele:

- identificarea în mod unic a fiecărui utilizator intern în sistem prin crearea de conturi unice și personalizate de acces;
- gestionarea centralizată și unitară a accesului utilizatorilor în sistem prin autorizarea utilizatorului doar la componentele și modulele funcționale ale sistemului conform cu drepturile de acces și atribuțiile specifice;

Precizăm că în cadrul prezentului proiect prestatorul nu va trebui să livreze certificatele digitale calificate.

4.1.2 Nivelurile de asigurare a încrederii prin mijloace de autentificare

În conformitate cu REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/1502 AL COMISIEI din 8 septembrie 2015 se aplică următoarele precizări și definiții:

1. „sursă sigură" înseamnă orice sursă, indiferent de formă, în privința căreia se poate avea încredere că furnizează date, informații și/sau dovezi exacte care pot fi utilizate pentru dovedirea identității;
2. „factor de autentificare" înseamnă un factor în privința căruia s-a confirmat că are legătură cu o persoană și care se încadrează în una dintre următoarele categorii:
   (a) „factor de autentificare bazat pe posesie" înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze că se afla în posesia acestuia;
   (b) „factor de autentificare bazat pe cunoștințe" înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze cunoașterea informației în cauză;
   (c) „factor de autentificare inerent" înseamnă un factor de autentificare care se bazează pe o caracteristică fizică a unei persoane fizice și în cazul căruia subiectul trebuie să demonstreze că prezintă respectiva caracteristică fizică;
3. „autentificare dinamică" înseamnă un proces electronic care utilizează criptografia sau alte tehnici pentru a oferi un mijloc de a crea, la cerere, o dovadă electronică a faptului că subiectul controlează datele de identificare sau se afla în posesia acestora, dovadă care se modifică la fiecare autentificare a subiectului în sistemul care verifică identitatea subiectului;
4. „sistem de management al securității informațiilor" înseamnă un set de procese și proceduri menite să gestioneze la niveluri acceptabile riscurile legate de securitatea informațiilor.

Sistemul va folosi următoarele niveluri de încredere:

- Nivelul minim pentru administratori și utilizatori interni va fi implementat prin autentificarea cu user și parolă prin aplicațiile de administrare a utilizatorilor (LDAP, IAM, acces securizat).
- Nivel minim pentru utilizatorii externi (persoane fizice și persoane juridice) care vor avea acces la alte informații decât cele publice va fi de nivel substanțial conform regulamentului 910/2014 și a regulamentului de punere în aplicare (UE) 2015/1502 al comisiei din 8 septembrie 2015.

Pentru utilizatorii externi autorizați (persoane fizice și juridice) care vor accesa informații (altele decât cele publice) se va implementa autentificarea folosind doi factori de autentificare, respectiv nume și

parolă și o modalitate suplimentară de tip one-time-password (ex: prin SMS sau e-mail sau folosind o aplicație mobilă).
În procesul de obținere a datelor de acces se va asigura că utilizatorii sunt înscriși atât cu numele și parola dar și cu numărul de telefon mobil și adresa de e-mail.
Pentru înregistrarea utilizatorilor externi va fi creată o pagină dedicată în cadrul interfeței portal extern, prin care utilizatorii își pot completa datele de identificare în pagina web securizată (https).
Prestatorul va trebui să ofere o soluție pentru înregistrarea utilizatorilor externi cu câmpuri predefinite și pentru validarea identității la distanță. Funcționalitatea de înregistrare online a utilizatorilor externi (componenta ghișeu virtual din cadrul portalului extern) trebuie sa fie implementata conform regulamentului 910/2014 și a regulamentului de punere în aplicare (UE) 2015/1502 al comisiei din 8 septembrie 2015.

4.2 ARHITECTURA TEHNICĂ ȘI FUNCȚIONALĂ

4.2.1 Arhitectura funcțională

Sistemul informatic va respecta principiile proiectelor de e-guvernare fiind:
Accesibil, promovând:

- Serviciile electronice oferite vor fi furnizate utilizatorilor folosind interfețe grafice de utilizare intuitive, adaptate tipurilor de utilizatori, permițând accesul unui număr cât mai mare de utilizatori, respectând și oferind funcționalități pentru implementarea standardelor de accesibilitate nivel A,AA a standardului EN 301 549 V2.1.2 (WCAG 2.1), aplicabile secțiunilor/funcționalităților implementate;
- Accesul unui număr cât mai mare de utilizatori prin intermediul:
  - componentei client utilizată de către persoanele fizice și organizațiile implicate în procesul de adopție și a publicului larg;
  - funcționalităților componentelor de business orientate pe fluxuri de lucru și destinate utilizării de către personalul implicat în procesul de adopție;
  - introducerea tehnologiei web în procesul de depunere a petițiilor online, această secțiune putând fi accesată pe portalul web;
- Serviciile electronice oferite vor fi furnizate utilizatorilor folosind interfețe grafice intuitive, adaptate tipurilor de utilizatori și permițând accesul unui număr cât mai mare de utilizatori ;
- Furnizarea serviciilor prin canale alternative, respectiv depunere/urmărire stare petiții de pe stații de lucru și de pe terminale mobile de tipul tabletelor, smartphone-urilor.
- Serviciu de petiții on-line prin intermediul componentei dedicate din portal cu alternativă de depunere în format fizic la ghișeu și înregistrare în sistem de către un operator, și inițierea fluxului de rezolvare a acesteia. De asemenea, răspunsul către solicitant poate fi transmis pe canale electronice (e-mail) sau pe canale clasice.

- O interfață intuitivă, ușor de navigat;
- Suport pentru utilizarea caracterelor specifice limbii române, cu etichete și mesaje în limba română, cu documentație de utilizare online în limba română, cerință care se va reflecta în toate interfețele aplicațiilor realizate;
- Asigurarea calității și consistenței conținutului, prin implementarea unor proceduri de control și validare a informațiilor introduse de utilizatori, cu evitarea redundanțelor prin utilizarea în comun a nomenclatoarelor și cataloagelor și prin controlul actualizării acestora;

Eficient, prin:

- Producerea de economii financiare, prin reducerea costurilor asociate procesului de adopție, reducerea numărului de formulare pre tipărite și înlocuirea lor cu documente electronice generate de sistem, s.a.
- Creșterea productivității muncii angajaților, prin eliminarea operațiunilor redundante în procesul de adopție, reducerea timpilor necesari desfășurării activităților specifice procesului de adopție, reducerea timpilor de generare a rapoartelor, reducerea timpilor de rezolvare a petițiilor, scurtarea timpilor necesari investigării și documentării prin accesibilitatea crescută a informației și introducerea de capabilități puternice de raportare, asigurarea accesului și posibilitatea prelucrării informațiilor la nivelul tuturor utilizatorilor, în baza rolurilor și permisiunilor definite.
- o mai bună organizare, prin optimizarea circuitelor informaționale la nivelul entităților implicate în procesul de adopție;
- o arhitectura scalabila, prin construirea unui nucleu unic de echipamente hardware și de comunicații care permite extinderea capacității și a numărului de utilizatori.
- De asemenea, prin arhitectura TIC propusă se asigură și posibilitatea diseminării informațiilor la distanță, către beneficiarul final, respectiv cetățeanul;
- promovarea serviciilor cu impact ridicat, prin punerea la dispoziție, pentru orice utilizator al serviciilor internet, a unor unelte de publicare și diseminare a informației către oricine își declară dorința de utilizare a sistemului sau posedă autorizația de acces necesară.

Eficace, prin:

- reducerea birocrației facilitată de introducerea mecanismelor de comunicare între cetățeni și instituție;
- creșterea satisfacției utilizatorului, prin creșterea gradului de dispersie a informației și serviciilor electronice implementate pentru cetățeni și pentru personalul implicat în procesul de adopție;
- servicii publice inclusive, prin punerea la dispoziția cetățenilor a unor servicii electronice, ceea ce permite transparența activității instituțiilor implicate.

Democratic, asigurând:

- deschidere, prin publicarea și diseminarea informațiilor de interes public și prin punerea la dispoziție către publicul larg a serviciului de petiții on-line;
- transparență și răspundere, prin integrarea unor funcționalității care reflectă în mod continuu statusul pe fluxurile de lucru și ritmul de rezolvare a sarcinilor;

- participarea cetățeanului, prin disponibilizarea unor servicii de colectare de informații direct de la acesta, prin asigurarea unor servicii de consultare de către cetățeni a informațiilor publice, prin integrarea pentru aceștia a serviciului de petiții on-line;

Inovativ și Neutru Tehnologic, utilizând tehnologii software și hardware de actualitate, care alături de respectarea standardelor moderne de implementare a sistemelor informatice complexe, vor asigura performanța sistemului informatic și vor permite extinderea ulterioară a funcționalităților și arhitecturii sistemului, independent de dezvoltatorul inițial, atât din punct de vedere tehnic, cât și ca licențe și drepturi de proprietate intelectuală.

Colaborativ, Soluția fiind bazată pe o abordare orientată permanent pe schimbul de informații actualizate și sincronizate on-line.

Sigur, prin protejarea confidențialității datelor furnizate de utilizatori și a celor stocate precum și asigurarea procedurilor de securizare a transferurilor de informații folosind servicii de comunicații securizate;

Scalabil, asigurând posibilitatea de extindere atât a funcționalităților sistemului cât și a parametrilor tehnici, pe măsura apariției unor noi cerințe.

Arhitectura modulară a sistemului propus va asigura o disponibilitate ridicată la nivelul componentelor critice și o scalabilitate liniară deopotrivă orizontală și verticală, pentru a acomoda ușor creșterea numărului de utilizatori sau a volumului de operații efectuate de aceștia, prin posibilitatea de suplimentare cu putere de procesare sau memorie, ori respectiv prin adăugarea de servere, în condiții de "înaltă disponibilitate ("high availability") - fără stoparea temporară sau cu opriri minime a serviciilor de producție.

Pachetul de licențe va fi livrat cu toate componentele software necesare pentru a asigura rularea aplicațiilor în bune condiții, fără a fi necesară achiziția de către Beneficiar de produse software/licențe suplimentare, atât pe perioada de derulare a contractului, cat și ulterior finalizării acestuia.

Toate componentele și subcomponentele vor trebui să se regăsească în clar în cadrul ofertei tehnice propuse. Nu facem referire la subscripții software, ci doar la licențe care trebuie să fie un pachet complet și perpetuu.

În cadrul proiectului vor trebui să fie implementate măsuri de securitate care să faciliteze implementarea unor politici de securitate, conform cerințelor noului Regulament General privind Protecția Datelor (GDPR), cel puțin referitoare la:

- Securitate adecvată - protecția împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri tehnice sau organizatorice,
- Protecția datelor cu caracter personal care dezvăluie originea rasială sau etnică, confesiunea religioasă și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice,
- Prelucrarea fotografiilor - fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice,
- Capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare,

- Capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică,
- Un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării,
- caracteristică esențială este conceptul de „data protection by design și by default" în sensul implementării de soluții și măsuri tehnice de securitate adecvate la momentul implementării mijloacelor și modalităților de prelucrare a datelor cu caracter personal.

În cadrul analizei de business vor fi identificate acele colecții de date pentru care vor trebui să fie implementate normele de aplicare GDPR .

Prestatorul soluției va implementa un portal informațional de tip „Enterprise" care va permite integrarea informațiilor, a documentelor, a rolurilor persoanelor și a proceselor, ca punct de acces unic, prin intermediul unei interfețe tip web.

Funcționalitățile principale ale acestor sisteme informatice EIP sunt integrarea și prezentarea. Acestea pot accesa informația din diferite surse și o prelucrează prin portal. Alte funcționalități principale includ:

- Integrare de conținut web;
- Integrare și publicare de fluxuri externe de informații;
- Single Sign On (SSO);
- Controlul și personalizarea accesului;
- Căutare în conținut;
- Prelucrare analitica și Rapoarte Inteligente.

Prestatorul va dezvolta funcționalități personalizate EIP (Enterprise Information Portal), oferind:

- Formulare web pentru captarea datelor și metadatelor actelor și documentelor necesare popularii sistemului (metadate descriptive, structurale, administrative, de conținut și statistice);
- Dezvoltare de „workflow"-uri pentru procedurile de lucru: de aprobare, de avizare, de semnătura, de publicare etc.;
- Configurarea accesului organizațional la arhivele electronice și la datele din sistem;
- Va asigura sesiuni de prezentare și asistență pentru configurarea și administrarea conținutului;
- Dezvoltarea modelului de date pe modelul funcțional al proceselor, unificând modelele de date anterioare;
- Dezvoltarea specificațiilor tehnice de integrare cu sisteme externe prin tehnologii web API REST sau SOAP API și instituții care vor dori să schimbe informații ulterior.

4.2.2 *Module necesare realizării sistemului informatic*

În vederea realizării sistemului informatic de tarifare rutiera se vor avea în vedere următoarele module necesare:

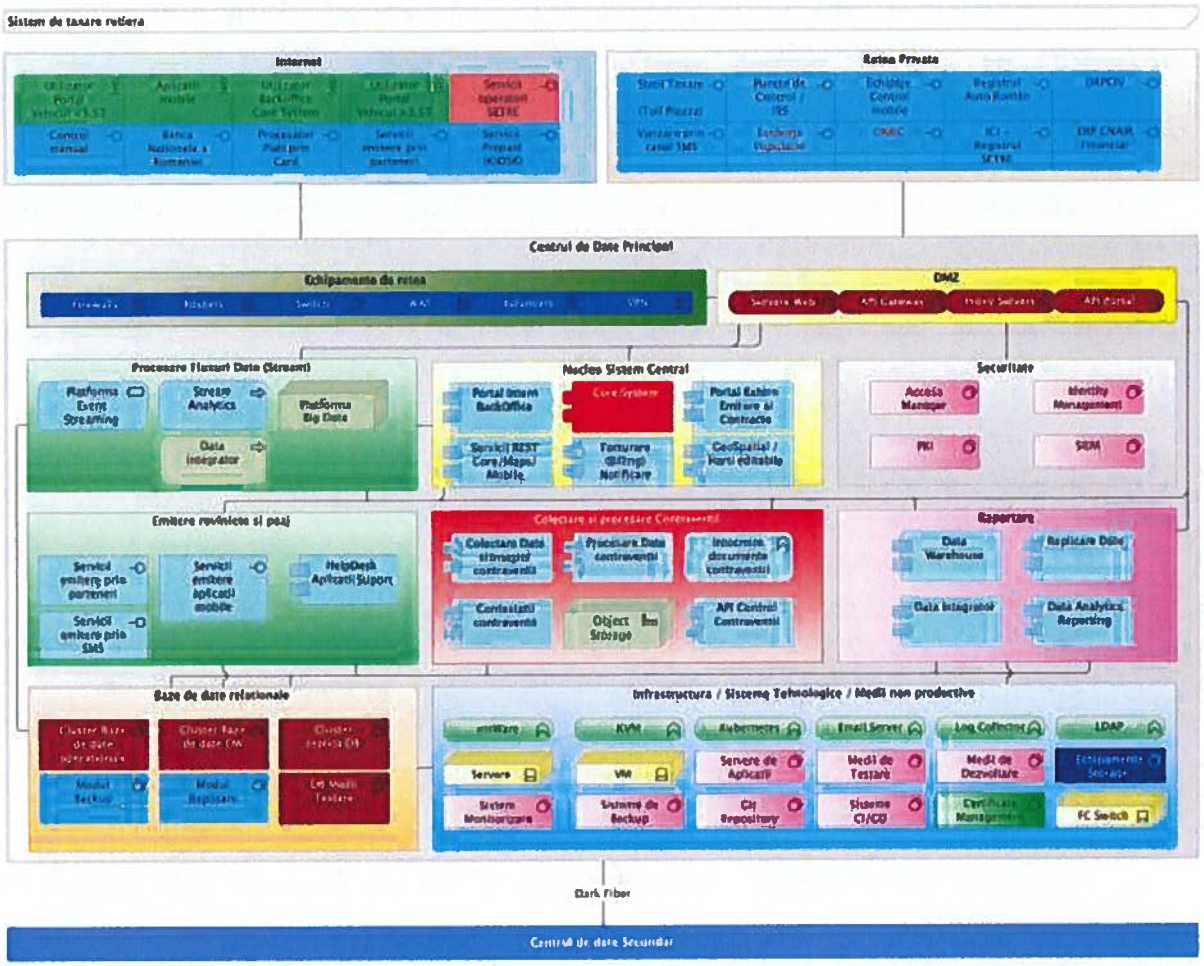


Figura 2 Arhitectura Logica și Componentele Funcționale

Nr.	Modul / componenta software	Funcționalitate
1	Componenta management aplicații containerizate	Grupează containerele care alcătuiesc o aplicație în unități logice pentru o gestionare și o descoperire ușoară
2	Componenta Big Data	Permite înregistrarea datelor privind pozițiile geografice ale autovehiculelor care se încadrează la modul tarifare având la baza distanta parcursa de un autovehicul
3	Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)	- Procesează in timp real datele recepționate de la operatorii SETRE sau aplicație mobile de urmărire traseu parcurs de un autovehicul - Notifica inadvertente legate de mesajele recepționate (exemplu – același număr auto se afla in 2 locuri diferite) - Determina daca datele recepționate pentru autovehicul sunt corecte din punct de vedere operațional (poziție geografica corecta, vehicul înrolat, etc.) - Afișează in timp real poziția pe harta geografica, poziția si mișcarea unui autovehicul
4	Componenta Platforma de gestiune fluxuri de date (streaming engine)	Persista mesajele recepționate de la operatorii SETRE sau aplicația mobile de urmărire traseu in vederea procesării ulterioare prin mecanisme de tip publish / subscribe
5	Componenta Data Integrator	Asigura transpunerea si agregarea datelor din modulul BigData in mod relațional si înregistrarea acestora in bazele de date relaționale.

Nr.	Modul / componenta software	Funcționalitate
		Asigura prelucrarea datelor in zona Data-Warehouse
6	Componenta Nucleu central (core system)	- Gestiune nomenclatoare - Gestiune clienți (persoane fizice si juridice) - Gestiune tarife pentru roviniete , peaj sau tarif per km - Gestiune porți virtuale (virtual gates) pentru segmente de drum - Gestiune parteneri si punct de lucru parteneri - Gestiune scutiri la plata rovinietei sau a tarifului de utilizare a infrastructurii rutiere - Gestiune tarif pre-paid si post-paid tarif de utilizare infrastructura rutiera - Gestiunea emiterilor de roviniete si peaj (inclusiv gestiunea trecerilor efectuate prin obiectivele cu tarif special) - Funcționalități de backoffice
7	Componenta de colectare si procesare contravenții	Oferă servicii pentru colectarea datelor de la punctele de control sau sistemele ITS Persista informațiile recepționate de la punctele de control in sistemele de tip object storage împreuna cu înregistrarea meta datelor aferente in bazele de date relaționale Procesează contravențiile si întocmește documentele de contravenție Oferă servicii web pentru echipajele de control mobile

Nr.	Modul / componenta software	Funcționalitate
		Înregistrează si procesează contestațiile la contravenții
8	Componenta servicii integrare si colectare date de la operatorii SETRE	Servicii specializate pentru înregistrarea datelor recepționate de la operatorii SETRE cu privire la evenimente si date geografice ale autovehiculelor cu MTMA > 3,5 tone
9	Componenta servicii pentru achiziție tarif de utilizare infrastructura in mod pre-paid	Servicii REST pentru integrarea intr-un dispozitiv multifuncțional (KIOSK) a următoarelor funcționalități: - Înrolare autovehicul in sistemul de tarifare a utilizării infrastructurii rutiere - Determinare traseu funcție de tipul autovehiculului , norma de poluare, MTMA si afișarea acestuia in mod harta geografica. Treseul se stabilește având la baza punctele de plecare si de destinație - Plata tarifului prin card bancar
10	Componenta aplicație mobila colectare traseu autovehicul > 3.5 tone	- Aplicație mobila pentru dispozitive mobile de tip smartphone, ANDROID sau IOS, care oferă utilizatorilor ce nu sunt înrolați la nici un operator SETRE posibilitatea de înregistrare a traseului parcurs.
11	Componenta aplicație mobila achiziție rovinieta si peaj (<3.5 tone)	- Aplicație mobila pentru dispozitive mobile de tip smartphone, ANDROID sau IOS, care facilitează emiterea rovinietelor si a peajului. Aplicația exista la acest moment in portofoliul CNAIR dar aceasta va trebui adaptata, modernizata si înglobata in noul sistem de tarifare electronica

Nr.	Modul / componenta software	Funcționalitate
12	Componenta GIS	- Permite definirea pozițiilor geografice ale tronsoanelor de drum care vor fi incluse in domeniile de taxare - Produce harți geografice pentru afișarea vizuala a tronsoanelor de drum - Afișează harta geografica a traseului parcurs de către un autovehicul
13	Componenta de facturare	Calculează si realizează facturi pe baza datelor prelucrate in modulul central precum si urmărirea încasărilor acestora pentru autovehiculele înrolate in modul tarif per kilometru
14	Servicii emitere roviniete si peaj prin parteneri	Servicii pentru emitere a rovinietelor si peaj-elor (tarif trecere obiectiv) prin parteneri.
15	Portal Extern	Portal pentru utilizatorii externi (internet) care asigura următoarele funcționalități: - Înrolarea unui client nou - Înrolarea unui autovehicul pe oricare din cele 2 moduri de tarifare – per timp sau per kilometru - Emitere roviniete si peaj - Expune informații clienților autentificați dupa caz despre rovinietele si peaj-ul achitat , traseul parcurs de un autovehicul si tariful aferent - Notificări despre rute ocolitoare - Informații despre tarifele practicate - Funcționalități de tip service desk / call center digital pentru utilizatorii externi

Nr.	Modul / componenta software	Funcționalitate
		Integrare: - Integrare cu procesator de plăti electronice (card) - Se integrează cu modulul central (core sistem) - Se integrează cu modulul GIS
16	Portal Intern	- Reprezintă interfața utilizator a modulului central (core sistem) – User Interface - Faciliteaza administrarea nucleului central (core sistem) pe baza de roluri de Securitate
17	Componenta DataWarehouse	- Cuprinde datamart-uri specializate pe arii distincte si moduri de tarifare
18	Componenta de analiză și prognoză (Analytics)	- Se va extinde actualul sistem de raportare care cuprinde dashboard-uri si rapoarte specifice rovinietelor si a peaj-ului cu analize si rapoarte specific noului tip de tarifare. - Abordarea va fi in modul extindere licentiere produse existente sau licentiere integrala in cazul utilizarii unor alte produse software de tip COTS.
19	Componenta baze de date relaționale	- Asigura persistenta datelor in mod relational - Abordarea va fi in modul extindere licentiere produse existente sau licentiere integrala in cazul utilizarii unui alt tip de baze de date decat cele existente in actualul sistem
20	Componenta replicare date	- Asigura replicarea datelor din baze de date relaționale

Nr.	Modul / componenta software	Funcționalitate
		- Abordarea va fi in modul extindere licențiere produse existente sau licențiere integrala in cazul utilizării unor alte produse software de replicare date
21	Modul contravenții	Asigura colectarea datelor de la punctele de control sau sistemele ITS Asigura procesarea datelor despre contravenții si întocmirea documentelor aferente contravențiilor pentru ambele moduri de tarifate – pe baza de timp si pe baza de distanta parcursa Asigura evidenta contestațiilor Se integrează cu modulul PKI in vederea emiterii de certificate digitale necesare securizării comunicației dintre punctele de control sau ITS si modulul de contravenții Asigura gestionarea punctelor de control si a sistemelor ITS de la care colectează date Persista in sisteme de tip object storage a imaginilor recepționate de la punctele de control Asigura funcționalitatea unui punct de control fie in mod verificare locala autovehicul fie prin transmitere integrala a imaginilor autovehiculelor Asigura suplimentar fără intervenție umana a recunoașterii numărului auto a autovehiculului din imagine (dubla verificare)

Nr.	Modul / componenta software	Funcționalitate
		Expune servicii web (REST) in scop de control valabilitate rovinieta , peaj, ruta preplătita sau înrolare la sistemul de tarifare prin operatorii SETRE. Aceste servicii vor fi utilizate de catre echipajele mobile de control
22	Componenta persistenta imagini de tip object storage	Componenta de tip Object Storage de inalta performanta compatibila Amazon Web Service S3
23	Componenta servere de aplicații	Se utilizează pentru componentele COTS sau dezvoltate custom ce impun utilizarea unui server de aplicații.
24	Componenta servere web	Serverele web vor fi utilizate pentru expunerea conținutului static ale aplicațiilor software sau ca si reverse proxy pentru aplicații web.
25	Componenta Api Gateway	API gateway este un instrument de management API care se află între un client și o colecție de servicii backend. Un gateway API acționează ca un reverse proxy pentru a accepta toate apelurile API, pentru a agrega diferitele servicii necesare pentru a le îndeplini și pentru a returna rezultatul corespunzător. Va fi utilizat ca si intermediar catre toate serviciile expuse catre sistemele externe cat si ca intermediar catre serviciile externe consumate de catre sistemele interne
26	Sistem de Management Acces	Sistem standard de management de acces.
27	Sistem de stocare profile utilizatori	Platforma care permite accesarea datelor despre utilizatori atât din baze de

Nr.	Modul / componenta software	Funcționalitate
		date cât și din directoare LDAP, cu posibilitatea de agregare selectivă a profilelor și expunerea acestor informații în format LDAP către alte sisteme;
28	Platforma de automatizare infrastructura	Platforma de automatizare infrastructura oferă următoarele funcționalități: - Inventar infrastructura - Automatizare procese de configurare, întreținere si relocare componente de infrastructura
29	Platforma PKI	Infrastructura de chei publice (PKI) este setul de hardware, software, politici, procese și proceduri necesare pentru a crea, gestiona, distribui, utiliza, stoca și revoca certificatele digitale și cheile publice. Certificatele si cheile publice vor fi utilizate pentru criptarea pachetelor cu mesaje de la punctele de control , sistemele ITS si echipajele mobile. De asemenea comunicația dintre operatorii SETRE si mașinile de tip self service (KIOSK) vor fi de tipul mutual authentication utilizat certificate si chei private emise din platforma PKI Platforma PKI se integrează cu modulele hardware HSM

4.2.3 Arhitectura tehnică

4.2.3.1 Cerințe generale

In definirea arhitecturii tehnice se vor considera lua următoarele:

- Mediul de producție - asigură funcționarea în regim de producție a sistemului informatic și reprezintă mediul care va fi utilizat efectiv de către Beneficiar;
- Mediul de testare și dezvoltare - asigură mediul pe care vor fi dezvoltate și testate toate componentele sistemului într-un mod integrat, înainte ca acestea să fie trecute în producție;
- Mediul de disaster recovery - asigură replica fidelă a mediului de producție, într-o locație geografică diferită față de locația ce găzduiește mediul de producție, astfel încât să poată fi implementate procedurile de recuperare în caz de dezastru;

4.2.3.2 Estimativ volumetric pentru dimensionarea mediului de productie

Pentru dimensionarea mediului de producție s-au luat în considerare următoarele:

- **La nivel comunicații internet si rețea privata:**

  Pentru schimburi de date intre punctele de control si datacenter a fost luat in calcul cel mai mare punct de control si anume cel de la stația de taxare Fetești. Maximul de trafic a fost înregistrat in luna august a anului 2021 cu valoarea de aproximativ 60.000 de autovehicule pe perioada de 24 de ore. Astfel, având in vedere faptul ca verificarea de plata a taxei de drum se face pentru fiecare autovehicul si adițional, se transmit către centru imagini si date pentru aproximativ 20% dintre autovehicule (doar pentru cele ce se încadrează pentru contravenție sau număr de identificare nerecunoscut, iar maximul de date pentru un autovehicul este de 20k), traficul de date s-ar situa la nivelul de 600 Mb per zi. La acest trafic de date se vor adaugă posibilul trafic aferent echipajelor de control care ar adera la acest punct de control si care se estimează la un nivel de 200 Mb / zi. Traficul total pe zi ar fi astfel de 800 Mb cu un vârf de +50 in intervalul orar 08 – 12. Ținând cont de faptul ca CNAIR își dorește o rețea de **300 de puncte de control fixe**, traficul total dinspre punctele de control si datacenter ar fi de 234 Gb/zi.

Pentru colectarea de date de la operatori SETRE despre poziția si evenimentele unui autovehicul si avand ca si suma estimata de km parcursa de autovehiculele de peste 3,5 tone de circa 30.000.000 de km pe zi, coroborat cu schimbul de date pe kilometru parcurs si cadența de transmitere a datelor de la OBU , estimatul de date transmise este de aproximativ **1 TB / zi**

Traficul însumat pentru emiterea rovinietelor si a peaj-ului, a înrolării unui nou autovehicul in vederea taxării la distanta parcursa si a schimbului de mesaje cu celelalte instituții ale statului ar fi estimat la 300Gb / zi.

Totalul general de trafic de date ar fi astfel in jurul a 1,5Tb/zi cu vârfuri de trafic in perioada 08 – 12 a zilei de +50% din traficul total

Daca se tine cont de faptul ca datele vor fi replicate si intr-un site secundar , atunci traficul general pe zi ar fi in jurul a 3 Tb / zi (se replica si date structurate ale bazelor de date relaționale si nu numai cele primare)

WAN bandwidth: **2 Gb/s** pentru mediul de producție.

- **La nivel stocare de date**

Ținând cont de faptul ca datele culese într-o zi vor fi procesate dar si stocate pe o perioada de minim 1 an in forma primita , se estimează ca total capacitate de stocare necesara pentru primul an de funcționare ar fi in jurul a 1,5 - 2Pb la nivel de datacenter

- Portalul extern la care vor avea acces persoanele fizice și juridice pentru informare trebuie să asigure un număr nelimitat de utilizatori / vizitatori externi (read only);
- Portalul extern la care vor avea acces persoanele fizice și juridice pentru operațiuni ce necesită autentificarea și gestionarea acestuia trebuie să asigure un număr de minim 4.000.000 de utilizatori autentificați (persoane fizice și juridice), din care 2000 concurenți;
- Portalul intern trebuie să asigure acces pentru un număr de 2000 utilizatori interni (angajați sau colaboratori ai Beneficiarului) din care 250 concurenți;

Soluția va fi cu acces centralizat, web-based, cu diverse grupuri de acces, însă capabilitățile generice nu vor fi diferite.

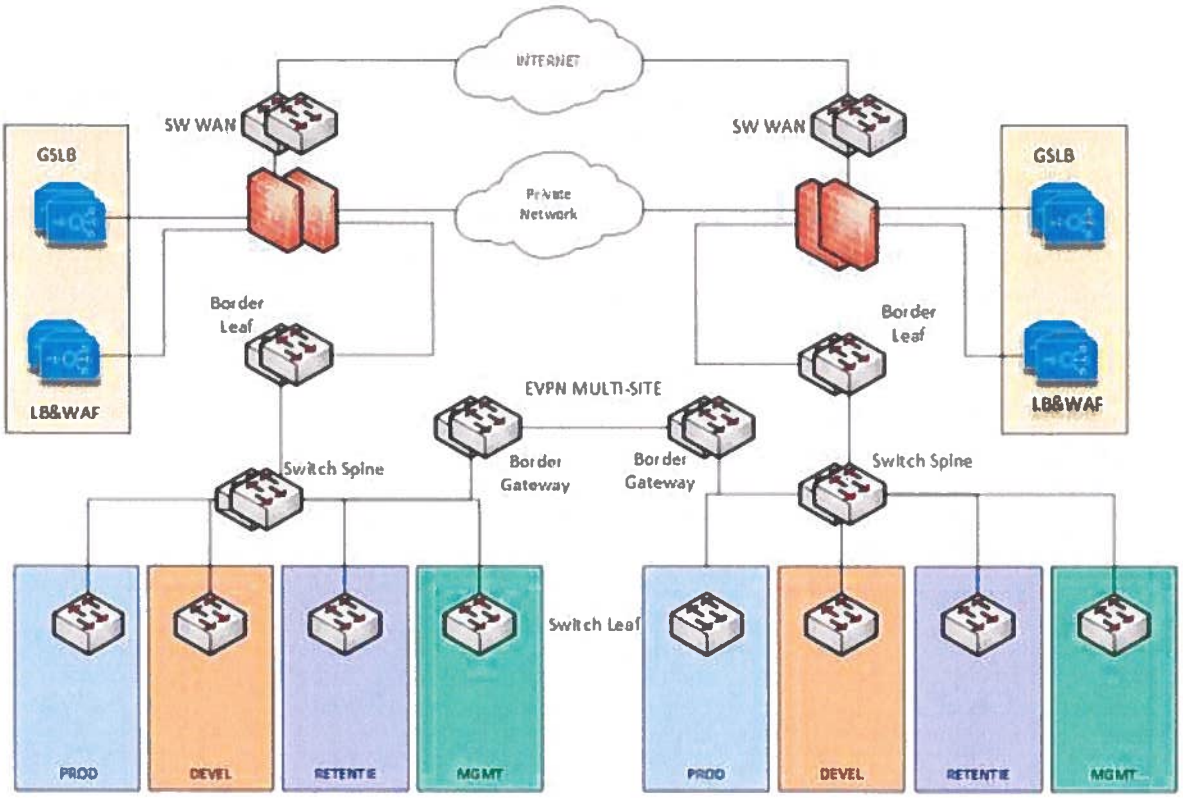


Figura 3: Arhitectura Fizică

Mediul de testare-dezvoltare va respecta arhitectura mediului de producție la nivel de topologie, diferența constând într-o alocare diferită de resurse. Acest mediu va fi instalat și configurat doar în site-ul principal.

Arhitectura mediului de producție trebuie să conțină următoarele zone: de producție, de dezvoltare, de retenție si de management, atât în site-ul principal cât și în site-ul secundar.

Mediul de disaster recovery va avea o arhitectura identica 1:1 cu mediul de producție, fiind instalat și configurat în site-ul secundar.

Din punct de vedere al resurselor de stocare, fiecare mediu are echipamentele fizice dedicate pentru stocarea datelor operaționale, la nivelul acestora urmând a fi alocate volume și spații diferite, asigurându-se că aceasta configurare nu afectează performanța, stabilitatea și securitatea mediului de producție.

4.2.3.3 Dimensionare

Soluția hardware furnizată va trebui să fie asigurată de soluții de tip server Enterprise care să permită virtualizarea/containerizarea resurselor.

Ținând cont de perioada de implementare alocată, se impune utilizarea unor produse software care au trecut cel puțin printr-un ciclu complet de dezvoltare, astfel încât să dovedească stabilitate la nivel

funcţional precum şi maturitate tehnologică. Aşadar, componentele din tabelul de mai jos trebuie să fie produse comerciale de tip COTS, care au asigurate accesul la:

- versiuni noi ale produselor software licenţiate, patch-uri de securitate, upgrade-uri cu îmbunătăţiri ale produselor software licenţiate şi totodată beneficiază de servicii expert furnizate de producător / distribuitor / prestator;
- servicii de optimizare a implementării în conformitate cu procesele de business pentru fiecare componenta software şi de integrare între componentele sistemului care să asigure implementarea cu succes a proiectului care este unul de interes naţional cu o arhitectura care permite integrarea cu alte sisteme informatice şi servicii electronice naţionale.

Dimensionarea componentelor aferente mediului de producţie va trebui să asigure minimul de resurse de procesare după cum urmează:

Nr. crt.	Componentă	Nr. noduri	Topologie	Nr. core-uri fizice per nod
1	Componenta modul central si servicii web	12	Cluster Multinod	16
2	Componenta contravenţii si servicii de control	8	Cluster Multinod	16
3	Componenta portal	4	Cluster Activ-Activ	16
4	Componenta server de aplicaţii	6	Cluster Activ-Activ	8
5	Componenta server web	8	Cluster Activ-Pasiv	4
6	Componenta de baze de date relaţionale si replicare date	6	Cluster Activ-Activ	8
7	Componenta de integrare date (Data Integrator)	2	Cluster Activ-Activ	8
8	Componenta de procesare fluxuri de date	4	Cluster Distribuit	16
9	Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)	4	Cluster Distribuit	16
10	Componenta de integrare şi gateway pentru servicii web (inclusiv developer portal)	4	Cluster Activ-Activ	16
11	Componenta Big Data (include si Componenta Platforma de gestiune fluxuri de date - streaming engine)	24	Cluster Distribuit	8
12	Componenta de analiză şi prognoză	2	Cluster Activ-Pasiv	16
13	Componenta GIS	2	Cluster Activ-Activ	16
14	Componenta Stocare centralizata profile utilizatori	4	Cluster distribuit	16
15	Componenta de gestiune acces utilizatori	4	Cluster Activ-Activ	16
16	Componenta de disaster recovery	1	Single Node	8
17	Componenta de analiză şi detecţie atacuri cibernetice	1	Single Node	16
18	Componenta PKI	4	Cluster Activ-Activ	8
19	Componenta SIEM	4	Single Node	16
20	Platforma CI/CD, Source repository, Code Quality	6	Cluster Distribuit	16
21	Alte resurse (Manager Virtualizare, Platforma Automatizare, DNS, Email)	6	Single Node	8

Pentru componentele ce implementează clustere de tip activ-activ, balansarea încărcării se va realiza prin intermediul echipamentelor hardware dedicate ADC / WAF sau prin mecanisme proprii puse la dispoziție nativ de către acele componente software.

Pentru mediul de testare se va asigura minimul de resurse de procesare după cum urmează:

Nr. crt.	Componentă	Nr. noduri	Topologie	Nr. core-uri fizice per nod
1	Componenta modul central si servicii web	6	Cluster Multinod	8
2	Componenta contravenții si servicii de control	6	Cluster Multinod	8
3	Componenta portal	2	Cluster Activ-Activ	8
4	Componenta server de aplicații	4	Cluster Activ-Activ	8
5	Componenta server web	4	Cluster Activ-Pasiv	4
6	Componenta de baze de date relaționale si replicare date	4	Cluster Activ-Activ	4
7	Componenta de integrare date (Data Integrator)	2	Cluster Activ-Activ	4
8	Componenta de procesare fluxuri de date	2	Cluster Distribuit	8
9	Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)	2	Cluster Distribuit	8
10	Componenta de integrare și gateway pentru servicii web (inclusiv developer portal)	2	Cluster Activ-Activ	8
11	Componenta Big Data (include si Componenta Platforma de gestiune fluxuri de date - streaming engine)	8	Cluster Distribuit	8
12	Componenta de analiză și prognoză	2	Cluster Activ-Pasiv	8
13	Componenta GIS	2	Cluster Activ-Activ	8
14	Componenta Stocare centralizata profile utilizatori	2	Cluster distribuit	4
15	Componenta de gestiune acces utilizatori	2	Cluster Activ-Activ	4
16	Componenta PKI	2	Cluster Activ-Activ	8

Dimensionarea componentelor aferente mediului productiv din site-ul secundar (Disaster recovery site) va trebui să asigure minimul de resurse de procesare după cum urmează:

Nr. crt.	Componentă	Nr. noduri	Topologie	Nr. core-uri fizice per nod
1	Componenta modul central si servicii web	12	Cluster Multinod	16
2	Componenta contravenții si servicii de control	8	Cluster Multinod	16
3	Componenta portal	4	Cluster Activ-Activ	16
4	Componenta server de aplicații	6	Cluster Activ-Activ	8
5	Componenta server web	8	Cluster Activ-Pasiv	4

6	Componenta de baze de date relaţionale si replicare date	6	Cluster Activ-Activ	8
7	Componenta de integrare date (Data Integrator)	2	Cluster Activ-Activ	8
8	Componenta de procesare fluxuri de date	4	Cluster Distribuit	16
9	Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)	4	Cluster Distribuit	16
10	Componenta de integrare şi gateway pentru servicii web (inclusiv developer portal)	4	Cluster Activ-Activ	16
11	Componenta Big Data (include si Componenta Platforma de gestiune fluxuri de date - streaming engine)	24	Cluster Distribuit	8
12	Componenta de analiză şi prognoză	2	Cluster Activ-Pasiv	16
13	Componenta GIS	2	Cluster Activ-Activ	16
14	Componenta Stocare centralizata profile utilizatori	4	Cluster distribuit	16
15	Componenta de gestiune acces utilizatori	4	Cluster Activ-Activ	16
16	Componenta de disaster recovery	1	Single Node	8
17	Componenta de analiză şi detecţie atacuri cibernetice	1	Single Node	16
18	Componenta PKI	4	Cluster Activ-Activ	8
19	Componenta SIEM	4	Single Node	16
20	Platforma CI/CD, Source repository, Code Quality	6	Cluster Distribuit	16
21	Alte resurse (Manager Virtualizare, Platforma Automatizare, DNS, Email)	6	Single Node	8

Sistemul va fi compus din cel puţin următoarele componente hardware şi de comunicaţii la nivelul site-ului principal care găzduieşte mediul de producţie şi mediul de testare-dezvoltare:

Nr. crt.	Componentă	Cantitate
4.4.1	Echipament server tip 1	20
4.4.2	Echipament server tip 2	15
4.4.3	Echipament stocare tip 1	1
4.4.4	Echipament stocare tip 2	1
4.4.5	Echipament stocare tip 3	1
4.4.6	Switch Distribuţie	2
4.4.7	Firewall Border	2
4.4.8	Switch LAN tip 1	2
4.4.9	Switch LAN tip 2	12
4.4.10	Switch LAN tip 3	6
4.4.11	Switch Border Gateway	2
4.4.11	Load Balancer	2
4.4.13	Soluţie de backup	1
4.4.14	HSM	2

4.4.15	Rack și accesorii	6

La nivelul site-ului secundar vor fi prevăzute următoarele componente hardware și de comunicații:

Nr. crt.	Componentă	Cantitate
4.4.1	Echipament server tip 1	16
4.4.2	Echipament server tip 2	13
4.4.3	Echipament stocare tip 1	1
4.4.4	Echipament stocare tip 2	1
4.4.5	Echipament stocare tip 3	1
4.4.6	Switch Distributie	2
4.4.7	Firewall border	2
4.4.8	Switch LAN tip 1	2
4.4.9	Switch LAN tip 2	12
4.4.10	Switch LAN tip 3	6
2.4.11	Switch Border Gateway	2
2.4.12	Load Balancer	2
2.4.13	Soluție de backup	1
2.4.14	HSM	2

4.2.3.4 Comunicații

Comunicațiile între centrele de date (principal și secundar) sunt asigurate prin intermediul Serviciului De Telecomunicații Speciale
Comunicațiile între centrele de date (principal și secundar) si punctele de control sunt asigurate prin intermediul Serviciului De Telecomunicații Speciale

Se dorește implementarea unui rețele programabile de comunicații pentru centrul de date. Astfel, se dorește livrarea la cheie a unei rețele programabile de comunicații in care platformele hardware si platforma software de administrare-operare sa fie strâns integrate si sa asigure scalabilitate, performanta, flexibilitate si reziliența. De asemenea, se dorește asigurarea de catre ofertant a interconectarii din punct de vedere logic cu rețeaua existenta precum si extinderea serviciilor din reteaua existenta in noul centru de date.
Arhitectura soluției trebuie sa includa pentru fiecare Centru de Date, in mod minimal, următoarele subcomponente hardware si software:

- **Nivelul Agregare**: Switch Agregare DC (Switch LAN tip 1, cap. 4.4.8);
- **Nivelul Access**: Switch Access DC cu interfețe 10/25 Gbps (Switch LAN tip 2, cap. 2.4.9);
- **Nivelul Administrare/Operare**: Platforma hardware si software de administrare a rețelei programabile și Switch-uri de management (Switch LAN tip 3, cap. 2.4.10);

Suplimentar, la nivelul întregii soluţii, pentru **Nivelul Interconectare Logica** se va furniza si o Platforma software de configurare centralizata a reţelelor programabile.

Nivelul Agregare trebuie sa îndeplinească următoarele cerinţe:

- Sa conecteze toate subcomponentele nivelului Acces
- Sa asigure o comunicaţie redundanta si scalabila intre subcomponentele nivelului Acces
- Sa asigure comunicaţia intre locaţii prin interconectarea scalabila si rezilienţa cu reţeaua de transport si/sau cu restul echipamentelor propuse in cadrul acestui proiect

Nivelul Acces trebuie sa asigure o arhitectura unitara si uniforma pentru accesul la reţea a sistemelor existente precum si a celor viitoare.

Nivelul Administrare/Operare trebuie sa asigure administrarea si operarea echipamentelor din nivelurile Agregare si Acces, precum si integrarea cu alte sisteme de management (de exemplu sisteme de virtualizare).

Nivelul Interconectare Logica trebuie sa asigure administrarea centralizata a reţelelor programabile din ambele locaţii (cea existenta si cea ofertata in cadrul acestui proiect) in mod unitar (resursele administrate sa se poată defini centralizat si unitar).

Nivelul Administrare/Operare trebuie sa asigure administrarea si operarea echipamentelor din nivelele Agregare si Acces ofertate, independent, printr-o Platforma hardware si software de administrare a reţelei programabile ce va fi ofertată in cadrul acestui proiect. In acest scop, Platforma hardware si software de administrare a reţelei programabile ofertată va asigura următoarele funcţionalităţi minimale:

- Să ofere o interfaţă grafică pentru administratorii reţelei;
- Să ofere o interfaţă programatică standardizată şi deschisă de tip "Representational State Transfer" (REST) sau echivalent, care să faciliteze integrarea cu alte platforme şi aplicaţii existente şi viitoare;
- Să ofere un grad înalt de redundanţă şi rezilienţă care să asigure protecţia (N+2) împotriva erorilor sistemelor pe care rulează Soluţia de Administrare a Reţelelor din Centre de Date;
- Să ofere toate licenţele necesare folosirii funcţionalităţilor împreună cu echipamentele cerute la nivelul Agregare şi nivelul Acces;
- Să asigure suportul fizic de calcul necesar pentru rularea în condiţii optime de performanţă, scalabilitate şi redundanţă, inclusiv modulele optice de conectare necesare pentru conectarea la reţea;
- Să ofere facilitaţi de monitorizare şi administrare a anomaliilor şi a erorilor de funcţionare ale sistemului;
- Să ofere facilităţi de monitorizare a performanţei atât pe termen scurt cât şi pe termen lung;
- Să ofere facilităţi de configurare automată a echipamentelor cerute la nivelul Agregare şi nivelul Acces conform unui set de reguli şi politici definite prin interfaţa grafică sau prin intermediul interfeţei programatice (API sau echivalent)
- Sa asigure segmentarea si micro-segmentarea reţelei Centrului de Date pe baza regulilor impuse de necesităţile operaţionale.

- Să ofere facilități de administrare și inventariere a componentelor hardware și software ale echipamentelor de la nivelul agregare și nivelul acces;
- Să poată fi extinsă pentru a suporta și alte echipamente decât cele solicitate la nivelul Agregare și nivelul Acces;
- Să suporte controlul cu echipamentele de rețea prin intermediul metodelor ca interfață de control de tip linie de comanda (CLI) dar și prin protocoale deschise ca OpenFlow, OpFlex sau echivalent;
- Să suporte implementarea funcționalităților pentru configurarea politicilor de securitate, metodelor de control al accesului si mecanismelor pentru optimizarea și balansarea traficului, prin introducerea în calea de comunicație între elementele de aplicație vizate a nodurilor fizice sau virtuale de procesare care implementează aceste funcționalități;
- Să suporte configurarea înlănțuirii unuia sau a mai multor noduri (fizice sau virtuale) de procesare a serviciilor precum controlul accesului, optimizarea și balansarea traficului, filtrarea traficului la nivel de aplicație; de asemenea, să suporte și configurarea ordinii în care traficul va fi procesat de către acestea;
- Să suporte metode prin care să permită integrarea cu versiuni ulterioare ale echipamentelor folosite pentru înlănțuirea nodurilor de procesare a serviciilor;
- Să fie compatibila si integrabila cu alte sisteme de management cum ar fi sisteme de management a hipervizorului, echipamente cu funcții ca balansarea traficului la nivelele ISO-OSI 4-7 sau echipamente de securitate de tip Firewall sau IPS;
- Să suporte cel puțin dublarea capacității - ca număr de porturi - la nivelul Access.

Pentru asigurarea administrării centralizate si a operării rețelelor programabile din cele doua locații (cea existenta si cea ofertata in cadrul acestui proiect) intr-un mod unitar, Platforma software de configurare centralizata a rețelelor programabile trebuie sa fie capabila sa ofere si funcționalitățile de configurare logica oferite de Platforma hardware si software de administrare a rețelei programabile la nivelul întregii rețele programabile (formata din rețelele centrelor de date din cele doua locații). De asemenea, aceasta trebuie sa permită configurarea interconectării nivelelor Agregare din cele doua locații, folosind o rețea capabila sa transporte trafic IPv4 cu capabilitati Layer 3 Unicast, precum si definirea unor servicii de conectivitate L2/L3 extinse peste mai multe retele programabile.

4.3 CERINȚE TEHNICE PENTRU COMPONENTELE SOFTWARE DE BAZĂ

4.3.1 Componenta portal

Portalul Web va reprezenta un punct unic de acces la sursele de informații si servicii si trebuie realizat pe o platforma flexibila si scalabila, capabila sa asigure standardizarea si reutilizarea resurselor si serviciilor, sa furnizeze permanent conținut si informații noi, precum si acces rapid la informații si servicii (componente ale soluției).

De asemenea, interacțiunea cu cetățenii si partenerii precum si colaborarea cu aceștia va fi asigurata prin intermediul platformei de portal si a componentelor sale.

Platforma de portal trebuie sa permită actualizarea rapida a conţinutului fără a necesita resurse de dezvoltare, distribuirea conţinutului, stabilirea roluri lor si a drepturilor de acces.
Platforma portal trebuie sa fie o componenta matura, integrata, stabila si sigura, de tip COTS, si ofere următoarele funcţionalităţi generale:

- interfaţa web, facila pentru prezentare si navigare rapida si simpla;
- Posibilitatea de a personaliza conţinutul;
- Caracteristici pentru securitate ridicata;
- Configurare in regim de înalta disponibilitate;
- Să ruleze pe sisteme de operare Windows, Linux.
- Sa poată fi configurat astfel încât sa permită crearea de zone securizate pe care utilizatorii sa le poată accesa din interiorul si exteriorul organizaţiei, in conformitate cu matricea drepturilor de acces;
- Trebuie sa fie un sistem deschis bazat pe standardele existente in domeniu;
- Trebuie sa permită administrarea facila;
- Dezvoltarea aplicaţiilor trebuie sa se facă uşor, respectând standardele in domeniu;
- Portalul trebuie sa ofere un punct centralizat de lucru pentru utilizatori si o interfaţa unica;
- Este necesar ca interfaţa portalului sa fie separata, din punct de vedere logic, de codul aplicatiilor integrate, astfel încât in cazul actualizării unei aplicaţii, sa se păstreze toate particularizările ce au fost efectuate asupra interfeţei;
- Conţinutul accesat prin portal trebuie sa poată fi automat afişat sau ascuns, pe baza rolurilor utilizatorilor, roluri care sunt predefinite;
- Administratorii trebuie sa poată controla drepturile utilizatorilor funcţie de rolul acestora sau funcţie de regulile definite;
- Posibilitatea de integrare şi comunicare în timp real cu o soluţie de Management al indentaţii externă portalului sau cu un director de utilizatori (AD/ LDAP) oferind inclusiv posibilitatea de sincronizare în timp real cu soluţia respectivă; Posibilitatea de a folosi o bază de date externă cu utilizatori;
- Sistemul portal trebuie sa permită utilizarea de mecanisme pentru autentificare, autorizare SSO si SSL; de asemenea, trebuie sa permită si integrarea cu soluţii de securitate;
- Pentru aplicaţiile care nu pot fi modificare (aplicaţii găzduite de alt provider) soluţia trebuie sa ofere posibilitati de SSO prin rescrierea de header web, servicii web, cookie-uri sau dezvoltare de agenti sau procese de autentificare custom;
- Nici o resursa web din interiorul sistemului nu trebuie sa poată fi accesata direct din exterior, orice acces realizandu-se prin intermediul serverelor web proxy;
- Sa integreze controlul accesului pentru componentele sistemului;
- Trebuie sa suporte autentificare de tip two-factor;
- Sa ceara utilizatorilor sa introducă date de identificare pentru accesul la aplicaţii;
- Sa permită impunerea unor filtre de acces (operaţiuni de autorizare) - cel puţin interval orar si locaţie de reţea de unde s-a iniţiat cererea de acces;

- Sa permită administratorului sistemului sa aleagă mai metode de autentificare si autorizare diferite pentru fiecare grup de resurse in parte;
- Sa ofere o interfață de administrare de tip web pentru accesul facil la configurări, care sa poată fi accesata doar de către administratorii de securitate ai soluției;
- Sa ofere SSO - autentificare unica pentru accesul la resurse; pe parcursul unei singure sesiuni de lucru utilizatorul fi autentificat o singura data , după care va putea accesa fără reautentificare toate aplicațiile web pentru care are drept de acces;
- Fiecare utilizator sa fie identificat de sistem pe baza unei sesiuni;
- Sistemul sa permită administratorilor terminarea manuala a sesiunilor utilizatorilor;
- Soluția trebuie sa ofere si proceduri de autentificare pentru serviciile web si aplicatii ce depind de parteneri sau provideri folosind mecanisme SAML 1.0, 1.1, 2.0, OpenID 1.0 si WS-Federation;
- Soluția trebuie sa asigure funcționalități de management al utilizatorilor si de control a drepturilor de acces:
  - Autentificarea unica a utilizatorilor prin servicii de tip Single Sign-On (SSO) si autorizarea acestora in sistem pe baza rolurilor si privilegiilor definite;
  - Utilizatorii trebuie sa aiba acces numai la aplicatiile si documentele pentru care li s-a acordat dreptul de acces;
  - Trebuie sa suporte un mod flexibil si unitar de gestiune a drepturilor si politicilor de acces ale utilizatorilor la toate resursele sistemului;
  - Trebuie sa permită supravegherea cererilor de servicii si operațiilor executate de o persoana care a generat, a modificat sau a stres o informație;
- Soluția trebuie sa permită deconectarea automata - trebuie sa ofere un mecanism prin care un utilizator sa fie deconectat in cazul in care nu a mai efectuat nicio tranzactie intr-o anumita perioada de timp;
- Sistemul de portal trebuie sa permită utilizarea pofilelor de utilizatori, administratorul putând seta astfel preferințele atât la nivel de profil, grup, cat si la nivel de utilizator. Aceste preferințe specifica atat accesul pe care il vor avea la diverse sectiuni ale portalului, cat si drepturile asupra acestor zone;
- Soluția trebuie sa permită limitarea autentificărilor la o singura instanța. Daca un utilizator încearcă sa se autentifice printr-o alta sesiune, atunci sesiunea initiala va fi inchisa automat;
- Soluția trebuie sa suporte SSO atât cu single cookie domain cat si cu multiple cookie domain pentru a asigura suport SSO intre aplicatii;
- Soluția trebuie sa asigure suport SSO de tip federație pentru a extinde procesele de SSO intre aplicații interne sau externe;
- Soluția trebuie sa aiba o arhitectura deschisa;
- Soluția trebuie sa suporte XML si sa aibă suport pentru servicii web;
- Sistemul trebuie sa fie flexibil din punct de vedere al clientului, putand fi accesat de pe majoritatea browserelor web existente pe piața;
- Sistemul portal trebuie sa permită folosirea de politici (colecții de setări) pentru administrarea următoarelor componente: utilizatori, grupuri, aplicații;

- Trebuie sa ofere nativ mecanisme de salvare si restaurare;
- Trebuie sa ofere posibilitatea de a recupera rapid informaţii dintr-o baza de date de conţinut, fără a fi necesara restaurarea întregii soluţii din care face parte acea baza de date;
- Trebuie sa permită un asistent de creare de site-uri ce permite setarea permisiunilor, crearea de şabloane de conţinut si adăugarea de teme personalizate;
- Trebuie sa permită dezvoltarea de aplicatii bazate pe standarde web;
- Trebuie sa pună la dispoziţie un mecanism robust de monitorizare a încărcării si performantei sistemului;
- Trebuie sa pună la dispoziţie un mecanism de configurare/scripting de tip command-line;
- Sa permită dezvoltarea de portrete folosind standardul JSR-286;
- Sa aibă o arhitectura dinamica si modulara ce permite actualizarea si instalarea portletilor fara a fi necesara oprirea platformei portal;
- Soluţia trebuie sa ofere capabilităţi de clustering si load balancing;
- Sa aibă o metodă de analiză anonimizată a traficului web, care să permită identificarea provenienţei vizitatorilor, a resurselor vizitate, informaţiilor demografice si dispozitivelor utilizate;
- Sa ofere suport pentru personalizare folosind un sistem de reguli care să susţină cel puţin afişarea de conţinut relevant utilizatorilor pe baza informaţiilor demografice ale utilizatorului, precum şi activităţi şi proprietăţi asociate profilului acestuia;
- Sa includa un sistem de colectare feedback (customer satisfaction / rate your experience);
- Sa ofere funcţionalităţi de editare instant a paginilor cu publicarea modificărilor într-un singur pas, fie la final fie programatic, specificând ce trebuie publicat, la ce ora şi în ce locaţie;
- Să ofere posibilitatea de definire de câmpuri suplimentare cel puţin la nivel de pagini, foldere, documente, imagini, mesaje din forum, blog, calendar şi wiki. Astfel, administratorii vor putea adăuga, edita sau şterge câmpuri suplimentare direct din cadrul sistemului, fără a fi nevoie să acceseze baza de date;
- Platforma trebuie să permită definirea de formulare de tip online, care să ofere capabilităţi de tipul:
  - Instrumente web de design necesare pentru proiectarea şi realizarea de formulare, de tip „pixel perfect", cu posibilitate de export în PDF sau HTML5;
  - Asigurarea autenticităţii şi integrităţii prin posibilitatea de aplicare de semnătură utilizând un certificat digital;
  - Descărcarea formularelor pe staţia de lucru a solicitantului, completarea de informaţii şi posibilitatea de a salva formularul cu datele completate, pentru o utilizare ulterioară;
  - Posibilitatea de a genera coduri de bare de tip 1D sau 2D ce vor codifica informaţiile completate în formular, aceste coduri fiind la rândul lor conţinute în respectivul formular, conform cu design-ul acestuia. Codul de bare generat trebuie să poată fi recunoscut ulterior atât în cazul în care formularul se tipăreşte/scanează, dar şi în cazul în care este transmis în format electronic;
  - sa permită publicarea unui formular web pe orice site sau aplicaţie web externa
  - sa permită asocierea de tipizate in format PDF, cu completarea automata sectiunilor din cadrul tipizatului in functie de valorile introduse in formularul online;

- sa permită versionarea formularelor publicate;
- sa permită generarea de statistici calitative si cantitative cu privire la datele completate de utilizatori (ex. numar de inregistrari, utilizarea campurilor din formular, histograme de valori, influenta valorilor dintr-un camp asupra celorlalte campuri);
- sa permită utilizarea de servicii web sau baze de date pentru selecția valorilor din nomenclatoare
- sa permită asocierea de permisiuni pentru fiecare formular in parte;
- sa ofere o gama larga de câmpuri disponibile (input de tip text, input de tip email, input de tip parola, input de tip free-text, dropdown, checkbox, selector data, selector timp;
- sa permită adăugarea de imagini in cadrul unui formular;
- sa permită configurarea regulilor de validare pentru fiecare camp din formular, precum si configurarea dependințelor intre câmpuri (ex. calcularea valorii dintr-un câmp pe baza altor câmpuri, selecție valori pe baza unei alte valori);
- sa permită traducerea unui formular in limbile Uniunii Europene folosind un serviciu de traducere automata. Traducerea sa poată fi modificata manual de catre utilizator;
- sa permită stocarea valorilor introduse de utilzatorii formularului in structuri tabelare in baza de date pentru analize ulterioare;

- Platforma portal trebuie sa ofere nativ următoarele funcționalități specifice pentru gestiune continut:
  - Platforma trebuie sa permită funcționalități avansate pentru gestionarea documentelor de orice tip precum si lucrul colaborativ pe documente si proiecte;
  - Soluția trebuie sa ofere posibilitatea de a configura ID-urile documentelor;
  - sa ofere posibilitatea publicarii continutului site-urilor prin feed-uri de tip RSS;
  - sa asigure utilizatorilor posibilitatea de a crea moduri personale de vizualizare a informațiilor publicate;
  - sa permită managementul versiunilor de continut;
  - sa permită implementarea de politici de retentie a continutului;
  - sa ofere un mecanism de clasificare si rulare automata a continutului catre spatiile de stocare aferente;
  - sa permită definirea de seturi de documente (stocate in locatii diferite) care sa permită tratarea lor ca o singura entitate;
  - sa pună la dispoziție un mecanism central de gestionare al meta datelor;
  - sa permită o navigare a conținutului bazata pe meta date;
  - sa permită definirea de politici de management al continutului pe durata intregului ciclu de viata;
  - sa permită definirea tipurilor de conținut;
  - sa permită generarea automata de identificatori unici pentru continut;
  - sa permită vizualizarea si editarea direct din interfata web a documentelor de tip doc, xls si ppt sau echivalent;

- sa permită filtrarea afisarii informațiilor prin publicarea lor catre audiente ce sunt compilate pe baza proprietatilor importate din directorul de utilizatori sau prin evaluarea grupurilor din care face parte utilizatorul.

- Platforma portal trebuie sa ofere nativ urmatoarele functionalitati specifice pentru gestiunea fluxurilor de lucru in cadrul organizatiei:
  - sa permită crearea de fluxuri de lucru folosind standardul BPMN 2.0;
  - sa ofere un editor web colaborativ, pentru crearea modelelor BPMN in care utilizatorii pot crea cu usurinta modele noi prin operații de tip drag & drop;
  - sa permită asocierea de ecrane dezvoltate in orice tehnologie activitatilor de interactiune umana de tip Human Task in cadrul unui model BPMN;
  - sa permită vizualizarea pasului curent din cadrul modelului BPMN aflat in executie;
  - sa permită gestiunea cazurilor folosind standardul CMMN (Case Management Model and Notation), inclusiv posibilitatea de a crea modele CMMN folosind un editor web vizual, in care utilizatorii pot crea cu ușurința modele noi prin operații de tip drag & drop;
  - sa ofere suport vizual pentru gestiunea modelelor decizionale folosind standardul DMN (Decision Model and Notation), inclusiv posibilitatea de a crea tabele de decizii in mod vizual, fără cunoștințe de programare;
  - sa ofere suport vizual pentru crearea de formulare de introducere de date, fara cunostinte de programare. Formularele vor putea fi incluse in cadrul fluxurilor de lucru;
  - sa permită versionarea fluxurilor de lucru;
  - sa ofere utilizatorilor o componenta vizuala de interacțiune cu activitățile aferente fluxurilor de lucru;
  - sa permită colaborare prin schimb de mesaje intre actorii implicați in execuția unui flux de lucru;
  - sa ofere suport pentru trimiterea automata de notificări din cadrul unui flux de lucru.

4.3.2 Componenta server de aplicații

Componenta servere de aplicatii va fi utilizata pentru produsele COTS care solicita deployment explicit in astfel de platforme. Este de preferat reutilizarea licentelor existente si/sau extinderea acestora dupa caz, dar acest aspect nu poate fi luat in considerare ca si obligatoriu atat timp cat solutia ofertantului ofera alternative arhitecturale.

Componenta server de aplicatii va asigura infrastructura necesara execuției aplicațiilor moderne bazate pe standarde deschise, și trebuie sa asigure un set de servicii standard pe care toate aplicatiile dezvoltate și instalate sa il poata accesa și utiliza:

- servicii de clusterizare pentru o scalabilitate și disponibilitate ridicata;
- servicii de balansare și dirijare a încărcării (load balancing);
- servicii de securitate pentru protejarea resurselor gazduite;
- servicii de management al tranzacțiilor la nivelul aplicațiilor.

Pentru a raspunde acestor cerinte și celor prezentate in descrierea arhitecturii tehnice și celei functionale, cerintele corespunzatoare platformei de aplicatii sunt:

- Mecanisme de grupare a serverelor in clustere de servere de aplicatii atat in topologii de tip activ-activ cat și activ-pasiv
- Stoparea temporara a unui nod din cluster pentru mentenanța și suport, nu trebuie sa afecteze disponibilitatea celuilalt nod (acest nod permitând executarea/ desfasurarea activitatilor curente)
- Mecanisme de balansare dinamica a incarcarii sistemului intre resursele administrate in cadrul aceluiasi cluster
- Mecanisme de scalare a sistemului pe orizontala și verticala
- Sa permită rularea pe sistemul de operare ofertat;
- Consola de administrare a serverelor de aplicatii cu capabilitati de gestiune a schimbarilor de configuratii:
  - blocarea unei configuratii in vederea modificarii
  - salvarea unei configuratii fara aplicare efectiva
  - revenirea la o configuratie anterioara
  - istoricul modificarilor

4.3.3 Componenta server web

Componenta server web are rolul de a dirija traficul HTTP către serverele de aplicații, totodată activând și ca proxy server, respectând topologia propusa prin arhitectura logica a sistemului. Avand in vedere rolul important al acestei componente se doreste implementarea unei solutii care sa satisfaca cel putin urmatoarele cerinte tehnice:

- Suport pentru SSL și autentificare de baza;
- Extensia funcționalităților pe baza de plugin-uri sau module;
- Operarea în mod reverse-proxy pentru virtualizarea accesului la resursele expuse de sistem;
- Funcționalități de rescriere a adreselor URL;
- Să dispună de mecanisme de balansare a încărcării;
- Să permită configurarea într-un mod de disponibilitate ridicata utilizând mecanisme de tip cluster;
- Să ofere suport pentru IPv4 și IPv6;
- Să permită rularea conținutului dinamic oferind suport pentru tehnologii de programare de larga răspândire;
- Să permită port tunneling;
- Să ofere servicii de web cache pentru creșterea performantei soluției și suport pentru compresia datelor;
- Sa permită instalarea in configurații de înalta disponibilitate utilizând mecanisme interne serverului web.

4.3.4 Componenta de baze de date relationale

Sistemul de gestiune al bazelor de date relaționale trebuie sa fie un sistem de administrare a bazelor de date de tip relațional si sa fie disponibil comercial (COTS – Commercial off the Shelf) si sa

ofere posibilitatea de a rula pe diverse platforme hardware precum si pe sistemele de operare majore existente pe piata (Windows, Linux) , oferind acelasi nivel de functionalitari pe sistemele de operare mentionate. Pentru a raspunde cerintelor de functionalitate si performanta cerute, sistemul de baze de date relaționale trebuie sa prezinte următoarele capabilități minime si obligatorii:

- 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 ;
- 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;
- sa ofere suport pentru proceduri stocate, triggeri si tranzactii autonome ;
- 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, anularea 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 permită 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

4.3.4.1 INFORMATION MANAGEMENT

Din perspectiva managementului datelor baza de date trebuie sa ofere mecanisme avansate de ILM (Information Lifecycle Managment) care sa permită organizarea acestora in mod dinamic si transparent fata de aplicatii prin asigurarea compresiei automate a datelor stocate in tabele dar si partitionarea acestora si a indecsilor dupa diverse criterii ajutand astfel la minimizarea spatiului ocupat de date si cresterea performantei. Partitionarea datelor trebuie sa poata fi facuta dupa cel putin urmatoarele criterii: interval, hash si lista dar si combinatii ale acestora. De asemenea pentru usurinta in administrare baza de date trebuie sa ofere un mecanism automat de creare de noi partitii, bazate pe un interval predefinit de catre administrator, pe masura ce datele sunt introduse in tabela.

4.3.4.2 *DISPONIBILITATE (HIGH AVAILABILITY)*

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

- balansare a incarcarii intre noduri la nivelul cererilor si executiilor pe baza de date cluster, inclusiv posibilitatea de interoga memoria cache de pe celelalte noduri
- 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 permită reconectarea automata la nodul sau nodurile ramase disponibile.
- Baza de date trebuie sa asigure propriul software de clustering si management al discurilor, astfel incat să permită rularea pe diferite platforme, sisteme de operare sau sisteme de fisiere, fara achizitionarea de soft aditional de la producatorul sistemului de operare, asigurandu-se totodata scalabilitatea orizontala a bazei de date.
- Sa permită balansarea încărcării intre noduri, la nivelul cererilor si execuțiilor pe baza de date cluster, indiferent de natura cererilor, astfel se va permite citirea si scrierea pe oricare din nodurile clusterului de baza de date, fără impunerea niciunei limitări.
- Sa ofere posibilitatea adăugării de noduri suplimentare in cazul in care sistemul necesita mai multa putere de calcul, oferind posibilitatea creșterii volumului de citiri si scrieri pe toate nodurile la nivelul bazei date, prin scalarea pe orizontala.

4.3.4.3 *MANAGEMENT PERFORMANTA*

Pentru asigurarea performantei maxime si asigurarea unui răspuns proactiv la eventualele degradări ale acesteia, baza de date trebuie sa ofere mecanisme interne de monitorizare si diagnosticare continua, automatizând 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, explorând in mod cuprinzător toate modalitățile de optimizare ale unei instrucțiuni SQL (inclusiv recomandarea de a fi creați indecși sau partiții adiționale), oferind sugestii de implementare pentru administratori inclusiv posibilitatea de implementare fără a fi necesara modificarea codului aplicației.
Din punct de vedere al operațiunilor de administrare, soluția de baza de date trebuie sa ofere o unealta cu interfața grafica accesibila web pentru administrarea bazei de date, care sa includă următoarele facilitați:

- 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 fișierelor de tip log
- vizualizarea in timp real a încărcării bazei de date, a activității utilizatorilor (inclusiv a interogărilor SQL pe care aceștia le rulează), a operațiilor mari consumatoare resurse (I /O si CPU) precum si raportarea acestor evenimente către administratori

BACKUP

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

4.3.4.4 SECURITATE SI CONFIDENTIALITATE

Ca si mecanisme de securitate oferite, baza de date trebuie sa includă restricționarea accesului la nivelul obiectelor bazei de date, aplicarea simultana a mai multor politici de securitate pe un același obiect al bazei de date precum si mecanisme native de restricționare a accesului utilizatorilor la nivel de înregistrare si coloana într-o tabela. Baza de date trebuie sa permită configurarea autentificării utilizatorilor pe baza de certificate digitale iar pentru sporirea siguranței 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 operațiile de criptare trebuie sa poată fi implementate intr-un mod transparent, fara a implica modificări la nivel de aplicație de business sau client si sa poată fi făcute, in funcție de nevoie, la nivel de coloana, tabela sau chiar baza de date si sa suporte cel puțin următorii 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 informații dintr-o tabela sau cand conectarea nu se face printr-o anumita aplicatie).

4.3.4.5 *OLAP / ANALYTICS*

Baza de date relationala trebuie sa includa mecanisme pentru definirea in baza de date de solutii OLAP, a cuburilor multi-dimensionale de date, in vederea raportarii agregate atat folosind interogari SQL cat si unelte dedicate acestui scop. Pe langa cuburile multi-dimensionale baza de date trebuie sa mai ofere:

- un limbaj consacrat de procesare statistica integrat in baza de date;
- intrumente avansate de tip Data Mining, precum: API-uri specializate, functii specifice (pentru clasificare, regresie, clustering, asociere, detectare de anomalii etc.), wizard, query builder, etc;
- capabilitati de data mining integrate in baza de date, astfel incat procesele de data mining sa se efectueze direct asupra datelor din baza de date, fara a fi necesara extragerea de subseturi de date intr-un server dedicate;
- capabilitatea de a folosi mai multi algoritmi de clasificare si predictive (Naïve Bayes, Support Vector Machines, Decision Trees, etc)
- API-uri pentru interfatarea si integrarea capabilitatilor de Data Mining cu aplicatii de tip enterprise si business intelligence precum si unelte pentru modelarea grafica a datelor si vizualizarea grafica a interogarilor analitice;
- mecanisme native de: analiza predictiva asupra datelor, mining pe informații de tip text, analize statistice, calcule numerice avansate. Aceste mecanisme trebuie sa poata folosi memoria si puterea de procesare a bazei de date si sa poata fi accesate atat prin interfata de tip SQL, cat si prin limbaje statistice

4.3.5 *Componenta de replicare date baze de date relaționale*

Componenta de replicare a datelor din bazele de date relaționale trebuie să îndeplinească următoarele funcționalități:

- Sa ofere posibilitatea trimiterii imediate a datelor sau la un moment ulterior (ales de către utilizator), fără a pierde integritatea tranzacției.
- Sa permită replicarea volumelor mari de date in timp real.
- Sa nu solicite un server middle tier dedicat pentru procesarea informațiilor
- Sa foloseasca protocolul TCP/IP pentru a trimite datele, pentru a elimina constrangerile legate de distantele geografice dintre sitemele sursa si destinatie.

- Sa permită replicarea selectiva, astfel incat in cazul in care intr-o tabela s-au modificat informaţii ce nu sunt necesare in procesul de transformare, acestea sa nu fie extrase si replicate.
- Sa permită compresia datelor rutate.
- Sa permită definirea de puncte de control pentru consistenta procesului de furnizare de date.
- Sa permită extragerea datelor si colectarea acestora in fisiere independente de platforma pe care ruleaza. Fiserele astfel obţinute vor putea fi încărcate in mod continuu in baza de date destinaţie
- Sa permită criptarea datelor.
- Sa permită gestionarea automata a memoriei.
- Asigurarea integritatii bazei de date prin aplicarea operaţiilor in ordinea in care au fost comise.
- Sa permită integrarea cu instrumente de extragere, transformare si încărcare a datelor (ETL) astfel încât asupra datelor extrase sa poată fi aplicate transformări complexe.
- Sa permită rollback dinamic – funcţionalitate pentru refacerea datelor in cazul in care baza de date master este corupta.
- Sa permită replicarea volumelor mari de date tranzacţionale intre baze de date eterogene cu impact minim asupra sistemului de productie.
- Soluţia trebuie sa fie disponibila in caz de dezastru
- Sa asigure integritatea tranzactionala asupra surselor si destinatiilor
- Sa includa functionalitati de arhivare si auditare
- Sa permită mentinerea noului sistem disponibil in permanenta, atat in timpul intreruperilor planificate, cat si a celor neplanificate.
- Sa permită timp de nefunctionare zero pentru intretinerea planificata (in timpul migrarilor si a actualizarilor).
- Sa permită replicarea datelor si sincronizarea pentru sisteme distribuite.
- Sa permită doar replicarea datelor comise
- Sa permită toleranta in caz de dezastru / recuperare in caz de dezastru
- Sa permită mecanisme de captare a datelor modificate (change data capture).
- Sa permită mecanisme rapide, paralele, masive de mutare a datelor intre bazele de date, diferite de cele standard de import/export.
- Sa permită sincronizarea de date pe mai multe centre de date intr-o configuratie activ-activ.
- Sa aiba capabilitati de detectare a conflictelor si de solutionare a acestora.
- Sa dispuna de o arhitectura modulara.
- Sa asigure consistenta datelor.
- Sa dispuna de o topologie flexibila (de exemplu: 1 sursa la 1 destinatie, 1 sursa la mai multe destinatii, mai multe surse la 1 destinatie, mai multe surse la mai multe destinatii, configuratie bidirectionala).

- Trebuie sa permită urmărirea imediata a tranzacțiilor de la nivelul bazelor de date (sursa – destinație).
- Sa permită replicarea instrucțiunilor de tip DDL (Data Definition Language)

4.3.6 Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)

Platforma de procesare a fluxurilor de date si analiza in timp real va permite preluarea, procesarea si analiza unui volum mare de date în timp real, folosind modele de corelație avansate, posibilități de îmbogățire (completare) a datelor preluate, încărcarea datelor procesate și mecanisme avansate de învățare automată.

Licențierea platformei va fi tip perpetuu, fără a exista limite referitor la fluxul de date ce va fi procesat prin platforma.

4.3.6.1 Designer interactiv pentru definirea fluxurilor de date

- Sa ofere un designer grafic ce va permite crearea de noi fluxuri de date (pipelines) cu posibilitate de vizualizare in timp real a datelor intermediare
- Sa ofere posibilitatea de definire facila a etapelor de procesare a datelor prin adaugatea de join-uri cu surse diferite de date, filtrari de date, agregari de date, interogari externe.
- Posibilitatea de a corela fluxuri de date, aplicarea de reguli predefinite, calcularea de câmpuri adiționale, filtrarea si agregarea datelor
- Sa oferte posibilitatea de adaugare etape custom (prin funcții extinse) ce vor putea fi utilizate ulterior de alți utilizatori

4.3.6.2 Funcționalități de analiza predictiva si Machine Learning (ML)

- Posibilitatea de a utiliza modele de învățare automată pentru a putea crea functii de decizie în timp real

- Posibilitatea de a realiza prognoze folosind algoritmi de Machine learning cum ar fi defecțiunile echipamentelor, comportamentul clienților, frauda și breșele de securitate
- Posibilitatea de reimportare a modele ML îmbunătățite pentru realizarea de predicții îmbunătățite
- Posibilitatea de a importa modele predictive create de data scientist pe medii de lucru dedicate
- Posibilitatea dea a ascunde complexitatea modelului pentru utilizare de către analiștii de date
- Posibilitatea de a defini etape custom pentru accesul la sistemele externe ce oferă servicii specializate

- Sa ofere un set predefinit de pattern-uri de analiza a fluxurilor de date ce acoperă arii cum ar fi: detecția anomaliilor, corelarea fluxurilor de date, analiza a trendului evoluției unor indicatori, analiza spațiala. De asemenea, sa ofere funcții predefinite pentru analiza statistica, financiara, analiza de log-uri.

4.3.6.3 *Funcționalități geo spațiale si localizare*

- Sa ofere posibilitatea de a implementa fluxuri de date utilizând date geo spațiale
- Posibilitatea de a gestiona o suita larga de poligoane ce pot fi stocate ca date de tip spațial la nivelul bazei de date
- Posibilitatea de a implementa mecanisme complexe de identificarea a orașului sau a adresei utilizând informații geo spațiale

4.3.6.4 *Capabilități de scalabilitate si procesare a unui volum mare de date*

- Sa ofere mecanisme avansate de scalare oferind posibilitatea de adăugare de noduri suplimentare in mod dinamic
- Sa ofere mecanisme avansate de înalta disponibilitate cu posibilitatea de a nodurilor indisponibile fără pierderi de date
- Sa ofere mecanisme de balansare a încărcării intre diferite noduri din cluster

4.3.6.5 *Conectivitate si manipulare fluxuri de date*

- sa ofere posibilitatea de conectare la multiple surse a de date pe diverse tehnologii, dar minimal platforma va trebui sa asigure conectivitate cel putin pentru: Kafka, JMS, MySQL, file based, soluția de replicare si capturare a modificărilor pe sisteme sursa descrisa in subcapitolul „ Componenta de replicare a datelor si identificare a modificarilor pe sistemele sursa"
- sa ofere posibilitatea de conectare ca si target, a unui set larg de tehnologii, dar minimal platforma va trebui sa asigure conectivitate cel putin pentru: Kafka, HDFS, Hive, Hbase, NFS, servicii de tip REST si solutia de baza de date descrisa in subcapitolul „ Componenta de baza de date", cel putin o solutie de cloud public disponibila pe piata

4.3.6.6 *Deployment*

- Sa permită implementarea conceptului de Continous Integration ce va permite interpretarea in timp real a fluxurilor de date
- Cloud ready: sa permită instalarea (deployment) atat in mediu on-prem, in datacenter-ul clientului, cat si in medii cloud atat ca IaaS (Infrastructure as a Service) cat si ca PaaS (Platform as a Service).
- Sa se integreze cu soluția de replicare si capturare a modificărilor descrisa in subcapitolul „ Componenta de replicare a datelor si identificare a modificărilor pe sistemele sursa"

4.3.7 *Componenta Platforma de gestiune fluxuri de date (streaming engine)*

Componenta trebuie sa includă nativ un broker distribuit de mesaje pentru procesare date și fluxuri de evenimente în timp real, care sa permită:

- Un model de mesagerie de tip publish-subscribe distribuit pe un număr mare de noduri;
- Partiționarea cozilor de mesaje;
- Replicarea mesajelor atat pe mai multe noduri din cadrul aceluiași cluster, cat si in cadrul unor clustere diferite (disaster recovery);
- Sa permită organizarea cozilor de mesaje in colecții diferite, cu politici de retentie diferite;

- Sa permită crearea de politici de retenţie a mesajelor pe o perioada de timp configurabila;
- Funcţionare continuă şi în cazul în care oricare din nodurile clusterului se defectează;
- Stabilirea de cote de utilizare a reţelei si a CPU;
- Sa ofere garanţii de livrare a mesajelor At most once, At least once, Exactly once;
- Sa includă algoritmi de compresie a datelor pentru reducerea traficului de retea;
- Sa permită criptarea mesajelor stocate;
- Sa includa mecanisme de autentificare a consumatorilor si autorizare a accesului la cozile de mesaje;
- Sa ofere capabilitati de monitorizare a parametrilor de funcţionare a clusterului, cozilor de mesaje, consumatorilor si producatorilor de mesaje;
- Sa permită streaming-ul datelor primite către alte sisteme;
- Sa permită utilizarea limbajului SQL pentru interogarea fluxurilor de date in timp real. Interogarile SQL pot fi atat continue, cat si one-off;
- Sa includa un instrument de vizualizare cozilor de mesaje si monitorizare a parametrilor de functionare;
- Sa ofere un API de tip REST pentru dezvoltarea aplicatiilor ce interactioneaza cu brokerul de mesaje.

4.3.8 Componenta de integrare şi gateway pentru servicii web

Aceasta componenta va asigura interconectarea sistemului informatic integrat cu aplicaţiile/sistemele informatice ale altor instituţii, precum şi securizarea serviciilor web. Avand in vedere rolul important al acestei componente se doreste implementarea unei solutii care sa satisfaca cel putin urmatoarele cerinte tehnice:

- **Servicii tip flux de lucru (proces)** - asigură capacităţile de control necesare organizării fluxului de lucru şi a interacţiunii între aplicaţii. Fluxurile de lucru sunt reprezentate ca procese de business - o colecţie de sarcini sau activităţi structurate, ce descriu un scenariu de utilizare şi produc un rezultat sau un serviciu specific;
- **Servicii de comunicare între aplicaţii** - permit schimbul de informaţii între modulele aplicative interne ale sistemului şi sistemele externe;
- **Servicii de transformare de date** - permit transferul de date externe, în diferite formate, astfel:
  - Trebuie transformate şi armonizate datele de la diferite surse, pentru a putea fi compatibile cu modelul de date intern;
  - Se vor defini şi aplica reguli de calitate a datelor;
  - Se va defini şi implementa un mecanism de tratare a erorilor;
- **Servicii de tip registru de servicii** - permite publicarea şi accesarea automată a celorlalte servicii operaţionale oferite pe magistrala de servicii;

Componenta trebuie sa asigure urmatoarele:

- va oferi o arhitectura de tip proxy de servicii web - de tip Web Services si API - Application Programming Interface cu functionalitati de transformare de date si securizare a mesajelor;
- Pentru a asigura un nivel ridicat de flexibilitate in modelarea fluxurilor de schimb de date, componenta de integrare şi transformare va suporta urmatoarele modele de comunicare: sincron

cerere/răspuns, asincron one-to-one, asincron one-to-many, asincron cerere/răspuns (synchronous-to-asynchronous bridging);

- Toate modelele de comunicare trebuie sa asigure atat persistenta mesajelor cat si garantarea livrarii acestora;
- Trebuie includa capabilităţi extinse de transformare şi dirijare a datelor bazate pe conţinutul transportat;
- Sa permită crearea de API-uri de tip REST, SOAP, GraphQL, WebSockets, Streaming;
- Crearea API-urilor trebuie sa poata fi facuta folosind un editor web ce ruleaza pe browserele majore Chrome, Edge, Firefox, Safari;
- In procesul de crearea a unui API trebuie sa:
  - permită aplicarea de limite cu privire la numarul maxim de cereri permise pe secunda si minut (rate-limiting);
  - permită configurarea modului de autentificare catre serviciul tinta;
  - permită load-balacing si failover catre serviciul tinta, pentru a putea balansa incarcarea si a asigura redundanta mai multor instante de serviciu;
  - permită maparea erorilor serviciului tinta catre erori de API definite de creatorul API-ului respectiv;
  - permită crearea de reguli de suspendare a API-ului in cazul in care serviciul tinta nu mai este disponibil;
  - permită gestionarea de versiuni multiple ale unui API;
  - Includă mecanisme de testarea a API-ului respectiv;
  - Includă mecanisme de colaborare intre dezvoltatori in procesul de crearea a API-ului;
  - Permită documentarea operatiilor aferente API-ului;
  - Permită alterarea fluxurilor de standard cerere, răspuns si eroare, cel puţin capabilitatea de a adaugă headere definite de utilizator, parametri, transformare implicita XML/JSON, rescriere URL, validare schema de date, politici CORS;
  - Permită configurarea securitatii API-ului:
    - SSL/TLS;
    - Autentificare de tip Basic, cu certificat, cheie API, OAuth;
    - Accesul la operatiile API-ului in functie de rolul utilizatorului;
- API-urile dezvoltate vor avea un ciclu de viata configurabil de utilizator care sa permită trecerea API-ului in productie, retragerea controlata din productie, blocarea si suspendarea acestuia;
- Sa ofere capabilitati de clustering si load-balancing prin deployment-ul API-urilor pe mai multe noduri de procesare;
- Sa permită crearea de aplicaţii complete prin gruparea API-urilor relevante aplicaţiilor, cat si crearea de fluxuri de orchestrare, procesare si transformare ce vor fi expuse prin intermediul API-urilor respective:
  - Să permită generarea automata de SDK-uri de dezvoltare pentru o aplicaţie in cel puţin doua limbaje de programare majore: Java, JavaScript, .NET, Python, C;

- Să includă capabilităţi de testare vizuala a API-urilor din cadrul unei aplicaţii, fara a avea cunoştinţe de programare;
- Să asigure modelarea şi execuţia fluxurilor de schimb de date in mod vizual;
- Să permită combinarea de multiple servicii web sincrone şi asincrone în cadrul fluxurilor de procese colaborative şi tranzacţionale;
- Să asigure filtrarea şi transformarea mesajelor XML utilizând cel puţin următoarele standarde deschise W3C Extensible Stylesheet Language Transformation (XSLT) şi xQuery (XML Query);
- să asigure interconectarea la sistemele externe de tip SOAP, REST, cozi de mesaje, baze de date;
- Să permită dezvoltarea de conectori catre sisteme noi;
- Să permită depanarea vizuala a unui flux de date modelat;
- Să permită crearea de job-uri programate in cadrul unui flux de date, cu executie la un anumit interval de timp;
- Să asigure securitatea serviciilor Web pe baza specificaţiilor standardelor WS-Security, WS-Policy şi WS-Security Policy pentru a asigura criptarea / decriptarea mesajelor în vederea asigurării confidenţialităţii mesajelor transportate si semnarea / verificarea digitală a mesajelor în vederea asigurării integrităţii şi non-repudierii mesajelor;
- Să permită monitorizarea si administrarea fluxurilor de date aflate in productie folosind un instrument vizual;

- Sa includă mecanisme de Continuous Integration (CI) si Continuous Deployment (CD);
- Sa includă capabilităţi de creare de API-uri pentru servicii de tip flux de evenimente:
  - sa permită definirea atat vizuala cat si programatica de surse si destinatii de date de tip flux de evenimente: cozi de mesaje, websocket, HTTP, TCP, baze de date, email;
  - sa permită extragerea de evenimente din surse de date de tip flux de evenimente in format JSON, XML, CSV, TXT, binar;
  - Sa permită aplicarea de operatori pentru interogarea si transformarea fluxului de evenimente si direcţionarea acestuia către un sistem destinaţie;
  - Sa permită realizarea de agregări pe baza atribute aplicate fluxului de date sursa;
  - Sa permită generarea de evenimente noi pe baza schemei de date a evenimentelor sursa;
  - Sa permită filtrarea si alterarea schemei de date a evenimentelor;
  - Sa permită reordonarea evenimentelor pe baza de diverse atribute;
  - Sa permită combinarea de evenimente din mai multe surse;
  - Sa permită limitarea numarului de evenimente transmis catre destinatie;
  - Sa permită identificarea de comportamente pe baza regulilor definite de utilizator in evenimentele sursa;
  - Sa permită limitarea ratei de salvare a evenimentelor in sistemele destinatie (rate-limiting);
  - Sa permită procesarea paralela a evenimentelor sursa pe baza regulilor definite de utilizator;
  - Sa permită crerea de tabele virtuale pe baza schemei de date a evenimentelor sursa, cu posibilitate de interogare folosind un limbaj similar SQL, adaugare, stergere, join si modificare de inregistrari;

- Sa permită generarea de evenimente programate in timp, la intervale regulate;
- Sa permită definirea de functii definite de utilizator utilizand un limbaj de programare si utilizarea acestora pentru manipularea evenimentelor sursa;
- Sa includă o librărie de funcții predefinite ce pot fi utilizate in manipularea evenimentelor sursa: operații matematice, manipularea datelor de tip text, operații pe șiruri si mape de date, aplicare de pattern-uri regex, manipularea înregistrărilor de tip data si timp, conversia unităților de măsura, deduplicare înregistrări, manipulare fișiere;
- Sa permită stocarea evenimentelor in baze de date;
- Sa permită conversia formatului evenimentelor pentru transmiterea in sistemul destinatie;

- Sa permită monitorizarea si diagnoza rapida a API-uilor aflate in productie fara cunostinte de programare: numar de apeluri, numar de erori, latenta, device-uri folosite de clienti, timpul de răspuns al sistemelor ținta, număr de tranzacții pe secunda, cele mai utilizate API-uri, cei mai activi consumatori de API;
- Sa permită monitorizarea detaliata a unui flux de date.

4.3.9 Componenta Big Data

Platforma de tip Big Data trebuie sa fie o platforma matura, sigura si scalabila, bazată pe un sistem distribuit de fișiere, care să permită stocarea și procesarea unor volume nelimitate de date cu ajutorul mai multor soluții care rulează integrat.

Modelul de licențiere trebuie să asigure posibilitate de transfer a soluției pe alte servere decât cele pe care se va instala aceasta inițial sau înlocuire a unora dintre ele, după necesități.

Avand in vedere rolul important al acestei componente se doreste implementarea unei solutii care sa satisfaca cel putin urmatoarele cerinte tehnice:

- O arhitectura bazata integral pe containere de tip Docker sau echivalent pentru a asigura flexibilitate maxima in ceea ce privește migrarea si scalabilitatea tuturor serviciilor platformei;
- Configurarea numarului de replici disponibile pentru un serviciu;
- Distributia automata a replicilor unui serviciu pe serverele din cadrul clusterului, cu posibilitatea de a defini reguli de plasament ce permit includerea/excluderea anumitor servere;
- Migrarea automata a unei replici daca un server nu mai este disponibil;
- Crearea unui număr nelimitat de rețele virtuale separate la nivel logic (Software-Defined Networking) si asocierea serviciilor cu una sau mai multe retele;
- Definirea si atașarea de volume de stocare la serviciile din cadrul clusterului;
- Limitarea consumului de resurse la nivelul unui serviciu (CPU, RAM);
- Includa o componenta nativa de tip load-balancer si reverse-proxy pentru distribuirea cererilor venite din exterior catre una din replicile unui serviciu;
- Colectarea log-urilor de catre sisteme specializate pentru analiza si corelare;
- Capacitate virtual nelimitată de stocare și procesare a datelor prin scalarea pe verticală și orizontală;
- Management unic pentru toate componentele platformei; acest management va trebui să poată fi făcut prin intermediul unei interfețe grafice de tip web care sa:

- permită vizualizarea si gestiunea clusterelor;
- permită vizualizarea si gestiunea replicilor unui serviciu din cadrul clusterului, inclusive configurarea numarului de replici ;
- permită configurarea variabilelor de environment, a retelelor atasate, a porturilor expuse, a limitelor de resurse (CPU, RAM) si a volumelor atasate;
- permită administratorului vizualizarea log-urilor tuturor replicilor unui serviciu;
- permită administratorului sa deschida o consola virtuala interactiva pentru accesarea containerului unui serviciu si executia de comenzi in cadrul containerului;
- permită gestiunea retelelor virtuale;
- permită definirea si deployment-ului serviciilor din cadrul clusterului pe baza de template-uri predefinite;
- marcarea unui server ca fiind in mod mentenanta, urmand ca toate serviciile aflate pe acesta sa migreze automat pe celelalte servere disponibile din cadrul clusterului;

- Pentru a putea fi efectuate operațiuni de provizionare și administrare în mod programatic, soluția va trebui să ofere instrumente de tip linie de comanda pentru funcțiile de management ale platformei;
- Sa includa un sistem de fișiere distribuit, de tip HDFS sau echivalent, ce asigura redundanta maxima a datelor stocate. Acesta va trebui să ofere scalabilitate nelimitată prin adăugarea de noi servere fizice cu capacitate locală de stocare;
- sa permită procesarea datelor stocate in cadrul sistemului de fisiere distribuit folosind algoritmi de tip MapReduce sau echivalent;
- Autentificare prin integrare cu servere LDAP si Kerberos;
- Controlul accesului la datele stocate, la nivel de directoare si fisiere;
- Criptarea transparenta a datelor stocate;
- Sa ofere capabilitati de stocare a fisierelor de mari dimensiuni si mecanisme de accelerare a accesului sistemelor externe la aceste tipuri de fisiere;
- Toate componentele platformei vor putea fi configurate în arhitecturi de tip înaltă disponibilitate;
- Sa includa nativ o bază de date structurate, optimizata pentru interogari pe volume mari de date, integrata cu restul componentelor platformei Big Data, care să ofere cel puțin următoarele:
  - sa fie o baza de date de tip OLTP, cu suport pentru tranzactii si operatii de tip create/update/delete;
  - să ofere suport complet pentru standardul SQL ANSI-99;
  - sa permită ingestia datelor folosind mecasnisme de tip streaming;
  - sa permită crearea de indecsi pe unul sau mai multe coloane din cadrul unei tabele;
  - sa ofere drivere JDBC si ODBC;
  - sa permită partitionarea tabelelor;
  - sa ofere capabilitati de incarcare in memorie a datelor utilizate frecvent;
  - sa permită procesarea datelor din baza de date folosind algoritmi de tip MapReduce sau echivalent;

- sa includa capabilitati de Machine Learning, cel putin algoritmi de clasificare binara si multi-clasa, regresie, clustering;
- sa permită crearea de interogari SQL de tip long-running, care sa genereze notificari cu privire la modificari asupra datelor;
- sa permită dezvoltarea de noi functii si proceduri SQL in functie de nevoi;
- sa ofere mecanisme de securitate, cel putin: utilizatori, autentificare, SSL/TLS, auditarea actiunilor utilizatorilor;
- sa ofere mecanisme de criptare transparenta a datelor;
- sa ofere mecanisme de backup si recovery;
- sa ofere mecanisme de calcul al statisticilor pentru o tabela;
- sa ofere API-uri de dezvoltare pentru limbajele Java, .NET si REST;

- Sa includa nativ o bază de date nestructurate (documente office, email-uri, imagini, audio, video, fisiere log, etc.), integrata cu restul componentelor platformei Big Data, care să ofere cel puțin următoarele:
  - stocarea datelor intr-un model dinamic bazat pe concepte, relatii si proprietati aferente conceptelor si relatiilor;
  - o gama larga de tipuri de date suportate: string, char, byte, float, double, integer, long, array, list, map, json, blob, spatial;
  - stocare a datelor in mod distribuit, pe mai multe noduri si partitii, pentru a permite interogarea paralela a cantitatilor mari de date;
  - sa permită procesarea datelor din baza de date folosind algoritmi de tip MapReduce sau echivalent;
  - acces la date pe baza de utilizatori și roluri, având în vedere cel puțin următoarele aspecte: controlul accesului la nivelul tuturor obiectelor din cadrul modelului conceptual: concepte, relații și proprietăți, precum și auditarea operațiunilor efectuate;
  - interogarea datelor folosind limbajul SQL, pentru rularea de analize folosind instrumente de raportare traditionale;
  - un limbaj standardizat de interogare a datelor nestructurate care sa permită rularea de interogari asupra conceptelor, relatiilor dintre ele si a atributelor asociate care sa:
    - nu impuna limite cu privire la adancimea de parcurgere a relatiilor dintre unul sau mai multe conceptele;
    - suporte căutări avansate de tip full-text: wildcard search, fuzzy search, range search, phrase search, boost, proximity search, operatori logici si grupari de operatori;
    - suporte cautari spatiale cel putin de tip contains si intersects;
    - fie extensibil, pentru a permite dezvoltarea de functii si proceduri in functie de nevoi;
    - permită rularea de algoritmi de procesare de tip centrality, page rank si shortest path.

4.3.10 Componenta de analiză și prognoză

Aceasta componentă va asigura generarea rapoartelor și va permite permite construirea, configurarea și generarea de rapoarte dinamice pe baza tuturor datelor înregistrate în sistem/baza de date și respectiv salvarea în diferite șabloane și formate pentru utilizări viitoare. In afara rapoartelor "standard" (rapoarte predefinite) prin intermediul modulului se vor putea realiza, de catre anumiti utilizatori, rapoarte de tipul "ad-hoc" pentru identificarea si analizarea anumitor situatii punctuale; rapoartele ad-hoc se vor putea transforma in rapoarte "standard", printr-o simpla operatiune de "publicare", fara a fi nevoie de redezvoltarea lor.

Componenta va prelua si va consolida datele din modulele operationale si alte surse de date, in cadrul Platformei Big Data. Preluarea datelor din modulele operationale se va face utilizand o unealta dedicata, de tip ETL. Avand in vedere rolul important al acestei componente se doreste implementarea unei solutii care sa satisfaca cel putin urmatoarele cerinte tehnice:

- Sa ofere compatibilitate cu baza de date si platforma Big Data ofertate in cadrul solutiei;
- Sa ofere conectori dedicati pentru diverse tipuri de surse de date (baze de date de diverse tipuri, fisiere de tip xls, csv, txt);
- Sa permită definirea proceselor de extragere - transformare - încărcare dintr-o interfața web, prin actiuni de tip drag & drop;
- Sa ofere suport pentru date comprimate, cel putin tar, zip, gzip, bzip2, xz, 7z, cpio
- Sa ofere suport pentru procesarea datelor in formatele binar, CSV, JSON, XML, Excel, date de tip logging (cel putin Common Log Format, Apache Error Log Format, Grok, log4, Apache Access Log Custom Format, RegExp)
- Sa ofere suport pentru pastrarea pozitiei existente in cadrul sursei de date pentru oprirea si continuarea mai tarziu a proceselor din punctul in care au ramas.
- Sa permită executarea de job-uri multiple în mod concurent;
- Sa permită procesarea înregistrărilor respinse sau care au generat erori;
- Să includa mecanisme de tip detectare a modificării datelor (Changed Data Capture);
- Să permită definirea și incorporarea de componente reutilizabile suplimentare. Aceste componente trebuie să acopere majoritatea tipurilor de transferuri de date: din fișiere în suport relațional, între tipuri diferite de baze de date relaționale, etc.
- Procesele de extracție, transformare și încărcare să poată fi definite vizual, prin selectarea și maparea vizuală a elementelor implicate.
- În cadrul mapărilor de date, să se permită definirea de filtre și de restricții asupra câmpurilor implicate;
- Să permită consolidarea pașilor de integrare de date sub forma unor fluxuri cu ramificare pe baza unor condiții si apelul altor fluxuri;
- Mediul de lucru să nu necesite cunoștințe avansate de programare;
- Să permită extinderea conectivității sistemului prin adăugarea de noi surse de date;

- Sa permită gestionarea următoarelor cerințe de proces: compresie/decompresie, mascare valori sensibile, conversie tip și/sau format date, manipulare și executare de operații aritmetice pe seturi de date, apeluri HTTP, filtrare, validare;
- Sa includa mecanisme de clustering si load-balancing pentru distribuirea automata a fluxurilor de date catre mai multe noduri de procesare;
- Sa includa capabilitati de monitorizare a fluxurilor de date aflate in executie, cu afisarea cel putin a numarului inregistrari procesate, inregistrari cu eroare, inregistrari aflate in asteptare;
- Sa includa un mecanism de generare evenimente pentru procesarea asincrona a inregistrarilor intr-un flux configurat;
- Sa permită integrare cu sisteme de tip LDAP pentru autentificarea utilizatorilor;
- Sa permită definirea de fluxuri de tip mircoservicii
- Sa permită initierea unui flux prin intermediu unui serviciu de tip REST
- Preluarea datelor se va face in mod automat, programat la anumite intervale de timp sau in functie de anumiti parametri;
- Datele preluate din modulele operationale vor fi incarcate in depozitul Big Data, in structuri dedicate, tabelare, pentru interogari rapide;
- Pe parcursul procesului de preluare si incarcare a datelor vor fi efectuate operatiuni de curatare/normalizare a datelor; eventualele erori identificate vor fi transmise spre remediere, considerand si optiunea de oprire sau continuare a procesului de prelucrare a datelor in functie de impactul pe care aceste erori il poate avea asupra consistentei rapoartelor;
- Accesul la date se va face doar prin intermediul interfetei de raportare;
- Rapoartele vor fi dezvoltate pe baza datelor stocate la nivelul Platformei Big Data, dar si din alte surse de date ce pot fi relevante (fisiere, baze de date relationale)
- Sa suporte un numar mare de conectori pentru cele mai cunoscute sisteme de baza de date.
- Rapoartele pot fi programate pentru a rula automat si a fi transmise pe email la factorii interesati sau pot fi accesate prin intermediul interfetei de raportare;
- Rapoartele și analizele vor permite să fie clasificate pe diferite categorii. Sistemul trebuie să gestioneze accesul grupurilor de utilizatori și sau utilizatorilor individual la anumite categorii de rapoarte.
- Modulul de raportare trebuie sa indeplineasca urmatoarele cerinte minime:
  - Sa permită configurare de tip „point-and-click";
  - Sa ofere funcționalități de navigare ghidată pentru utilizatorii finali, cu posibilități multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât și pentru grafice;
  - Sa permită combinarea rezultatelor obținute din surse de date diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
  - Sa permită datelor în format tabelar al informațiilor afișate;
  - Sa permită crearea de rapoarte utilizand un editor vizual de interogari, dar si scrierea manuala a interogarilor SQL complexe;
  - Sa permită salvarea interogarilor SQL ca notite pentru utilizare ulterioara;

- Sa permită definirea de tablouri de bord și includerea rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
- Sa permită modificarea tablourilor de bord sau a rapoartelor, posibilitatea de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
- Sa permită parametrizarea tablourilor de bord si a datelor afisate in functie de diverse criterii relevante;
- Accesul la informație se va realiza printr-un nivel de metadate care va ascunde utilizatorilor finali complexitatea structurilor fizice de date;
- Sa permită crearea de coloane in cadrul tabelelor virtuale, bazate pe formule de calcul;
- Sa permită crerea de modele virtuale de date pe baza unei interogari; sa permită utilizarea unui model virtual ca sursa de date pentru interogari noi;
- Sa permită includerea dashboard-urilor in alte aplicatii;
- Sa includa un mecanism de caching al datelor utilizate frecvent, pentru accelerarea timpului de livrare al rapoartelor;
- Sa permită configurare cache-ului pentru o anumita interogare, pentru accelerarea livrarii rapoartelor de utilizeaza date care nu se schimba frecvent;
- Sa includa un mecanism de analiza si vizualizarea automata a datelor din cadrul unei tabele, cu propunerea automata a celor mai relevante vizualizari pentru datele din tabela respectiva (ex: histograme de valori, harti, linii de trend, agregari etc.) ;
- 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;
- Se permită restrictionarea accesului la date in functie de utilizator si grup de utilizatori. Restrictionare accesului trebuie sa poata fi facut la nivelul unei surse de date, tabela sau anumite randuri si coloane dintr-o tabela;
- Sa permită restrictionarea accesului la interogari, tablouri de bord si rapoarte, atat la nivel de utilizator, cat la nivel de grup de utilizatori;
- Sa permită auditarea actiunilor utilizatorilor, inclusiv auditarea accesului la date, precum si vizualizarea informațiilor de audit din cadrul zonei de administrare;
- Sa permită integrarea cu servere LDAP pentru utilizatori si grupuri de utilizatori;
- Sa suporte unul din standardele SAML, JWT sau OAuth pentru integrarea cu platforme de Single Sign-On;
- Accesarea datelor de pe platforme relaționale, multidimensionale, foi de calcul sau din cadrul platformei Big Data;
- Interacțiunea utilizatorilor finali cu aplicația se va face într-o interfață de tip web, fără a necesita instalarea de componente software suplimentare pe calculatoarele utilizatorilor;
- Va expune o interfață de administrare atât a drepturilor de acces la diferite zone, cât și a drepturilor de acces pe diferite tipuri de acțiuni;

- Va permite afisarea datelor atat sub tabelara cat si grafica: bar chart, stacked bar chart, histogram, line chart, gauge, donut, waterfall, pivot table, funnel chart, pie chart, scatter plot, map;
- Va permite definirea de borne personalizate cu denumire personalizata si data calendaristica, pentru a marca diverse evenimente importante in timp. Bornele vor fi afisate automat in cadrul vizualizarilor din tabloul de bord ce afiseaza informații legate de data/timp;
- Va oferi capabilități de drill-down (navigare în adâncime) pe diferite nivele de agregate;
- Va permite acces la surse de date multiple, în mod transparent pentru utilizatorul final;
- Va oferi utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât și în aplicația de analiză și raportare;
- Va dispune de mecanisme de alertare pentru utilizatorii finali;
- Va oferi utilizatorilor finali posibilitatea subscrierii la alertele definite;
- Să nu necesite replicarea datelor pe un server separat, ci să folosească capabilitățile bazelor de date sursa;
- 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);
- Sa permită filtrare consecutivă a segmentelor de date analizate („slice & dice");
- Să permită tuturor utilizatorilor crearea sau modificarea de rapoarte, analize ad-hoc și tablouri de bord, acordarea drepturilor specifice (consultare, creare de obiecte etc.) urmând a fi făcută de către administratori;
- Sa permită rularea de scenarii de tip "what-if";
- Sa permită definite de sabloane de filtre ce pot fi aplicate de utilizator asupra rezultatelor unei interogari;
- Sa permită definirea de sabloane de agregari ce pot fi aplicate de utilizator asupra rezultatelor unei interogari;
- Sa ofere un mecanism de federare a interogarilor pentru combinarea datelor din mai multe surse de date in cadrul aceleiasi interogari SQL (ex. join-ul tabelelor din diferite baze de date intr-o singura interogare SQL).

Pe lângă rapoartele operationale descrise mai sus, sistemul va include o platforma specializată pentru analiza avansată și prognoza, ce va utiliza datele stocate in cadrul platformei Big Data.

Modulul pentru analiza avansată trebuie sa indeplineasca urmatoarele cerinte:

- Sa includa nativ un motor pentru procesare analitică de volume mari de date în memorie, ale cărui funcționalități să permită:
  - Acces la datele din cluster prin interogare de tip standard SQL;
  - Librarie de Machine Learning care să includă cel puțin:
    - Algoritmi de clasificare, regresie, clustering și collaborative filtering ;
    - Analiza și caracterizare seturilor de date (featurization): extragerea (feature extraction), transformarea, selecția și reducerea dimensiunilor seturilor de date;

- Posibilitatea de a construi fluxuri de procesare, transformare si machine learning;
- Capabilitati pentru construcția și tuning-ul fluxurilor de machine learning;
- Persistenta: salvare și încărcare algoritmi, modele și fluxuri;
- AutoML;

- Procesare date în limbaje multiple inclusiv Java, Scala, Python si R;
- Procesare distribuită de date pe bază de cache în memoria fiecărui nod;
- Capabilități de streaming;
- Reprezentare date tip graf;

- Sa includa nativ un motor distribuit de interogare federata a datelor, pentru analiza simultana a datelor din mai multe surse de date, care sa permită cel putin:
  - conectarea mai multor surse de date, cel putin baze de date, fisiere, cozi de mesaje;
  - utilizarea nativa a bazei de date structurate si a bazei de date nestructurate din cadrul platformei Big Data;
  - suport complet pentru standardul SQL;
  - posibilitatea de a efectua operatii de tip join pe tabele apartinand unor surse diferite;
  - sa ofere drivere (ex. JDBC, ODBC) pentru conectarea sistemelor externe;
  - Sa ruleze in mod distribuit, pentru a putea efectua operatii pe seturi mari de date ;
  - Sa ofere conectivitate cu o gama variata de sisteme de baze de date relationale, columnare, NoSQL, BigData, CSV, cozi de mesaje si multe altele ;
  - Sa ofere capabilitati de analiza avansata a datelor federate, cel putin utilizand functii pentru: sumarizare, machine learning, date spatiale, JSON ;
  - sa permită creara de view-uri simple si view-uri materializate ;
  - sa permită vizualizarea planului de executie pentru o interogare SQL ;
  - sa ofere un instrument vizual de monitorizare a interogarilor efectuate, cu afisarea planului de executie si a timpului consumat;
- Sa includa nativ un instrument colaborativ pentru elaborarea proceselor de analiza avansata si rularea experimentelor de tip data science, care sa permită:
  - crearea de experimente folosind limbaje de programare de larga utilizare: Python, Scala, R;
  - realizarea de analize specifice asupra datelor existente, cu posibilitati de vizualizare sub diferite forme grafice: bar chart, line chart, distributie de valori, matrice de corelare a variabilelor, scatter plot, box plot, heatmap, histograme de valori, pie chart, 3D, grafice animate pentru afisarea progresului in timp;
  - publicarea rezultatelor obtinute ca aplicatii web.

4.3.11 Componenta GIS

Componenta geospațială trebuie să asigure accesul corect la datele GIS indiferent de sistemul de coordonate asociat acestor date. Această componentă trebuie să permită transcalculul automat al coordonatelor între sistemele de coordonate (internaționale, naționale și/sau locale, fie că sunt predefinite în aplicație sau definite de utilizator).

Dezvoltarea ulterioară a funcțiilor la nivelul componentei geospațiale (funcţii suplimentare sau interfeţe utilizator specializate) să se facă prin medii de dezvoltare (programare) standard, fără costuri suplimentare pentru specializări în limbaje de programare de tip proprietar.
Componenta geospațială trebui să permită:

a) Publicarea de servicii GIS in arhitectura REST sau SOAP in cadrul unui portal web
b) Portalul trebuie sa permită vizualizarea hartilor publicate, impreuna cu straturile si metadatele aferente
c) Pentru o harta publicata in portal, utilizatorii sa poata:
    a. cauta obiecte de interes dupa numele acestora
    b. naviga in cadrul hartii prin functii de tip pan, zoom, selectare arie de interes
    c. naviga in cadrul hartii prin introducerea unei perechi de coordonate spatiale (latitudine, longitudine)
    d. vizualiza straturile aferente hartii, cu posibilitate de ordonare si configurare transparenta
    e. adaugă straturi suplimentare in funcție de nevoi
    f. tipări zona de harta afișata pe ecran, cu posibilitatea de configura rezolutia, formatul paginii si alte informații necesare: legenda, scara, font
    g. măsura distanta
    h. distribui harta pentru includerea in aplicații externe
    i. vizualiza metadatele asociate hartii si ale straturilor spațiale incluse
    j. vizualiza puncte de interes de pe harta impreuna cu metadatele asociate
    k. exporta zona de harta afișata in formate recunoscute: GeoJSON, GML, KML, CSV, Shapefile
    l. realiza interogări complexe in mod vizual dupa metadatele asociate obiectelor din cadrul hartii prin utilizarea de operatori logici (AND, OR, NOT)
    m. interoga obiectele din cadrul hartii prin desenarea de catre utilizator a unei zone folosind forme geometrice de tip cerc, dreptunghi
d) Portalul sa permită realizarea de tablouri de bord interactive prin includerea de widget-uri de tip grafic, tabel, harta si indicatori de performanta
e) Sa includa un motor de date spatiale care sa:
    a. organizarea modului de lucru in proiecte;
    b. permită crearea de straturi spatiale folosind baze de date si fisiere;
    c. pentru un strat spatial sa permită configurarea sistemului de coordonate, stilul de afisare si metadatele aferente;
    d. sa permită crearea de straturi spatiale ce grupeaza mai multe sub-straturi spatiale;
    e. sa permită crearea de straturi spatiale de tip raster;
    f. sa permită crearea de straturi spatiale de tip reverse-proxy catre alte servere ce contin informații spatiale spatiale;
    g. sa includa mecanisme de caching pentru optimizarea performantei datelor spatiale si a straturilor raster;
    h. sa permită publicarea hartilor si a straturilor spațiale in formate recunoscute in industrie: WMS, WFS, WCS, WMTS;

i. sa permită realizarea si publicarea de operații spațiale in format WPS
j. sa ofere un mecanism avansat securitate bazat pe utilizatori, grupuri de utilizatori si roluri care sa:
    i. permită restrictionarea accesului la straturile spatiale in functie de rolurile asociate;
    ii. permită restrictionarea accesului la serviciile WMS, WFS, WCS, WMTS, WPS;
    iii. restrictioneze accesul la datele publicate pe baza de autentificare folosind nume de utilizator si parola si certificat;
    iv. permită integrarea cu servere LDAP;
    v. permită integrarea cu mecanisme de tip Single Sign-On;
k. sa permită rularea in cluster, cu mecanisme de balansare a incarcarii pe mai multe noduri pentru a mari capacitatea in functie de numarul de cereri;
l. sa permită rularea in mediu containerizat, precum si pe sisteme de operare Linux si Windows
m. sa oferea API-uri de dezvoltare de tip REST pentru dezvoltarea de aplicatii.

f) Conectarea la un serviciu de imagini satelitare cu acoperire globala de inalta rezolutie (< 3 metri) gen GoogleEarth, BingMaps sau echivalent, pentru a permite utilizatorului sa vizualizeze si editeze propriile date suprapuse peste imagini satelitare, fara a fi nevoit sa achizitioneze aceste imagini. Se va nominaliza in oferta aceste servicii. Conectarea la volume mari de date şi gestiune în aceeaşi fereastră hartă de surse multiple de date de la diferite instituţii;
g) Definirea de hărţi tematice;
h) Sistemul trebuie sa permită administrarea numai printr-o interfata de tip browser web. Întreaga interfata a sistemului trebuie sa se bazeze pe o harta de fundal care sa gestioneze informațiile georeferentiate.
i) Componenta geospațială trebuie sa permită selectia straturilor din hartile afisate;
j) Sa permită editarea straturilor vectoriale precum si crearea de straturi vectoriale noi folosind un editor specializat care sa:
    a. utilizeze straturile spatiale stocate in motorul de date spatiale;
    b. permită lucrul cu date de tip vector si raster;
    c. includa instrumente pentru digitizarea straturilor spatial;
        i. desenare elemente folosind punct, linie, poligon, cerc, elipsa, dreptunghi, decupare poligon, umplere poligon, split, merge;
        ii. mutare, rotire, redimensionare, simplificare geometrie element;
        iii. stergere elemente;
        iv. snapping in cadrul procesului de digitizare;
    d. includa instrumente pentru lucrul cu straturi de tip raster;
    e. utilizeze protocoale si formate standard definite de OGC (Open Geospatial Consortium): WMS, WMTS, WFS, WFS-T, WCS, WPS, GML;
    f. permită incarcarea datelor GPS in format GPX (GPS eXchange format);

4.3.12 Stocare centralizata profile utilizatori

Pentru optimizarea costurilor autoritatea contractantă dorește reutilizarea licențelor existente descrise la capitolul 3.8 aferente soluției de stocare a profilelor utilizatorilor, dar acest aspect nu trebuie considerat ca fiind obligatoriu.

Soluția de stocare a pofilelor de utilizatori trebuie să permită:

- Stocarea utilizatorilor să se realizeze în mod centralizat;
- Sa permită accesarea datelor despre utilizatori atât din baze de date cât și din directoare LDAP, cu posibilitatea de agregare selectivă a pofilelor și expunerea acestor informații în format LDAP către alte sisteme;
- Să asigure securitatea datelor private;
- Pentru asigurarea unui nivel ridicat de accesibilitate, sa ofere o interfață grafica web pentru consultarea datelor despre utilizatori și operarea componentei
- Să reprezinte sursa unica de profile de utilizatori pentru autentificarea in toate componentele funcționale;
- Directorul de utilizatori centralizat trebuie sa fie conform cu standardul LDAP v3 sau echivalent
- Componenta trebuie sa permită integrarea cu alte sisteme fără a utiliza agenți
- Sa permită protejarea datelor la acces – autentificare la interogarea directorului (nume utilizator și parola)
- Sa permită filtrarea accesului astfel încât fiecare utilizator sa poată citi doar datele de care are nevoie
- Filtrarea trebuie sa se poată realiza la nivel de atribut LDAP
- Sa permită criptarea parolei fiecărui utilizator in parte
- Sa permită integrarea cu celelalte componente ale sistemului general astfel încât sa existe o singura sursa de utilizatori pentru toate nivelele (aplicație, baza de date, etc)
- Sa permită rularea pe sistemul de operare ofertat.

Pentru a asigura un nivel de securitate avansata se vor instala si configura doua instanțe separate pentru stocarea pofilelor de utilizatori împărțite după tipul de utilizatori :

  - O zona pentru utilizatori externi persoane fizice si juridice
  - O zona pentru utilizatori interni ai CNAIR si ale partenerilor care consuma serviciile web expuse de către sistemul de tarifare rutiera – fie pentru roviniete si peaj , fie cele de tarifare per distanta parcursa, precum si a accesului administratorilor la sistemele ce compun întreg sistemul informatic, acolo unde acestea pot fi integrate cu un sistem de tip LDAP.

4.3.13 Componenta de gestiune acces utilizatori

Sistemul informatic va fi compus din mai multe componente, fiecare îndeplinind cerinţe funcţionale si tehnice specifice. Pentru a se asigura un control al accesului centralizat la nivelul portalului extern, a nucleului central precum si la serviciile web, unificarea experienţei de utilizare dar şi pentru a creste nivelul de securizare şi a scădea costurile operaţiunilor administrative legate de controlul accesului la aplicaţiile şi componentele sistemului, se doreşte implementarea unei componente de securizare a accesului la interfeţe web si servicii web in mod centralizat.

4.3.13.1 Soluţie gestiune acces utilizatori aplicaţii web si servicii web

Pentru optimizarea costurilor autoritatea contractanta doreşte reutilizarea licenţelor existente descrise la capitolul 3.8 aferente solutiei de gestiune a accesului utilizatorilor la resurse, dar acest aspect nu trebuie considerat ca fiind obligatoriu.

Având in vedere rolul important al acestei componente se doreşte implementarea unei soluţii care sa satisfacă cel puţin următoarele cerinţe tehnice:

- Sa protejeze resursele împotriva acceselor neautorizate - atât din interiorul cat şi din exteriorul retelei;
- Nici o resursa web din interiorul sistemului nu trebuie sa poată fi accesata direct din exterior, orice acces realizându-se prin intermediul serverelor web proxy;
- Sa integreze controlul accesului pentru componentele sistemului;
- Sa ceara utilizatorilor sa introducă date de identificare pentru accesul la aplicaţii;
- Sa permită administratorului sistemului sa poată alege metode de autentificare şi autorizare diferite in funcţie de alocarea grupurilor;
- Sa ofere o interfaţă de administrare de tip web pentru accesul facil la configurări, care sa poată fi accesata doar de către administratorii de securitate ai soluţiei;
- Sa ofere SSO - autentificare unica pentru accesul la resurse; pe parcursul unei singure sesiuni de lucru utilizatorul fi autentificat o singura data, după care va putea accesa fără reautentificare toate aplicaţiile web pentru care are drept de acces;
- Fiecare utilizator sa fie identificat de sistem pe baza unei sesiuni;
- Sistemul sa permită administratorilor terminarea manuala a sesiunilor utilizatorilor;
- După un timp configurabil de inactivitate sesiunile utilizatorilor trebuie sa fie terminate in mod automat;
- Numărul de sesiuni pe care un utilizator le poate deschide trebuie sa poată fi limitat de către administratori;
- Toate evenimentele de acces - autentificări reuşite, autentificări nereuşite, autorizări reuşite, autorizări nereuşite trebuie sa poată fi auditate;
- Datele colectate prin auditarea accesului trebuie sa fie stocata într-o baza de date pe care sa poată fi rulate in caz de nevoie rapoarte;

- Toate componentele software ale soluției de control acces trebuie sa permită rularea in mod disponibilitate ridicata;
- Autentificarea și controlul accesului utilizatorilor în sistem se va realiza în mod centralizat și integrat pentru toate componentele funcționale ale sistemului;

Din punct de vedere tehnic, componenta de control al accesului utilizatorilor va trebui sa asigure:

- Sa permită accesarea simultana a mai multor surse de identități pentru realizarea autentificării și autorizării;
- Toate politicile de control al accesului trebuie sa poată fi definite utilizând interfață web a soluției, fără a necesita cunoștințe de programare sau rularea de scripturi pe server;
- Sa suporte cel puțin următoarele metode de autentificare:
  - Nume de utilizator și parola;
  - Certificate digitale;
  - Oauth 2.0;
  - OpenID ;
  - SAML 2.0;
  - Autentificare automata cu utilizator de domeniu Windows;
- Nivelul de auditare trebuie sa fie configurabil (succes, nereușita, etc);
- Sa realizeze criptarea informației transferata intre componentele sistemului și clienti;
- Soluția de control acces sa ofere integrare cu componenta sever web, ce va fi punctul principal de acces al utilizatorilor;
- Sa permită autentificare multi-factor prin SMS, email sau aplicații mobile;
- Sa ofere capabilități de autentificare adaptiva prin analiza automata a comportamentului utilizatorilor folosind algoritmi de învățare automata pentru a:
  - cere metode adiționale de autentificare in cazul in care s-a identificat un comportament ce deviaza de la normal;
  - bloca autentificarea utilizatorului;
- Sa permită impunerea unor filtre de acces (operațiuni de autorizare) la anumite resurse pe diverse criterii definite de utilizator
- Sa ofere conector pentru integrare cu sisteme externe de autentificare: Open ID, Facebook, Google, Microsoft, Twitter si Office365;
- Sa permită dezvoltatorilor dezvoltarea de noi mecanisme de autentificare.

4.3.14 Componenta de virtualizare și containerizare

Soluția de virtualizare și containerizare de tip COTS - Commercial off the Shelf va fi licențiată pentru toate echipamentele server tip 1 și tip 2 solicitate în cadrul caietului de sarcini prin model de licentiere perpetua sau tip subscripție și va oferi următoarele funcționalități:

-
- Soluția trebuie să permită adăugarea de noi sisteme de calcul sau de stocare, în grupul de resurse, fără întreruperea serviciilor;

- Soluția trebuie să permită redistribuirea încărcării pe resursele noi adăugate fără întreruperea serviciilor;
- Soluția trebuie să dispună de capacități de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie migrate automat pe celelalte host-uri din cluster, iar host-ul degradat să fie trecut automat în mentenanță după evacuarea mașinilor virtuale;
- Oferă o arhitectură independentă de un sistem de operare de uz general și cu o amprentă pe disc cât mai mică pentru a permite ca instalarea și boot-area hipervizorului să fie făcută foarte rapid, direct de pe discurile din server, din rețea sau pe de pe un stick USB;
- Oferă integrare REST API pentru alte sisteme de tip back-up & restore, respectiv de monitorizare și configurare, precum și automatizare prin ansible si terraform;
- oferă suport pentru o gamă largă de sisteme de operare instalate la nivel de mașină virtuală - Windows ServerDesktop, RedHat, SuSE, Ubuntu, Debian, Oracle Linux;
- Să asigure o densitate mare de mașini virtuale, oferind suport pentru configurații fizice generoase la nivel de host, prin configurarea cel puțin RAM de memorie RAM;
- Să permită rularea de aplicații mari consumatoare de resurse, oferind suport de configurare a mașinilor virtuale cel puțin la 128 procesoare virtuale și 5TB RAM;
- 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) și de licențiere precum și pentru asigurarea continuității în funcționare a aplicațiilor în cazul unor întreruperi parțiale neplanificate;
- Suport larg pentru aplicații terțe din partea ISV (Independent Software Vendors);
- Permite balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vedere asigurării resurselor optime pentru funcționare;
- Asigură comutatoare de rețea virtuale (switch-uri) administrate centralizat, la care să se conecteze mașinile virtuale și interfețele de rețea fizice de pe fiecare host;
- Administratorii infrastructurii virtuale pot configura accesul bazat pe roluri și pot să aloce resursele de infrastructură virtuală echipelor de dezvoltatori având vizibilitate asupra aplicațiilor instalate și a resurselor consumate;
- Oferă interfața de management bazată pe interfața web HTML 5, accesibilă de pe majoritatea sistemelor de operare și browser-erelor existente precum Firefox (Windows, Mac OSX, Linux), Google Chrome (Windows, Mac OSX, Linux) și IE/Edge (Windows) pentru simplificarea managementului.
- Platforma de virtualizare trebuie să se integreze cu una din infrastructurile de virtulizare deja existente. Prin integrare se înțelege funcționarea nativă și complet compatibilă a platformei de virtualizare furnizate cu una din platformele de virtualizare deja existente și management-ul unificat/centralizat al acestora.
- Toate componentele software instalate în cadrul platformei de virtualizare (ex: server de aplicații, baze de date etc) trebuie să fie licențiate în conformitate cu politica de licențiere a producătorului

acestora. Se va ține cont de platforma de virtualizare ofertată în vederea stabilirii numărului adecvat de licențe necesare pentru produsele software astfel încât acestea să fie în compliantă cu politica de licențiere.

Pentru componentele de tip COTS cum ar fi baze de date relaționale sau componente BigData se pot oferta soluții care partiționează infrastructura hardware cu mecanisme proprii care sa segmenteze componentele software.

Functie de arhitectura propusa de fiecare ofertant, se pot include soluții care partiționează infrastructura hardware cu mecanisme proprii care sa segmenteze componentele software.

4.3.15 Componenta de disaster recovery

Soluția de Disaster Recovery pentru mediul virtual va oferi următoarele funcționalități:

- crearea si managementul planurilor de Disaster Recovery direct din interfata de management a mediului virtual;
- permite arhitecturi diferite, in care protectia poate fi configurata bidirectional sau in care se utilizeaza un site de comun pentru protejarea mai multor site-uri;
- suport pentru diferite metode de replicare, la nivel de host sau la nivel de storage, si descoperirea automata a mașinilor virtuale protejate prin cele doua metode;
- poate integra diferite solutii de replicare sincrona sau asincrona, la nivel de storage: ISCSI, FibreChannel sau NAS, pe baza unor plugin-uri (storage replication adapters) oferite de producatorii solutiilor de stocare;
- se integrează cu replicarea asincrona la nivel de host asigurand protectia granulara, la nivel de masina virtuala si recuperarea mai multor puncte in timp, cu un RPO (recovery point objective) configurabil intre 5 minute si 24 ore;
- permite maparea resurselor din site-ul de disaster recovery la masinile virtuale protejate;
- permite rularea de scripturi (out of guest sau in guest) pentru extinderea planurilor de Disaster Recovery;
- permite definirea de roluri pentru controlul accesului la planurile de Disaster Recovery;
- alerteaza automat operatorul in cazul in care legatura cu site-ul protejat a cazut, oferind totodata optiunea de recuperare rapida, pe baza planurilor prestabilite si testate, in site-ul de Disaster Recovery;
- asigura pornirea automata a masinilor virtuale in caz de Disaster Recovery, permitând stabilirea ordinii de boot-are a acestora;
- asigura un mecanism simplu de reconfigurare a adreselor IP pentru recuperarea masinilor virtuale in site-ul de Disaster Recovery;
- asigura managementul si monitorizarea planului de Disaster Recovery direct din interfata de management a mediului virtual, permitând oprirea temporara si interventia manuala in caz de necesitate pentru rezolvarea eventualelor problemelor aparute;
- asigura reprotejarea automata, in oglinda, a masinilor virtuale protejate prin inversarea replicarii catre site-ul original protejat;

- asigura testarea automata a planului de disaster recovery in orice moment de timp si fara intreruperea functionarii sau protectiei masinilor virtuale protejate prin utilizarea de snapshot-uri la nivel de storage si recuperarea masinilor virtuale intr-un mediu de lucru izolat;
- asigura curatarea automata a site-ului de Disaster Recovery dupa efectuarea testelor (ex. oprirea masinilor, stergerea snapshot-urilor)
- rezultatele testelor sunt stocate si pot fi vizualizate sau exportate direct din interfata de management a mediului virtual;
- permite utilizarea planului de Disaster Recovery si pentru migrari planificate, in care masinile virtuale protejate sunt oprite intr-o stare consistenta a aplicatiilor la nivelul site-ul protejat, dupa care se face sincronizarea datelor cu site-ul de Disaster Recovery si refacerea pe baza planului de Disaster Recovery a masinilor virtuale protejate.

4.3.16 Componenta de analiză și detecție atacuri cibernetice

Soluția reprezintă o platformă de securitate cibernetică care utilizează algoritmi specializați de învățare automată nesupravegheată și analiză comportamentală sau mecanisme complexe de inteligență artificială pentru a monitoriza traficul de date din cadrul unei infrastructuri IT&C. Aceasta este capabilă să analizeze și să detecteze atacurile cibernetice avansate (Advanced Persistent Threat) și atacurile cibernetice necunoscute (zero-day).

Platforma va avea un senzor specializat (echipament de tip server) la nivel de site, acest senzor fiind format din componente hardware și software, care analizează traficul intern și extern existent într-o rețea informatică. Senzorul trebuie să respecte următoarele specificații hardware minimale:

- Dimensiune maximă, rackabil 19": 2U;
- Interfețe administrare: 1 x 10/100/1000 BASE-T;
- Interfețe pentru analiză/monitorizare (minim): 1 x 10/100/1000 BASE-T, 2 x 10 GBASE-T, 2 x 1Gbe/10Gbe SFP+;
- Cantitate trafic de date analizat: 4.9 Gbps;
- Sursă de alimentare: Dublă , 100-240V;

Componenta hardware este reprezentată de serverele fizice care asigură resursele necesare funcționării în parametri optimi a componentei software.

Componenta software este cea care conține algoritmii proprietari, mecanismele de învățare automată și analiză comportamentală.

Soluția trebuie să dispună de mecanisme de actualizare în mod offline, fără conexiune la Internet.

Sistemul trebuie să aibă capacitatea de a analiza o rețea informatică, învățând comportamentul rețelei și generând un model de comportament pentru fiecare dispozitiv și utilizator din rețea, astfel având posibilitatea de a detecta activitățile anormale.

Soluția folosește o combinație de învățare automată supravegheată și învățare automată nesupravegheată pentru a ajuta la detectarea, răspunsul și investigarea autonome a amenințărilor cibernetice.

Solutia analizeaza traficul brut din fiecare parte a ecosistemului digital în zeci de algoritmi de învățare automată, în principal nesupravegheați, pentru a afla cum arată comportamentul normal în cadrul organizației in vederea detectiei oricarui tip de atac, inclusiv amenințările zero-day.
Sistemul monitorizează și analizează:

- Traficul de rețea direct către Internet (inbound/outbound);
- Traficul de rețea către Internet (inbound/outbound) care trece prin noduri de rețea intermediare de tip servere Proxy;
- Traficul de rețea asociat protocolului DNS;
- Traficul de rețea asociat protocolului DHCP;
- Traficul de rețea din rețeaua LAN internă generat la accesarea unor aplicații sau servicii;
- Traficul de rețea din rețeaua LAN internă generat în procesul de autentificare a stațiilor de lucru/serverelor la serverul de domeniu (Domain Controller);
- Orice alt trafic de rețea generat între oricare dispozitive din rețeaua LAN internă.

Echipamentul primește/procesează/analizează trafic de rețea folosind metoda SPAN sau prin folosirea unor dispozitive de tip Network TAP.
Când soluția detectează anomalii și generează alerte, aceasta trebuie să aibă capabilitatea de a salva și de a exporta traficul de rețea asociat alertelor respective.
Sistemul folosește algoritmi de învățare automată nesupravegheată (unsupervised machine learning).
Sistemul nu are nevoie de seturi de date, reguli predefinite pentru detecția anomaliilor.
Soluția identifică atacuri cibernetice necunoscute. Metodele avansate de învățare automată corelează modelele comportamentele obținute pentru a detecta amenințări cibernetice necunoscute.
Modelele comportamentale obținute permit detectarea unor activități anormale, deviații de la comportamentul normal al rețelei, detectând astfel amenințările și atacurile cibernetice în timp real.
Utilizând algoritmii de analiză comportamentală, soluția poate identifica aplicații malware care existau in rețea anterior instalării acesteia.
Sistemul clasifică amenințările identificate în funcție de importanța acestora.
Detectează comunicațiile dintre dispozitivele victimă din cadrul rețelei și serverele de Comandă și Control.
Sistemul are opțiunea de a șterge datele colectate, fără a afecta funcționalitatea internă a echipamentului.
Asigura efectuarea de backup/restore a configurațiilor generale.
Sistemul permite integrarea cu servere de tip LDAP.
Soluția dispune de un mecanism ce poate investiga incidentele de securitate in mod 100% autonom care poate produce un raport în limbaj natural.
Sistemul transmite notificări prin E-mail despre alertele identificate. Adresa de e-mail poate fi configurată de către administrator.
Sistemul trebuie să asigure crearea unor conturi cât și tipuri de acces diferite pentru utilizatorii sistemului. Astfel se pot crea conturi pentru utilizator cu anumite drepturi de vizualizare în interfața grafică.

Sistemul dispune de o interfaţă grafică interactivă prin care utilizatorul poate vizualiza activitatea de analiză şi monitorizare.
Accesarea interfeţei grafice se poate realiza dintr-un browser web, folosind o conexiune criptată bazată pe certificat digital.
Pentru conexiunea la interfaţa grafică este necesară autentificarea utilizatorului pe baza unui nume de utilizator şi a unei parole.
Interfaţa grafică dispune de un meniu principal cu diverse opţiuni disponibile unui utilizator în funcţie de permisiunile acestuia.
Descoperă/identifică subreţelele şi dispozitivele din cadrul acestora din reţeaua analizată.
Echipamentul furnizează, în funcţie de traficul analizat, informaţii despre dispozitivele identificate.
Soluţia facilitează vizualizarea istoricului de alerte pentru un dispozitiv informatic.
Pentru fiecare dispozitiv se poate selecta un interval de timp pentru a vedea istoricul conexiunilor.
Soluţia asigură gruparea dispozitivelor informatice în baza unor activităţi similare (ex: conexiuni către aceeaşi destinaţie).
Din interfaţa grafică utilizatorul poate efectua căutări după cuvinte cheie (Ex: adrese IP, hostname, nume de domeniu, etc.).
Pentru fiecare domeniu sau adresă IP ale unui server de comandă şi control accesate din interiorul reţelei se pot extrage/vizualiza dispozitivele interne care au efectuat conexiuni către acesta.
Utilizatorul poate modifica intervalul de timp pentru care se doreşte vizualizarea alertelor.
Alertele identificate sunt afişate în interfaţa grafică în funcţie de nivelul de severitate atribuit de către echipament. De asemenea se poate alege un interval de timp pentru vizualizare.
Pentru fiecare alertă soluţia va furniza detalii suplimentare precum: data şi ora, cine a generat alerta (adresă IP, hostname, etc.).
Utilizatorul are opţiunea de a eticheta un dispozitiv informatic identificat în cadrul unui tip de comportament ca fiind legitim (similar cu procesul de whitelist).
Utilizatorul poate să filtreze afişarea dispozitivelor în funcţie de un tip de comportament / categorie de detecţie.
Pentru fiecare dispozitiv soluţia generează şi stochează informaţii despre comportamentul dispozitivului sub forma unui istoric al conexiunilor realizate. Asupra acestui istoric de conexiuni utilizatorul poate aplica opţiuni de filtrare. De asemenea utilizatorul poate descărca conexiunile sub forma unui fişier .pcap.
Soluţia trebuie să poată genera rapoarte automate despre întreaga reţea şi incidentele detectate. Rapoartele pot fi descărcate pentru vizualizarea într-o aplicaţie externă.
Utilizatorul poate eticheta (poate adăuga tag-uri) anumite incidente, dispozitive sau utilizatori din reţea.
Soluţia dispune de un modul ce asigură o căutare avansată în datele colectate din trafic. Căutarea poate fi realizată în funcţie de anumite valori, folosind parametri specifici, expresii regulate sau operatori logici.
Platforma trebuie să poată fi integrată cu sisteme de tip SIEM.
Sistemul trebuie să asigure actualizarea software-ului în mod offline (nefiind conectat la Internet).

Sistemul trebuie să asigure managementul centralizat al tuturor senzorilor instalați în diverse locații.
Sistemul trebuie să faciliteze comunicarea criptată dintre serverul de management si senzori.
Soluția trebuie să poată detecta următoarele tipuri de activități și comportamente, prin mecanisme specifice (machine learning, analiză comportamentală) :

- Conexiuni interne și externe;
- Transfer de date intern și extern;
- Dispozitive conectate din rețeaua internă;
- Dispozitive conectate din exterior;
- Conexiuni active din rețeaua internă;
- Conexiuni active din exterior;
- Comportament/activitate anormală a unui dispozitiv;
- Cereri DNS reușite/nereușite;
- Autentificări Kerberos (reușite/nereușite);
- Conexiuni suspicioase de la un dispozitiv către mai multe destinații;
- Conexiuni SMB nereușite/reușite;
- Scanarea adreselor din rețea (Address scans on the network);
- Activitate minare criptomonede;
- Metode folosite de aplicațiile malware pentru mișcarea laterală;
- Sistemul de operare al dispozitivelor;
- Identificare servere de tip Proxy;
- Transfer de fișiere EXE;
- Transfer de fișiere RAR;
- Transfer de fișiere cu format necunoscut/payload;
- Atacuri de tip Bruteforce;
- Atacuri de tip Heartbleed;
- Aplicații specifice atacurilor de tip Advanced Persistent Threat (APT);
- Detecția anomaliilor în utilizarea credențialelor;
- Comunicații cu rețeaua TOR;
- Scanare de porturi;
- Conectarea pe porturi non-standard sau compromiterea unui port legitim / port hijacking;
- Monitorizare trafic SMTP;
- Anomalii în traficul serverelor DNS (Traffic changes to DNS servers);
- Cereri DNS de tip DynDNS (DynDNS DNS requests);
- Pierdere excesivă a conexiunilor sau a pachetelor;
- Certificate SSL invalide

Tehnologia trebuie să fie 100% „on premise", fără a fi necesară conectarea în Internet pentru orice fel de motiv cu privire la funcționalitatea produsului. Orice tip de date sau informații culese de la client nu se trimit în extern, sau la producător, fără acordul clientului. Toate actualizările software trebuie efectuate offline, în mod centralizat și automat. Componenta software trebuie să se afle in întregime pe servere fizice, complet sub controlul clientului și în interiorul rețelei sale.

Senzorii din cadrul platformei vor fi instalați și configurați în locații fizice diferite, astfel se va asigura comunicarea și partajarea în mod securizat a datelor între aceștia. Senzorii se pot administra la nivel local.
Solutia va fi licentiata astfel incat sa fie inclus mecanismul de detectie prin invatare cat si mecanismul de raspuns autonom la atacurile avansate de securitate cibernetica

4.3.17 Componenta SIEM

Soluția reprezintă o platformă de securitate cibernetică care utilizează algoritmi specializați de învățare
Soluție la cheie de tip SIEM, ce va conține toate componentele software necesare bunei funcționări a acesteia. Soluția va fi instalată la sediul beneficiarului și va centraliza alertele de securitate colectate.
Soluția trebuie să asigure preluarea evenimentelor de securitate de la nivelul tuturor echipamentelor de retea protejate și transmiterea acestora către componenta SIEM
Ofertantul va asigura maparea rețelei informatice în care sunt conectate echipamentele în soluția SIEM prin definirea zonelor de rețea și a asset-urilor existente, integrarea tuturor surselor generatoare de date existente, surse menționate la momentul instalării, și transmiterea automată către soluția SIEM a alertelor de securitate în conformitate cu cerințele beneficiarului în momentul instalării.
În cadrul locatiei beneficiarului, ofertantul va asigura instalarea componentei SIEM pe suportul hardware pe care furnizorul îl va pune la dispoziție.
Soluția trebuie să asigure în mod implicit colectarea și interpretarea evenimentelor de la cel puțin următoarele sisteme de operare:

- Windows 2012, 2019, 2022;
- Redhat linux 8,9
- Oracle Linux 8,9

Soluția trebuie să permită instalarea în mod distribuit a componentelor sale, pe noduri care să asigure redundanță.
Soluția trebuie să ofere capacitatea de a mări performanța de corelare prin adăugarea unor instanțe (noduri) suplimentare
Soluția trebuie să ofere facilități de normalizare a datelor obținute de la surse diferite de evenimente.
Soluția trebuie să permită stocarea evenimentelor colectate și în format brut.
Soluția trebuie să asigure colectarea evenimentelor prin intermediul unei componente disponibile sub formă de agenți/produs de colectare software. Această componentă trebuie să îndeplinească și rolul de normalizare jurnale și evenimente.
Componentele de tip agenți de colectare trebuie să poată fi instalate atât local, centralizat pe o singură platformă de gestiune, cât și la distanță în locații dispersate din punct de vedere geografic.
Componentele de tip agenți de colectare vor normaliza și cataloga evenimentele într¬-un format comun, folosind o taxonomie cu cel puțin 50 de câmpuri predefinite.
Soluția trebuie să asigure mecanisme de protecție a integrității datelor stocate prin intermediul semnăturilor de tip hash.
Soluția trebuie să dețină, la punctul de colectare, un mecanism de stocare temporară de tip „cache". Acest mecanism va asigura retransmiterea ulterioară a datelor pentru a evita supraîncărcarea rețelei.

Soluția trebuie să asigure exportarea evenimentelor colectate în format CSV.
Soluția trebuie să asigure filtrarea opțională a evenimentelor la nivelul agentului de colectare.
Soluția trebuie să dețină un mecanism integrat de agregare a evenimentelor de securitate colectate.
Soluția trebuie să ofere un mecanism integrat de compresie a datelor stocate și permite definirea unor politici diferite de retenție a evenimentelor colectate.
Soluția trebuie să asigure corelarea evenimentelor colectate din surse de log-uri diferite.
Soluția trebuie să dispună de obiecte predefinite specifice sistemului de colectare, corelare și raportare, pentru o punere inițială în funcțiune cât mai rapidă și mai facilă (filtre, reguli de corelare, alerte, rapoarte etc.) dar să ofere și posibilitatea de a defini propriile obiecte fără niciun fel de limitări sau restricții funcționale sau de licențiere.
Soluția trebuie să asigure execuția de corelări bazate pe reguli și să ofere posibilitatea definirii unor acțiuni de răspuns ce includ cel puțin:

- crearea unui eveniment;
- notificare în interfața grafică;
- execuția automată a unor comenzi configurabile cel puțin la nivelul soluției de analiză și la nivelul agenților de colectare;
- transmiterea unui email.

Soluția trebuie să asigure corelarea în cadrul unei reguli în momentul detecției unui număr predefinit de evenimente similare.
Soluția trebuie să asigure crearea de către utilizator a regulilor de corelare și să ofere un mecanism pentru testarea acestora. Pentru crearea regulilor, soluția trebuie să permită utilizarea operatorilor booleeni (OR și AND).
Toate obiectele și resursele definite la nivelul soluției de către utilizatori trebuie să poată fi salvate pentru a fi reutilizate ulterior.
Rezultatele regulilor de corelare trebuie să poată fi utilizate secvențial și automat în cadrul altor reguli de corelare.
Soluția trebuie să asigure definirea de liste de câmpuri (din cele incluse în taxonomia implicită) astfel încât ele să poată fi aplicate la nivelul obiectelor specifice soluției.
Soluția trebuie să asigure definirea de filtre de evenimente și salvarea acestora astfel încât ele să poată fi utilizate ulterior la nivelul celorlalte obiecte specifice soluției.
Soluția trebuie să asigure integrarea informațiilor de la produse de analiză a vulnerabilităților de rețea și utilizarea acestor informații în procesul de corelare.
Soluția trebuie să asigure crearea unor liste de asseturi/ adrese IP pentru monitorizare și notificarea automată în cazul identificării acestora în fluxul traficului de rețea.
Soluția trebuie să integreze informații de geolocație pentru adresele IP identificate în trafic.
Soluția trebuie să asigure colectarea evenimentelor de securitate generate din mai multe locații geografice.
Soluția trebuie să asigure monitorizarea în timp real prin afișarea în consola de management dedicată sau într-o interfață web a rezultatelor operației de corelare a evenimentelor de securitate.

Soluția trebuie să asigure monitorizarea centralizată a stării agenților de colectare și a celorlalte componente ale soluției.
Consola de management poate fi instalată în retele/locații diferite față de unde este instalată soluția.
Soluția trebuie să ofere posibilitatea de notificare a utilizatorilor sau grupurilor de utilizatori în funcție de anumiți parametri configurabili.
Soluția trebuie să asigure rularea unor comenzi direct la nivelul evenimentelor de interes, astfel încât să poată fi obținute informații suplimentare (de exemplu: ping, traceroute, whois, nslookup, informații despre port).
Soluția trebuie să dețină capabilități de auto-descoperire a infrastructurii existente.
Soluția trebuie să asigure vizualizarea evenimentelor colectate în format brut și normalizat.
Soluția trebuie să ofere posbilitatea de clasificare și prioritizare a evenimentelor în funcție de criticitatea acestora.
Soluția trebuie să asigure investigarea incidentelor de securitate pornind de la evenimentul corelat până la identificarea evenimentelor primare ce au generat alerta.
Soluția trebuie să aibă o componentă de raportare care trebuie să fie parte integrată a soluției.
Formatul raportului trebuie să poată fi personalizat atât la nivel de informații fixe/template cât și la nivel de conținut, precum și modul de prezentare al acestuia (informații în mod text, afișări vizuale diverse precum tabele sau chart-uri).
Rapoartele trebuie să poată fi configurate să ruleze pe un set predefinit de date apărute într-o perioadă de timp configurabilă, inclusiv pe date istorice (evenimente colectate în trecut).
Soluția trebuie să includă posibilitatea integrării mai multor interogări de evenimente sau categorii de evenimente în cadrul aceluiași raport.
Soluția trebuie să asigure funcționalități de arhivare/backup pentru rapoartele generate.
Soluția trebuie să ofere rapoarte predefinite și să permită utilizatorilor crearea altor tipuri de rapoarte sau particularizarea celor predefinite.
Soluția trebuie să asigure exportarea rapoartelor cel puțin în următoarele formate: PDF și XLS.
Soluția trebuie să asigure rularea în mod programat și manual a proceselor de generare a rapoartelor.
Soluția trebuie să asigure transmiterea rapoartelor programate prin email în mod automat.
Soluția trebuie să asigure definirea asset-urilor din rețea și popularea cu cel puțin următoarele informații:

- nume;
- nivel de criticitate;
- adresă/adrese IP;
- adresă/adrese MAC;
- zonă de rețea;
- vulnerabilități identificate.

Soluția trebuie să ofere un mecanism integrat de management al incidentelor de securitate ce permite:

- transmiterea alertei pe e-mail și/sau afișarea ei în sistemul de management al soluției;
- definirea de grupuri de destinatari organizați pe mai multe nivele;
- escaladări automate către urmatoarele nivele în cadrul unui grup de destinatari;

- personalizarea conținutului mesajului de alertă pe baza informațiilor din evenimentele ce au generat alerta.

Soluția trebuie să asigure definirea rolurilor de administrare "role-based".
Soluția trebuie să asigure crearea unor spații de lucru diferite utilizatorilor, în funcție de rolul acestora.
Autentificarea utilizatorilor pentru acces la administrarea soluției trebuie să se poata realiza pe baza de conturi de utilizatori definiți local, integrare cu sisteme terțe precum Microsoft Active Directory, RADIUS sau LDAP.
Soluția trebuie să asigure accesul securizat la interfața grafică, prin intermediul protocolului SSL.
Soluția trebuie să asigure configurarea personalizată de panouri de monitorizare pe bază de grafice și tabele și posibilitatea accesării fluxului de evenimente/graficului de evenimente specific unei anumite înregistrări direct din aceste panouri;
Soluția trebuie să asigure salvarea configurației din interfața grafică, configurație ce include cel puțin următoarele resurse:

- reguli;
- surse de evenimente;
- informații despre vulnerabilități;
- rapoarte;
- utilizatori;
- grupuri de utilizatori.

Configurația salvată poate fi importată în instanța soluției SIEM din care a fost creată.
Soluția trebuie să includă un sistem integrat pentru stocarea evenimentelor, tip bază de date.
Soluția trebuie să ofere mecanisme proprii de colectare, agregare și parsare pentru evenimentele provenite de la soluțiile care nu se regasesc într-o listă predefinită.
Solutia trebuie sa ofere functionalitati de auditare și log-uri a sistemului.
Licențiere: licența soluției va fi de tip perpetuă și va fi de minim 4000 de Evenimente per secunda sustinute.
Tehnologia trebuie să fie 100% „on premise", fără a fi necesară conectarea în Internet pentru orice fel de motiv cu privire la funcționalitatea produsului. Orice tip de date sau informații culese de la client nu se trimit în exterior, sau la producător, fără acordul clientului. Toate actualizările software trebuie efectuate offline, în mod centralizat și automat. Componenta software trebuie să se afle in întregime pe servere fizice, complet sub controlul clientului și în interiorul rețelei sale.
Solutia trebuie sa includa mecanisme de integrare cu platforma MISP si sa permită colectarea de feed-uri de Threat Intelligence.
Solutia trebuie sa includa mecanisme proprii de Case Management pentru a facilita monitorizarea incidentelor cat si a diferitilor indicatori de performanta.
Solutia trebuie sa permită asignarea automata a incidentelor unui analist sau grup de analisti.
Solutia trebuie ofere un workflow complet pentru analisti. Trebuie sa poata invoca colectarea unor date aditionale, dovezi sau actiuni relevante pentru un incident pentru a-i oferi context.
Va pastra un istoric al actiunilor analistilor in ordine cronologica.
Solutia trebuie sa permită consolidarea alertelor intr-un singur incident.

Solutia trebuie sa asigure raspunsul la inceidente prin crearea si declansarea in mod automat de playbook-uri.
Accesul utilizatorilor la interfata si capabilitatile solutiei trebuie sa fie bazat pe roluri(RBAC).
Solutia trebuie sa ofere o serie de playbook-uri Out of the Box.
Solutia trebuie sa permită integrarea cu solutii de securitate de la vendori precum: Cisco, Fortinet, Juniper, PaloAlto, Microsoft.
Solutia trebuie sa permită stocarea unor informaţii sub forma de liste ce pot fi referentiate ulterior in cautari.
Solutia trebuie sa aiba optiunea de a incarca documente externe ce pot fi folosite ca materiale aditionale in incidente sau ca proceduri de lucru pentru analisti.

4.3.18 Componenta PKI

Platforma Public Key Infrastructure (PKI) care va fi tip COTS (Commercial off the Shelf) va gestiona certificate digitale şi chei de criptare pentru asigurarea următoarelor principii de securitate:

- Autentificare
- Confidenţialitate
- Integritate

În acest sens se are în vedere utilizarea tehnologiilor PKI în vederea implementării principiilor mai sus menţionate, astfel:

- Autentificare: va fi asigurata prin certificate digitale emise la nivel local, pentru fiecare dispozitiv şi server în parte. Sistemul va utiliza aceste certificate digitale pentru autentificare prin integrare şi cu componenta de gestiune a identităţii utilizatorilor şi a accesului.
- Confidenţialitate: va fi asigurata prin criptarea informaţiilor, utilizând tehnologiile PKI şi algoritmi standard recunoscuţi la nivel internaţional. Sistemul va utiliza certificatele digitale pentru criptare.
- Integritate: Sistemul va utiliza certificatele digitale şi se va integra cu echipamentele HSM pentru criptarea informaţiilor şi verificarea validităţii semnăturilor astfel încât să fie asigurată non-repudierea.

Platforma PKI trebuie să asigure următoarele funcţionalităţi:

- Integrare cu echipamentele HSM ofertate pentru utilizarea capabilităţilor de criptare hardware;
- Scanarea întregii reţele pentru certificate şi consolidarea acestora într-un depozit central;
- Descoperirea de certificate din surse diferite, indiferent de CA emitent. Suport pentru procese de descoperire la cerere, programate şi recurente;
- Scanează certificate SSL într-o varietate de locaţii, inclusiv servere de e-mail SMTP, balansoare de încărcare, AWS, AD, MS-CA şi căi de directoare partajate;
- Capabilitate de verificare toate aceste puncte finale variate pentru a se asigura că niciun certificat existent nu este omis în procesul de scanare. Posibilitatea de selectare a unui proces de descoperire granular, doar pentru certificatele de interes selectabile din lista de certificate disponibile;
- Posibilitate de planificare recurentă a descoperirii certificatelor, pentru menţinerea la zi a informaţiilor din depozit, astfel încât acesta să ţină evidenţa certificatelor şi să poate preciza

automat sursa acestora, permițând totodată recuperarea rapidă a celei mai recente versiuni a unui certificat;

- Descoperirea de certificate de la mașini ale căror credențiale sunt indisponibile precum și de la mașini care sunt prezente în zonele demilitarizate (DMZ). Posibilitatea conectării agentului la platformă printr-o conexiune securizată de tip HTTPS și verificarea stării mașinii monitorizate;
- Posibilitatea de creare de diferite grupuri de certificate care pot fi instalate în anumite locații/servere;
- Creare de certificate proprii de tip root-CA. Certificatele root-CA trebue să poate fi stocatete autonom, iar administratorii să le poată folosi pentru a semna cereri de certificat generate local.
- Scanarea periodică a certificatelor - preluarea stărilor CRL și OCSP, verificarea vulnerabilităților Poodle și Heartbleed și semnalarea certificatele nesigure;
- Automatizarea instalării certificatelor într-o locație dorită direct din interfața platformei, posibilitatea utilizării de agenți pentru instalare de certificate pe mașini prezente în zonele demilitarizate (DMZ);
- Instalarea unui certificate pe mai multe mașini/servere sau posibilitatea instalării unui grup de certificate pe o singură mașină/server;
- Monitorizarea și urmărirea în mod activ a valabilitatății certificatelor de la nivelul depozitului central. Trimiterea de rapoarte periodice și alerte în timp util proprietarilor de domenii, notificându-i ori de câte ori certificatele ajung la expirare iminentă;
- Posibilitatea reînnoiri automate sau la cerere a certificatelor, oferind metode flexibile de configurare a numărului de zile înainte de care certificatele trebuie să fie reînnoite automat;
- Generarea, semnarea și gestionarea cererilor de semnare a certificatelor (CSR) dintr-o singură interfață. Administratorii privilegiați trebuie să poată semna orice Certificate Signing Request (CSR) existent, iar odată ce un CSR este semnat, certificatul emis va fi actualizat automat în cadrul depozitului central;
- Capabilitate de integrare cu CA-uri multiple (locale sau publice) - import, solicitare, instalare, reînnoire, revocare și ștergere de certificate din CA-uri multiple din cadrul unei singure interfețe de la nivelul platformei. Posibilitatea de generare de rapoarte analitice organizate pentru certificatele gestionate de fiecare CA în parte;
- Tablou de bord intuitiv cu widget-uri dedicate pentru identificarea rapidă a certificatelor expirate, a certificatelor SHA-1 și a vulnerabilităților SSL;
- Stabilirea unui mecanism de auditare solid în jurul utilizării cheilor SSH. Captarea tuturor activităților executate în aplicație ca piste de audit, inclusiv timpul și rezultatul execuției, adresa IP de la care a fost efectuată acțiunea și alte detalii;
- Administratorii pot genera instantaneu rapoarte pentru a revizui sau a demonstra eficacitatea managementului cheilor SSH. Platforma trebuie să captureze în timp real momentul în care cheile SSH sunt create, implementate, accesate și actualizate până în momentul în care sunt șterse;
- Platforma trebuie să gestioneze securizat cheile SSH respectând standarde internaționale precum PCI-DSS și NIST;

- Generarea de copii de rezervă ale depozitului central prin definirea de procese recurente configurabile de către administratorii privilegiați. Copia de rezervă trebuie să conțină informațiile în mod criptat astfel încât să prevină accesul neautorizat la date;
- Integrare cu servere LDAP, inclusiv Active Directory, pentru provizionare și autentificarea utilizatorilor.

4.3.19 Componenta de monitorizare infrastructură și aplicații

Platforma de tip COTS de monitorizare infrastructură și aplicații va asigura managementul infrastructurii și serviciilor furnizate de noul sistem în cazul operării sistemului în producție. Scopul acestei componente este eficientizarea activității în organizația IT, precum și creșterea calității serviciilor oferite, bazat pe bune practici și pe automatizarea proceselor. Aceasta va asigura un management cuprinzător al evenimentelor, o monitorizare proactivă a performanței, precum și un sistem automatizat de alertare (pe email și SMS), raportare și realizare grafică pentru elemente de rețea, sisteme de operare, pachete software dezvoltate intern sau adaptate și aplicațiile ce se vor implementa în cadrul proiectului.

Platforma de monitorizare infrastructură și aplicații va realiza monitorizarea serviciilor prin modelare bazată pe componentele de infrastructură, iar informațiile colectate vor fi puse la dispoziția administratorilor într-un tablou de bord unic. Componenta va fi dimensionată ținând cont de alocarea de resurse conform arhitecturii sistemului. Cerințele specifice la care aceasta componenta a sistemului trebuie să răspundă sunt următoarele:

- monitorizarea integrată a elementelor de infrastructură legate de rețea, sisteme, aplicații eterogene. Platforma va gestiona dispozitive de rețea provenind de la diferiți producători, diferite sisteme de operare, diferite tipuri de aplicații - baze de date, servere de internet etc.;
- crearea (descoperirea automată) și prezentarea de hărți care să prezinte legăturile dintre diferite componente de infrastructură (elemente de rețea, servere, aplicații) pentru a oferi o imagine totală a sistemului și a serviciilor din rețea;
- generarea și prezentarea în interfață grafică de evenimente în cazul în care apar situații de excepție;
- afișarea stării serviciilor în timp real, prin intermediul tabloului de bord;
- colectarea datelor de performanță despre infrastructură și servicii respectiv raportarea acestora;
- păstrarea evenimentelor într-o bază de date relațională accesibilă prin ODBC/JDBC;
- folosirea de standarde: comunicarea între componentele soluției să fie bazată pe protocoale standard, să fie utilizate limbaje de programare standard;
- să existe capabilități de monitorizare predefinite incluse în soluția livrata, adaptate tehnologiilor oferite în cadrul celorlalte subsisteme/platforme funcționale;
- capabilități de monitorizare configurabile;
- să dispună de o interfață grafică nativă web, prin care să se poată realiza operațiile de configurare;

4.4 CERINȚE TEHNICE PENTRU COMPONENTELE HARDWARE CENTRALE

4.4.1 Echipament server tip 1

1.	**Descriere generală**
	• Echipament de tip server quad-socket pentru sisteme informatice • Răcire Front to Back
2.	**Procesor**
	Serverul va fi echipat cu minim 4 procesoare de tip Intel Xeon sau echivalent de ultimă generație, având următoarele caracteristici: • Frecventa: 2.9 GHz sau superior; • Bus Speed min 16GT/s; • Cache: 45 MB sau superior; • Număr de core-uri per procesor: minim 16 core-uri cu 32 fire de execuție; • Număr procesoare instalate: minim 4;
3.	**Memorie**
	• Minim 2TB Registered ECC DDR5 memorie instalată, cu functionalitati de protective avansata a memoriei RAM, cum ar fi: o Fault resilient mode (FRM) o Demand Scrubbing o Patrol Scrubbing • Minim 64 sloturi total (minim 32 libere) pentru memorie RAM cu suport pentru minimum 4TB RAM. • Metode suportate de protecție a memoriei: Advanced ECC
4.	**Hard disk drive:**
	• Minim 2 disk-uri SSD M.2 480GB care să poată fi configurate într-o matrice de tip RAID 1

	• Serverul va fi echipat cu un număr minim de 16 bay-uri pentru disc-uri. • Sistemul trebuie livrat cu toate modulele şi accesoriile necesare pentru instalarea discurilor în mod hot-swap.
5.	**Interfaţa grafică**
	• Minim 16MB memorie video
6.	**Securitate**
	• TPM 2.0; • Suport inclus pentru verificarea semnăturilor criptografice ale driverelor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS boot loader şi altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze; • Suport inclus pentru verificarea şi validarea autenticităţii firmware-ului componentelor critice ale echipamentului (interfeţe de reţea, 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 ofertat pentru a fi autentificate la instalare; • Include suport pentru un mecanism de audit al tuturor operaţiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Logurile acestor informaţii de audit vor fi securizate şi vor putea fi accesate doar din componenta de management a soluţiei propuse; • Suport inclus pentru resetarea sistemului la starea iniţială (setările din fabrică), cu toate datele şi configuraţiile eliminate din mediile de stocare interne ale echipamentului; • Firmware rollback; • UEFI Server Firmware; • posibilitatea de a dezactiva "Secure Boot".
7.	**Interfeţe de reţea**

	• Minim 8 x Ethernet 25Gbps SFP28 echipate în configurația ofertată (8 buc Cablu DAC 25Gbps 3m incluse). Placile de retea trebuie sa aiba capabilitatea PXE boot. • Interfața de rețea separată pentru administrare la distanță, diferită de cele 8 interfețe de rețea (1 buc patch CAT 6 3m inclusă). • Soluția ofertata trebuie sa beneficieze de Root of Trust – astfel încât sa permită verificarea actualizărilor de firmware printr-un set de chei criptografice scrise de către producător la nivel de controller hardware, permițând astfel un nivel de securitate suplimentar fata de o verificare standard la nivel de firmware software
8.	**Sloturi de expansiune**
	• Minim 8 sloturi extensie PCIe din care minim 4 sloturi de tip PCIe x16 electric (cu 16 LAN-uri PCI Express conectate).
9.	**Conectori interfețe I/O**
	• Minim: 1 x serial, 1 x VGA, minim 3 x USB din care minim 1 x USB 3.0
10.	**Carcasă**
	• Montabil în rack cu șine glisante. Serverul va fi echipat cu mecanism de închidere pentru a putea securiza accesul la disc-urile instalate.
11.	**Sursa de alimentare**
	• Minim 2 surse hot plug și redundante instalate cu o putere de minim 1400W. • Sursele, clasa Platinum sau echivalent, vor fi dimensionate pentru a permite echiparea maximală a serverului (număr maxim de module de procesare dedicate, număr maxim de disc-uri și de module de memorie) fără necesitatea schimbării surselor.
12.	**Ventilatoare**
	• Ventilatoare redundante (N+1), hot plug
13.	**Administrare**
	Echipamentul trebuie să fie livrat cu capabilități hardware incluse pentru: • administrarea și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți;

- a asigura compatibilitatea, modulul hardware de administrare trebuie să fie furnizat de același producător cu cel al serverelor;
- inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, plăci HBA, controllere RAID, unități de stocare;
- update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticității acestora;
- generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură;
- funcționalitatea de validare a configurației față de o referință;
- monitorizarea stării de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică;
- instalare și configurare locală și la distanță, inclusiv configurare RAID;
- management operațional cu următoarele funcții: monitorizarea stării sistemului, managementul evenimentelor și alarmelor, inventarul componentelor, inventarul și instalarea update-urilor și patch-urilor, analiza performanței, diagnoza în timp real, repornirea și reconfigurarea automată a serverului;
- LCD display sau panou cu leduri; panoul LCD/LED livrat va permite citirea mesajelor de eroare fără operațiuni suplimentare;
- monitorizare a ventilatoarelor, surselor de alimentare și temperaturii, panou LCD sau cu LED-uri pentru diagnosticarea rapidă a stării de funcționare a componentelor critice: memorii, procesoare, surse de alimentare, ventilatoare, disk-uri, interfețe PCI, placă de bază;
- analize predictive de eroare (fără aplicație externă) pentru: disc-uri, memorii, cu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componentele enumerate anterior (Predictive Failure Analysis);
- suport instalat și activat cu licențiere perpetuă pentru managementul serverului de la distanță (redirectare interfață grafică, tastatură și mouse, posibilitate de pornire/oprire de la distanță, suport SSL, SNMP, suport pentru remote virtual media).

Sistemul de management trebuie să fie echipat cu următoarele facilitați:

- management de la distanță;
- redirectare interfață grafică cu tastatură și mouse;
- posibilitate de pornire/oprire de la distanță;
- suport pentru remote media (virtual CD);
- suport pentru SSL (Secure Socket Layer);
- monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice;
- managementul evenimentelor și alarmelor;
- inventarul și monitorizarea componentelor serverului (inclusiv GPU, module optice SFP);
- instalarea update-urilor și patch-urilor pentru componentele serverului;
- analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat;
- repornirea și reconfigurarea automată a serverului;
- integrarea cu Active Directory / LDAP;
- redirectare consolă serială;
- autentificare two-factor;
- integrare cu sisteme de management al virtualizarii;
- RESTFul API cu suport Redfish
- Interfețe acces utilizator: HTML5 Web GUI, SSH, telnet, redirecționare pe port serial;
- port dedicat Gigabit Ethernet ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului.

	Echipamentul trebuie livrat împreună cu aplicaţie pentru instalarea şi configurarea serverului dezvoltată de producătorul serverului capabilă de instalare în mod neasistat.
14.	**Aplicaţie Administrare**
	• Trebuie să permită administrarea şi monitorizarea serverelor dintr-o interfaţă centralizată, fără necesitatea de a instala agenţi; • Pentru a asigura compatibilitatea, aplicaţia trebuie să fie furnizată de acelaşi producător cu cel al serverelor; • Trebuie să permită inventarierea şi configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de reţea, plăci HBA, controllere RAID, unităţi de stocare; • Trebuie să permită update-uri de firmware, BIOS şi drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticităţii acestora; • Trebuie să permită generarea de fişiere de configurare şi posibilitatea aplicării lor pe alte servere din infrastructură; • Trebuie să permită instalarea sistemelor de operare şi virtualizare pe serverele aflate în administrare; • Permite stocarea pe un NAS extern cu funcţionalitate de retenţie a fişierelor, pentru a asigura protecţia la ştergere şi modificare a fişierelor de update, template-urilor de configurare şi imaginilor de sistem de operare; • Trebuie să ofere funcţionalitatea de validare a configuraţiei faţă de o referinţă; • Monitorizează starea de funcţionare a serverelor şi subcomponentelor: alerte, indicatori de performanţă şi consum de energie electrică; • Permite ştergerea securizată a unităţilor de stocare de tip SSD si HDD. • Trebuie să genereze grafice cu nivele de încărcare şi utilizare ale serverelor cu un istoric pe o perioada configurabilă de cel puţin 1 an Aplicaţia de administrare va fi instalată, configurată de către ofertant şi va cuprinde toate serverele.
15.	**Compatibilitate cu sisteme de operare**

	• VMware vSphere 8 • Red Hat Enterprise Linux 9 • Windows Server 2022 • Ubuntu 22.04 • Compatibilitatea cu sistemele de operare va fi probată prin menționarea sistemelor de calcul ofertate pe pagina web a producătorilor sistemelor de operare (HCL).
16.	**Conformitate cu standarde europene**
	Conformitate CE cu următoarele standarde europene în vigoare: • Siguranța în exploatare: 014/35/EU; • Echipamente de joasă tensiune: 014/35/EU; • Compatibilitate electromagnetica: 2014/30/EU; • Declarație RoHS: 2011/65/EU.
17.	**Alimentare cu energie electrică**
	• Surse de alimentare interne redundante (1+1) AC, 220V, 50 Hz • Cabluri IEC C13 la C14, minim 1,5m, certificate de producătorul echipamentului. Cablurile trebuie să fie prevăzute cu sistem de înlăturare accidentală la ambele capete.
18.	**Format**
	• Rackmountable 19", maxim 2U (2 rack unit).
19.	**Accesorii**
	• Echipamentele vor fi livrate împreună cu toate accesoriile necesare punerii în funcțiune chiar dacă acestea nu au fost solicitate în mod expres. • Va fi livrat împreuna cu kit-ul de montare în rack format din șine glisante (listate ca fiind compatibile pe site-ul producătorului) și alte elemente de montare, dacă este cazul.

20.	**Garanție și suport**
	• Soluția ofertată trebuie să beneficiaze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

Pentru optimizarea proceselor aferente bazelor de date, pot fi ofertate appliance-uri dedicate de procesare și stocare date, realizate de același producător cu cel al software-ului bazelor de date. Aceste appliance-uri vor fi montate în rack-urile deja existente ale beneficiarului, nefiind accepte appliance-uri care necesită în mod obligatoriu rack-uri customizate. Fiecare appliance de procesare trebuie să respecte următoarele cerințe minimale:

1.	**Procesor:**
	Serverul va fi echipat cu minim 2 procesoare x86 de ultimă generație, având următoarele caracteristici: • Frecventa: 2.6 GHz sau superior; • Număr de core-uri per procesor: minim 96 core-uri; • Număr procesoare instalate: minim 2; • Număr procesoare suportate: minim 2.
2.	**Memorie**
	• Minim 3 TB memorie RAM
3.	**Hard disk drive:**
	• Minim 2 x 3.84 TB NVMe Flash.
4.	**Interfața de rețea**
	• Minim 8 x Ethernet 10/25Gbps SFP28 echipate în configurația ofertată. Se vor livra minim două HBA-uri distincte pentru interfețele de tip SFP28. • Minim 2 interfete RoCE 100Gbps. • Interfața de rețea separată pentru administrare la distanță (diferită de cele 10 interfețe de rețea)
5.	**Sursa de alimentare**
	• Minim 2 surse hot plug, redundante instalate;.
6.	**Administrare**
	• Sistem incorporat de monitorizare a discurilor, ventilatoarelor, surselor de alimentare, temperaturii si administrare de la distanta;
7.	**Garanție și suport**
	• Soluția ofertată trebuie beneficiază de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate

	(firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

Fiecare appliance de stocare trebuie să respecte următoarele cerințe minimale:

1.	**Procesor:**
	Serverul va fi echipat cu minim 2 procesoare x86 de ultimă generație, având următoarele caracteristici: • Frecventa: 2.6 GHz sau superior; • Număr de core-uri per procesor: minim 32 core-uri; • Număr procesoare instalate: minim 2; • Număr procesoare suportate: minim 2.
2.	**Memorie**
	• Minim 256 GB memorie RAM
3.	**Capacitate de stocare instalată:**
	• Minim 50TB capacitate bruta de stocare realizata din module flash NVMe.
4.	**Interfața de rețea**
	• Minim 2 interfete RoCE 100Gbps. • Interfața de rețea separată pentru administrare la distanță (diferită de cele 2 interfețe de rețea)
5.	**Sursa de alimentare**
	• Minim 2 surse hot plug, redundante instalate;.
6.	**Administrare**
	• Sistem incorporat de monitoriuzare a discurilor, ventilatoarelor, surselor de alimentare, temperaturii si administrare d ela distanta;
7.	**Garanție și suport**
	• Soluția ofertată trebuie beneficiază de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță,folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea

	echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

În cazul în care se optează pentru ofertarea appliance-urilor dedicate de procesare și stocare baze de date acestea trebuie să fie livrate împreună cu minim 2 switch-uri cu porturi de 100Gb pentru interconectare, iar cantitățile minime, pentru fiecare tip de appliance, sunt următoarele:

- 3 appliance-uri dedicate de procesare baze de date
- 3 appliance-uri dedicate de stocare baze de date

Toate appliance-uril dedicate de procesare și stocare baze de date trebuie să includă toate licențele și componentele (hardware și software) necesare în vederea funcționării tuturor componentelor instalate în cadrul acestui sistem.

Pentru fiecare appliance dedicat de procesare baze de date ofertat se poate reduce cantitatea de servere tip 1 (punctul 4.4.1) ofertată cu 4 bucăți.

Capacitatea utilă a echipamentului de stocare tip 2 (punctul 4.4.4) poate fi redusă cu capacitatea utilă (rezultată după aplicarea mecanismelor de protecție a datelor) ofertată în cadrul appliance-urilor dedicate de stocare baze de date. Indiferent de capacitatea utilă ofertată în cadrul appliance-urilor dedicate de stocare baze de date, capacitatea utilă a echipamentului de stocare tip 2 (punctul 4.4.4) nu poate fi mai mică de 100TiB.

4.4.2 Echipament server tip 2

1.	**Descriere generală**
	• Echipament de tip server dual-socket pentru sisteme informatice • Răcire Front to Back
2.	**Procesor**
	Serverul va fi echipat cu minim 2 procesoare de tip Intel Xeon sau echivalent de ultimă generație, având următoarele caracteristici: • Frecventa: 2.8 GHz sau superior; • Bus Speed min 16GT/s; • Cache: 60 MB sau superior; • Număr de core-uri per procesor: minim 32 core-uri cu 64 fire de execuție; • Număr procesoare instalate: minim 2; • Număr procesoare suportate: minim 2.
3.	**Memorie**
	• Minim 1024 GB Registered ECC DDR5 memorie instalată, SDDC, • Minim 32 sloturi total (minim 16 libere) pentru memorie RAM cu suport pentru minimum 2 TB RAM. • Metode suportate de protecție a memoriei: Advanced ECC.
4.	**Hard disk drive:**
	• Minim 2 disk-uri SSD M.2 480GB care să poată fi configurate într-o matrice de tip RAID 1 • Serverul va fi echipat cu un număr minim de 8 bay-uri pentru disk-uri. • Sistemul trebuie livrat cu toate modulele și accesoriile necesare pentru instalarea discurilor în mod hot-swap.
5.	**Interfața grafică**

	• Minim 16MB memorie video
6.	**Securitate**
	• TPM 2.0; • Suport inclus pentru verificarea semnăturilor criptografice ale driverelor 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 inclus pentru verificarea și validarea autenticității firmware-ului componentelor critice ale 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 ofertat 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). Logurile 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; • Firmware rollback; • UEFI Server Firmware; • Posibilitatea de a dezactiva "Secure Boot".
7.	**Interfețe de rețea**
	• Minim 8 x Ethernet 25Gbps SFP28 echipate în configurația ofertată (8 buc Cablu DAC 25Gbps 3m incluse). Placile de retea trebuie sa aiba capabilitatea PXE boot. • Interfața de rețea RJ45 separată pentru administrare la distanță, diferită de cele 8 interfețe de rețea (1 buc patch CAT 6 3m inclusă). • Soluția ofertata trebuie sa beneficieze de Root of Trust – astfel încât sa permită verificarea actualizărilor de firmware printr-un set de chei criptografice scrise de

	către producător la nivel de controller hardware, permiţând astfel un nivel de securitate suplimentar fata de o verificare standard la nivel de firmware software
8.	**Sloturi de expansiune**
	• Minim 3 sloturi extensie PCIe din care minim 1 slot de tip PCIe x16 (cu 16 LANE-uri PCI Express conectate).
9.	**Conectori interfeţe I/O**
	• Minim: 1 x serial, 1 x VGA, minim 3 x USB din care minim 1 x USB 3.0
10.	**Carcasă**
	• Montabil în rack cu şine glisante. Serverul va fi echipat cu mecanism de închidere pentru a putea securiza accesul la discurile instalate.
11.	**Sursa de alimentare**
	• Minim 2 surse hot plug şi redundante instalate cu o putere minimă de 800W • Sursele, clasa Platinum sau echivalent, vor fi dimensionate pentru a permite echiparea maximală a serverului (număr maxim de discuri şi de module de memorie) fără necesitatea schimbării surselor.
12.	**Ventilatoare**
	• Ventilatoare redundante (N+1), hot plug
13.	**Administrare**
	Echipamentul trebuie să fie livrat cu capabilităţi hardware incluse pentru: • administrarea şi monitorizarea serverelor dintr-o interfaţă centralizată, fără necesitatea de a instala agenţi; • a asigura compatibilitatea, modulul hardware de administrare trebuie să fie furnizat de acelaşi producător cu cel al serverelor; • inventarierea şi configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de reţea, plăci HBA, controllere RAID, unităţi de stocare; • update-uri de firmware, BIOS şi drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticităţii acestora;

- generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură;
- funcționalitatea de validare a configurației față de o referință;
- monitorizarea stării de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică;
- instalare și configurare locală și la distanță, inclusiv configurare RAID;
- management operațional cu următoarele funcții: monitorizarea stării sistemului, managementul evenimentelor și alarmelor, inventarul componentelor, inventarul și instalarea update-urilor și patch-urilor, analiza performanței, diagnoza în timp real, repornirea și reconfigurarea automată a serverului;
- LCD display sau panou cu leduri; panoul LCD/LED livrat va permite citirea mesajelor de eroare fără operațiuni suplimentare;
- monitorizare a ventilatoarelor, surselor de alimentare și temperaturii, panou LCD sau cu LED-uri pentru diagnosticarea rapidă a stării de funcționare a componentelor critice: memorii, procesoare, surse de alimentare, ventilatoare, disk-uri, interfețe PCI, placă de bază;
- analize predictive de eroare (fără aplicație externă) pentru: disc-uri, memoriicu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componentele enumerate anterior (Predictive Failure Analysis);
- suport instalat și activat cu licențiere perpetuă pentru managementul serverului de la distanță (redirectare interfață grafică, tastatură și mouse, posibilitate de pornire/oprire de la distanță, suport SSL, SNMP, suport pentru remote virtual media).

Sistemul de management trebuie să fie echipat cu următoarele facilitați:

- management de la distanță;
- redirectare interfață grafică cu tastatură și mouse;
- posibilitate de pornire/oprire de la distanță;
- suport pentru remote media (virtual CD);

	• suport pentru SSL (Secure Socket Layer); • monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice; • managementul evenimentelor și alarmelor; • inventarul și monitorizarea componentelor serverului (inclusiv GPU, module optice SFP); • instalarea update-urilor și patch-urilor pentru componentele serverului; • analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat; • repornirea și reconfigurarea automată a serverului; • integrarea cu Active Directory / LDAP; • redirectare consolă serială; • autentificare two-factor; • integrare cu sisteme de management al virtualizarii; • RESTFul API cu suport Redfish • Interfețe acces utilizator: HTML5 Web GUI, SSH, telnet, redirecționare pe port serial; • port dedicat Gigabit Ethernet ce permite accesarea sistemului de management indiferent de stadiul de funcționare a serverului. Echipamentul trebuie livrat împreună cu aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului capabilă de instalare în mod neasistat.
14.	**Aplicație Administrare**
	• Trebuie să permită administrarea 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 serverelor;

	• Trebuie să permită inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, plăci HBA, controllere RAID, unități de stocare; • Trebuie să permită update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătura 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 NAS extern cu funcționalitate de retenție a fișierelor, 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; • Aplicația de administrare va fi instalată, configurată de către ofertant și va permite administrarea tuturor serverelor.
15.	**Compatibilitate cu sisteme de operare**
	• VMware vSphere 8 • Red Hat Enterprise Linux 9 • Windows Server 2022 • Ubuntu 22.04 • Compatibilitatea cu sistemele de operare va fi probată prin menționarea sistemelor de calcul ofertate pe pagina web a producătorilor sistemelor de operare (HCL).

16.	**Conformitate cu standarde europene**
	Conformitate CE cu următoarele standarde europene în vigoare: • Siguranţa în exploatare: 014/35/EU; • Echipamente de joasă tensiune: 014/35/EU; • Compatibilitate electromagnetica: 2014/30/EU; • Declaraţie RoHS: 2011/65/EU.
17.	**Alimentare cu energie electrică**
	• Surse de alimentare interne redundante (1+1) AC, 220V, 50 Hz • Cabluri IEC C13 la C14, minim 1,5m, certificate de producătorul echipamentului. Cablurile trebuie să fie prevăzute cu sistem de înlăturare accidentală la ambele capete.
18.	**Format**
	• Rackmountable 19", maxim 1U (1 rack unit).
19.	**Accesorii**
	• Echipamentele vor fi livrate împreună cu toate accesoriile necesare punerii în funcţiune chiar dacă acestea nu au fost solicitate în mod expres. • Va fi livrat împreuna cu kit-ul de montare în rack format din şine glisante (listate ca fiind compatibile pe site-ul producătorului) şi alte elemente de montare, dacă este cazul.
20.	**Garanţie şi suport**
	• Soluţia ofertată trebuie să beneficiaze de servicii de garanţie şi suport pentru minim 5 ani de la data recepţiei, având SLA 24x7 timp de răspuns 4 ore şi servicii de mentenanţă, folosind un canal de comunicare între centrul de date al autorităţii contractante şi centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect şi înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanţia hardware va fi de minim 60 de luni.

	• Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

4.4.3 Echipament stocare tip 1

1.	**Descriere**
	• Echipament de stocare de înaltă performanță, cu rol de suport pentru stocarea datelor aferente componentei Big Data și alte date cu cerințe ridicate de performanță • Echipament de stocare multi-controller de ultimă generație, cu caracteristici de performanță de nivel înalt;
2.	**Arhitectură**
	• Echipamentul de stocare de înaltă performanță va fi echipat cu cel puțin 2 controller-e SAN active, scalabil la min. 4 controller-e SAN active, pentru a asigura o configurație redundantă de tip cluster activ-activ la nivelul echipamentului;

	• Controller-ele trebuie să fie de tip hot-swap; • Echipamentul trebuie să asigure o disponibilitate de 99.9999%
3.	**Protocol de acces la date**
	• Echipamentul de stocare va permite acces la datele stocate prin protocoale de tip block (SAN): FC (Fiber Channel) şi iSCSI;
4.	**Porturi acces host-uri**
	• Echipamentul de stocare ofertat va dispune de minim 16 porturi 25GbE. În funcţie de tipul porturilor echipamentului (electrice sau optice), acesta va fi livrat fie cu module optice (pentru echipament şi switch-urile de tip leaf în care va fi conectat) şi fibre optice necesare interconecării tuturor porturilor de 25GbE ale echipamentului, fie cu cabluri DAC cu lungimea de 25GbE 3 m. • Porturile vor fi distribuite în mod egal pe fiecare controller din echipamentul de stocare ofertat;
5.	**Memorie**
	• Echipamentul de stocare va avea instalată o cantitate de memorie pentru cache global şi management de metadate, de minim 1.5 TB per sistem ofertat din care minim 50% RAM; • Scalabilitate la 3 TB memorie cache global, prin adăugarea de controller-e adiţionale; • Memoria RAM trebuie să fie protejată prin mecanisme de mirroring pe mediu non-volatil, în cazul unor avarii la sistemul de alimentare electrică;
6.	**Nivele RAID**
	• Echipamentul de stocare ofertat va asigura configurarea şi optimizarea matricelor RAID sau echivalent în configuraţii cu minim două discuri de paritate asociate fiecărui set de discuri componente al unei matrice RAID sau echivalent; • Sistemul de stocare trebuie să includă drive-uri flash hot-spare sau capacitate adiţională pentru hot-spare, conform bunelor practici definite de producătorul

	echipamentului, având disponibil cel puțin două drive-uri flash sau echivalent capacitate de stocare hot-spare distribuită pe toate modulele din echipament;
7.	**Tehnologie stocare**
	• Suport pentru echipare și expansiune cu medii de stocare de tip flash;
8.	**Capacitate instalată**

	• Echipamentul de stocare de înaltă performanță va fi echipat cu o capacitate de stocare minimă ce se va încadra în următorii parametri:
	  • Cel puțin 250 TiB capacitate de stocare utilă totală rezultată în urma configurării în RAID (sau echivalent) cu dublă paritate.
	  • Pentru seturi de date tip baze de date SQL, mașini virtuale, echipamentul de stocare ofertat va asigura cel puțin 500 TiB capacitate de stocare totală efectivă garantată de către ofertant, prin deduplicarea și compresia inline a datelor. În cazul neîndeplinirii cerinței minimale 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 solicitate.
	  • Capacitatea de stocare utilă va fi realizată din medii de stocare de tip flash, hot-swap, de aceeași capacitate, în proporție de 100%;

9.	**Performanță**
	Echipamentul de stocare ofertat trebuie să livreze cel puțin 300000 IOPS cu un profil de 50% rată de citire, 50% rată de scriere, 70% random, 30% secvențial, dimensiune IO de 32KB. 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 < 1 ms; Parametrii vor fi demonstrați printr-un raport certificat de producător pentru configurația propusă.

10.	**Extensia capacității de stocare**
	Echipamentul de stocare va asigura următoarea capabilitate minimă de extensie a capacității de stocare: • Suport pentru cel puțin 180 de drive-uri flash în interiorul sistemului de stocare, de tip hot-swap, prin adăugarea de module de expansiune și/sau controllere; • Suport pentru module de expansiune cu sloturi de 2,5"; • Modulele de expansiune se vor conecta la echipamentul de stocare prin magistrale de date redundante. • În cazul în care, pentru interconectarea redundantă a nodurilor/modulelor de expansiune și pentru extensia ulterioară, sistemul de stocare necesită echipamente de interconectare de tip switch, atunci acesta va fi livrat cu minim două switch-uri configurate in HA sau echivalent. • Echipamentul de stocare suportă scalabilitate la minim 2 PiB capacitate de stocare utilă a datelor;
11.	**Managementul platformei**
	• Echipamentul de stocare va asigura un sistem de management și monitorizare accesibil pe o interfata de retea dedicata; • Echipamentul de stocare va asigura monitorizarea performanței și capacității platformei de stocare; • Echipamentul de stocare trebuie să includă fără costuri adiționale cel puțin posibilitatea administrării prin intermediul unei interfețe web securizate SSL și/sau aplicație dedicată de management, precum și consola de administrare la distanță SSH/Telnet. Toate funcțiile native ale sistemului de stocare, precum și funcționalitatea licențiată separat vor fi accesibile în mod integrat prin intermediul acestor unelte de administrare, astfel încât operațiunile de configurare și administrare vor putea fi efectuate indiferent de locație și de modalitatea de acces; • Atât în scop administrativ cât și în vederea accesului la seturile de date, platforma de stocare va permite nativ definirea de utilizatori locali și roluri de utilizare, cu seturi diferite de permisiuni granulare, aplicabile acțiunilor administrative și/sau seturilor de date. De asemenea, va permite integrarea cu un sistem director de tip

LDAP, pentru sincronizarea utilizatorilor și a drepturilor de acces la seturile de date partajate de sistem.

- Echipamentul va permite integrarea cu un sistem NTP/SNTP pentru sincronizarea informațiilor de timp.
- Uneltele de administrare prin interfața web și/sau aplicație dedicată vor fi ușor de folosit și vor implementa majoritatea acțiunilor administrative (definirea de volume, LUN-uri, exportul seturilor de date indiferent de protocolul folosit pentru export, configurarea funcțiilor de partajare, optimizare și backup, adăugarea/eliminarea de noduri la/din cluster, definirea relațiilor de replicare, etc) într-o singură interfață, fără a fi nevoie de acces la uneltele în linie de comandă, iar pentru un număr de operațiuni importante de configurare va pune la dispoziție asistenți de configurare.
- De asemenea, va integra un panou unificat de afișare a informațiilor legate de performanță (inclusiv gradul de ocupare al procesoarelor, nivel I/O, latență în funcție de protocolul de comunicație și tipul de export al volumelor, numărul de operațiuni efectuate asupra seturilor de date), informațiilor legate de gradul de ocupare (inclusiv gradul de ocupare per volum de date și tipul de partajare al resurselor), respectiv afișarea informațiilor legate de starea controller-elor, a relațiilor de replicare între echipamente și a evenimentelor informaționale și/sau de alertare survenite în funcționarea oricărui element hardware sau funcție software;
- Interfața grafică de administrare trebuie să fie de tip HTML5;
- Pentru asigurarea unui nivel optim de disponibilitate operațională, echipamentul de stocare ofertat va asigura update și upgrade software și hardware al platformei fără întreruperea serviciilor.
- Ca parte a funcțiilor de administrare și diagnosticare, echipamentul de stocare trebuie să includă standard un mecanism de alertare pe e-mail, configurabil pentru un set specific de adrese e-mail și/sau către o platforma de suport disponibilă la producătorul sistemului de stocare. De asemenea, va permite integrarea în unelte dedicate de management al infrastructurilor prin suport complet pentru protocolul SNMP si prin existența în mod gratuit a descriptorilor și parametrilor platformei astfel încât integrarea se va face în mod facil în uneltele de management ce nu au implicit profile definite pentru sistemul specific preconizat. Tot în scopul operațiunilor de management și diagnosticare sistemul va integra un set de LED-uri ce afișează cel puțin starea curentă a echipamentului;

12.	**Optimizarea capacitaţii de stocare**
	• Echipamentul de stocare va avea capabilităţi de tip „Thin Provisioning" (alocarea către nodurile de procesare a unei capacităţi de stocare mai mare decât cea fizic disponibilă) „Deduplicare Inline" (reducerea în timp real a blocurilor de date identice la un singur set de blocuri de date unice în vederea optimizării spaţiului de stocare), respectiv capabilităţii de tip „Compresie Inline" (compresia în timp real a blocurilor de date unice în vederea optimizării spaţiului de stocare); • Echipamentul de stocare va asigura rebalansarea datelor pe matricele de discuri în cazul în care sunt adăugate discuri suplimentare;
13.	**Protecţia şi replicarea datelor**
	• Echipamentul de stocare va avea încorporate componente ce asigură protecţia controller-elor şi a memoriei cache la căderile de curent prin salvarea automată a datelor din cache pe mediile de stocare, înainte de oprirea echipamentului; • Echipamentul de stocare trebuie să includă mecanisme de realizare a: o snapshot-urilor manual şi în mod programabil, cu opţiune de retenţie şi ştergere automată a acestora atunci când expiră (Scheduled Snapshot); o clone ale volumelor de date, cu impact minimal asupra performanţelor echipamentului de stocare; o resincronizării copiilor locale integrale, de tip clonă, fără rescrierea în totalitate a acestora dacă există date istorice, chiar şi după intervale lungi de timp sau chiar dacă relaţia dintre volume a fost eliminată la un moment dat; • Echipamentul de stocare ofertat trebuie să includă funcţionalitate de criptare a datelor (validată FIPS 140-2) prin mecanism AES-256, pentru toate mediile de stocare instalate în sistem; • Va include licenţele necesare pentru tipuri diferite de replicare date la distanţă (sincron, asincron); • Toate funcţionalităţile software solicitate mai sus vor fi incluse în configuraţia ofertată a echipamentului de stocare, licenţiate perpetuu, pentru întreaga capacitate de stocare ofertată;
14.	**Sisteme de operare suportate**

	Echipamentul de stocare va suporta minim următoarele sisteme de operare: • Microsoft Windows Server; • VMware vSphere; • Linux;
15.	**Alimentare**
	• Cabluri IEC C13 la C14, minim 1,5m, certificate de producătorul echipamentului. Cablurile trebuie să fie prevăzute cu sistem de înlăturare accidentală la ambele capete. • Surse de alimentare interne redundante AC, 220V, 50 Hz • Pentru asigurarea redundanței complete a echipamentului propus fiecare element major component al echipamentului de stocare (controller, șasiu discuri, etc) trebuie să ofere alimentare redundantă prin cel puțin două surse independente de alimentare. Sursele trebuie să ofere funcționalitate hot-swap pentru înlocuirea rapidă, fără oprirea alimentării sistemului și fără întreruperea serviciilor asigurate de platformă;
16.	**Ventilație**
	• Toate elementele de asigurare a ventilației sistemului trebuie să fie de tip hot-swap pentru înlocuirea lor rapidă în caz de avarie, fără întreruperea funcționalităților oferite de echipamentul de stocare;
17.	**Cerințe constructive**
	• Echipamentul de stocare trebuie să fie montabil în rack-uri standard de 19"; Se vor folosi rack-urile existente de 19"; • Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporți, șuruburi/captive);
18.	**Accesorii**
	• Sistemul ofertat va fi livrat împreună cu toate accesoriile necesare, inclusiv pentru conectarea extensiilor si a punerii în funcțiune, chiar dacă acestea nu au fost solicitate în mod expres.

19.	**Garanţie şi suport**
	• Soluţia ofertată trebuie să beneficiaze de servicii de garanţie şi suport pentru minim 5 ani de la data recepţiei, având SLA 24x7 timp de răspuns 4 ore şi servicii de mentenanţă, folosind un canal de comunicare între centrul de date al autorităţii contractante şi centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect şi înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanţia hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcţionare şi solicitarea rezolvării acestora în funcţie de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terţ. De asemenea, se va asigura dreptul de a face update-uri şi upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri şi au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiţionale. • Toate funcţionalităţile software solicitate vor include licenţiere perpetuă pentru întreaga configuraţie a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi şi să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricaţie a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

4.4.4 Echipament stocare tip 2

1.	**Descriere**
	• Echipament de stocare de înaltă performanță, cu rol de suport pentru stocarea datelor aferente bazelor de date relaționale, mediilor virtuale și alte date cu cerințe ridicate de performanță • Echipament de stocare multi-controller de ultimă generație, cu caracteristici de performanță de nivel înalt;
2.	**Arhitectură**
	• Echipamentul de stocare de înaltă performanță va fi echipat cu cel puțin 2 controller-e SAN active, scalabil la min. 4 controller-e SAN active, pentru a asigura o configurație redundantă de tip cluster activ-activ la nivelul echipamentului; • Controller-ele trebuie să fie de tip hot-swap; • Echipamentul trebuie să asigure o disponibilitate de 99.9999%
3.	**Protocol de acces la date**
	• Echipamentul de stocare va permite acces la datele stocate prin protocoale de tip block (SAN): FC (Fiber Channel) și iSCSI;
4.	**Porturi acces host-uri**
	• Echipamentul de stocare ofertat va dispune de minim 16 porturi 25GbE. În funcție de tipul porturilor echipamentului (electrice sau optice), acesta va fi livrat fie cu module optice (pentru echipament și switch-urile de tip leaf în care va fi conectat) și fibre optice necesare interconecării tuturor porturilor de 25GbE ale echipamentului, fie cu cabluri DAC cu lungimea de 25GbE 3 m. • Porturile vor fi distribuite în mod egal pe fiecare controller din echipamentul de stocare ofertat;
5.	**Memorie**
	• Echipamentul de stocare va avea instalată o cantitate de memorie pentru cache global și management de metadate, de minim 1 TB per sistem ofertat din care minim 50% RAM;

	• Scalabilitate la 2 TB memorie cache global, prin adăugarea de controller-e adiţionale; • Memoria RAM trebuie să fie protejată prin mecanisme de mirroring pe mediu non-volatil, în cazul unor avarii la sistemul de alimentare electrică;
6.	**Nivele RAID**
	• Echipamentul de stocare ofertat va asigura configurarea şi optimizarea matricelor RAID sau echivalent în configuraţii cu minim două discuri de paritate asociate fiecărui set de discuri componente al unei matrice RAID sau echivalent; • Sistemul de stocare trebuie să includă drive-uri flash hot-spare sau capacitate adiţională pentru hot-spare, conform bunelor practici definite de producătorul echipamentului, având disponibil cel puţin două drive-uri flash sau echivalent capacitate de stocare hot-spare distribuită pe toate modulele din echipament;
7.	**Tehnologie stocare**
	• Suport pentru echipare şi expansiune cu medii de stocare de tip flash;
8.	**Capacitate instalată**

	• Echipamentul de stocare de înaltă performanţă va fi echipat cu o capacitate de stocare minimă ce se va încadra în următorii parametri:
	  • Cel puţin 500 TiB capacitate de stocare utilă totală rezultată în urma configurării în RAID (sau echivalent) cu dublă paritate.
	  • Pentru seturi de date tip baze de date SQL, maşini virtuale, echipamentul de stocare ofertat va asigura cel puţin 1000 TiB capacitate de stocare totală efectivă garantată de către ofertant, prin deduplicarea şi compresia inline a datelor. În cazul neîndeplinirii cerinţei minimale de capacitate de stocare efectivă, ofertantul va asigura în mod gratuit drive-uri flash adiţionale, controllere (dacă este cazul) şi toate componentele necesare asigurării capacităţii de stocare utile efective solicitate.
	  • Capacitatea de stocare utilă va fi realizată din medii de stocare de tip flash NVMe, hot-swap, de aceeaşi capacitate, în proporţie de 100%;

9.	**Performanţă**

	Echipamentul de stocare ofertat trebuie să livreze cel puțin 300000 IOPS cu un profil de 50% rată de citire, 50% rată de scriere, 70% random, 30% secvențial, dimensiune IO de 32KB. 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 < 1 ms; Parametrii vor fi demonstrați printr-un raport certificat de producător pentru configurația propusă.
10.	**Extensia capacității de stocare**
	Echipamentul de stocare va asigura următoarea capabilitate minimă de extensie a capacității de stocare: • Suport pentru cel puțin 180 de drive-uri flash în interiorul sistemului de stocare, de tip hot-swap, prin adăugarea de module de expansiune și/sau controllere; • Suport pentru module de expansiune cu sloturi de 2,5"; • Modulele de expansiune se vor conecta la echipamentul de stocare prin magistrale de date redundante. • În cazul în care, pentru interconectarea redundantă a nodurilor/modulelor de expansiune și pentru extensia ulterioară, sistemul de stocare necesită echipamente de interconectare de tip switch, atunci acesta va fi livrat cu minim două switch-uri configurate in HA sau echivalent. • Echipamentul de stocare suportă scalabilitate la minim 2 PiB capacitate de stocare utilă a datelor;
11.	**Managementul platformei**
	• Echipamentul de stocare va asigura un sistem de management și monitorizare accesibil pe o interfata de retea dedicata; • Echipamentul de stocare va asigura monitorizarea performanței și capacității platformei de stocare;

- Echipamentul de stocare trebuie să includă fără costuri adiţionale cel puţin posibilitatea administrării prin intermediul unei interfeţe web securizate SSL şi/sau aplicaţie dedicată de management, precum şi consola de administrare la distanţă SSH/Telnet. Toate funcţiile native ale sistemului de stocare, precum şi funcţionalitatea licenţiată separat vor fi accesibile în mod integrat prin intermediul acestor unelte de administrare, astfel încât operaţiunile de configurare şi administrare vor putea fi efectuate indiferent de locaţie şi de modalitatea de acces;
- Atât în scop administrativ cât şi în vederea accesului la seturile de date, platforma de stocare va permite nativ definirea de utilizatori locali şi roluri de utilizare, cu seturi diferite de permisiuni granulare, aplicabile acţiunilor administrative şi/sau seturilor de date. De asemenea, va permite integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor şi a drepturilor de acces la seturile de date partajate de sistem.
- Echipamentul va permite integrarea cu un sistem NTP/SNTP pentru sincronizarea informaţiilor de timp.
- Uneltele de administrare prin interfaţa web şi/sau aplicaţie dedicată vor fi uşor de folosit şi vor implementa majoritatea acţiunilor administrative (definirea de volume, LUN-uri, exportul seturilor de date indiferent de protocolul folosit pentru export, configurarea funcţiilor de partajare, optimizare şi backup, adăugarea/eliminarea de noduri la/din cluster, definirea relaţiilor de replicare, etc) într-o singură interfaţă, fără a fi nevoie de acces la uneltele în linie de comandă, iar pentru un număr de operaţiuni importante de configurare va pune la dispoziţie asistenţi de configurare.
- De asemenea, va integra un panou unificat de afişare a informaţiilor legate de performanţă (inclusiv gradul de ocupare al procesoarelor, nivel I/O, latenţă în funcţie de protocolul de comunicaţie şi tipul de export al volumelor, numărul de operaţiuni efectuate asupra seturilor de date), informaţiilor legate de gradul de ocupare (inclusiv gradul de ocupare per volum de date şi tipul de partajare al resurselor), respectiv afişarea informaţiilor legate de starea controller-elor, a relaţiilor de replicare între echipamente şi a evenimentelor informaţionale şi/sau de alertare survenite în funcţionarea oricărui element hardware sau funcţie software;
- Interfaţa grafică de administrare trebuie să fie de tip HTML5;

	• Pentru asigurarea unui nivel optim de disponibilitate operațională, echipamentul de stocare ofertat va asigura update și upgrade software și hardware al platformei fără întreruperea serviciilor. • Ca parte a funcțiilor de administrare și diagnosticare, echipamentul de stocare trebuie să includă standard un mecanism de alertare pe e-mail, configurabil pentru un set specific de adrese e-mail și/sau către o platforma de suport disponibilă la producătorul sistemului de stocare. De asemenea, va permite integrarea în unelte dedicate de management al infrastructurilor prin suport complet pentru protocolul SNMP si prin existența în mod gratuit a descriptorilor și parametrilor platformei astfel încât integrarea se va face în mod facil în uneltele de management ce nu au implicit profile definite pentru sistemul specific preconizat. Tot în scopul operațiunilor de management și diagnosticare sistemul va integra un set de LED-uri ce afișează cel puțin starea curentă a echipamentului;
12.	**Optimizarea capacitații de stocare**
	• Echipamentul de stocare va avea capabilități de tip „Thin Provisioning" (alocarea către nodurile de procesare a unei capacități de stocare mai mare decât cea fizic disponibilă) „Deduplicare Inline" (reducerea în timp real a blocurilor de date identice la un singur set de blocuri de date unice în vederea optimizării spațiului de stocare), respectiv capabilității de tip „Compresie Inline" (compresia în timp real a blocurilor de date unice în vederea optimizării spațiului de stocare); • Echipamentul de stocare va asigura rebalansarea datelor pe matricele de discuri în cazul în care sunt adăugate discuri suplimentare;
13.	**Protecția și replicarea datelor**
	• Echipamentul de stocare va avea încorporate componente ce asigură protecția controller-elor și a memoriei cache la căderile de curent prin salvarea automată a datelor din cache pe mediile de stocare, înainte de oprirea echipamentului; • Echipamentul de stocare trebuie să includă mecanisme de realizare a: o snapshot-urilor manual și în mod programabil, cu opțiune de retenție și ștergere automată a acestora atunci când expiră (Scheduled Snapshot); o clone ale volumelor de date, cu impact minimal asupra performanțelor echipamentului de stocare; o resincronizării copiilor locale integrale, de tip clonă, fără rescrierea în totalitate a acestora dacă există date istorice, chiar și după intervale lungi

	de timp sau chiar dacă relaţia dintre volume a fost eliminată la un moment dat; • Echipamentul de stocare ofertat trebuie să includă funcţionalitate de criptare a datelor (validată FIPS 140-2) prin mecanism AES-256, pentru toate mediile de stocare instalate în sistem; • Va include licenţele necesare pentru tipuri diferite de replicare date la distanţă (sincron, asincron); • Toate funcţionalităţile software solicitate mai sus vor fi incluse în configuraţia ofertată a echipamentului de stocare, licenţiate perpetuu, pentru întreaga capacitate de stocare ofertată;
14.	**Sisteme de operare suportate**
	Echipamentul de stocare va suporta minim următoarele sisteme de operare: • Microsoft Windows Server; • VMware vSphere; • Linux;
15.	**Alimentare**
	• Cabluri IEC C13 la C14, minim 1,5m, certificate de producătorul echipamentului. Cablurile trebuie să fie prevăzute cu sistem de înlăturare accidentală la ambele capete. • Surse de alimentare interne redundante AC, 220V, 50 Hz • Pentru asigurarea redundanţei complete a echipamentului propus fiecare element major component al echipamentului de stocare (controller, saşiu discuri, etc) trebuie să ofere alimentare redundantă prin cel puţin două surse independente de alimentare. Sursele trebuie să ofere funcţionalitate hot-swap pentru înlocuirea rapidă, fără oprirea alimentării sistemului şi fără întreruperea serviciilor asigurate de platformă;
16.	**Ventilaţie**

	• Toate elementele de asigurare a ventilației sistemului trebuie să fie de tip hot-swap pentru înlocuirea lor rapidă în caz de avarie, fără întreruperea funcționalităților oferite de echipamentul de stocare;
17.	**Cerințe constructive**
	• Echipamentul de stocare trebuie să fie montabil în rack-uri standard de 19"; Se vor folosi rack-urile existente de 19"; • Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporți, șuruburi/captive);
18.	**Accesorii**
	• Sistemul ofertat va fi livrat împreună cu toate accesoriile necesare, inclusiv pentru conectarea extensiilor si a punerii în funcțiune, chiar dacă acestea nu au fost solicitate în mod expres.
19.	**Garanție și suport**
	• Sistemul ofertat trebuie să beneficiaze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale.

	• Toate funcţionalităţile software solicitate vor include licenţiere perpetuă pentru întreaga configuraţie a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi şi să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricaţie a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

4.4.5 Echipament stocare tip 3

1.	**Descriere generală**
	• Echipamentul este destinat pentru stocarea imaginilor şi a altor documente gestionate de către sistem la nivel central. • Echipamentul de stocare enterprise de tip obiect trebuie să fie de tip cluster multi-nod cu capabilităţi de procesare şi de stocare, având posibilitatea de a replica datele la distanţă, către sisteme similare multiple şi să permită accesul de tip activ-activ la datele stocate în centrele de date; • Arhitectura echipamentului trebuie să fie de tip scale-out;
2.	**Capacitate instalată**
	• Echipamentul trebuie să includă cel puţin 1.5 PiB capacitate de stocare utilă (fără deduplicare, compresie sau alte mecanisme de extindere virtuală a spaţiului de stocare) rezultată după configurarea redundanţei pentru stocarea datelor, configuraţie ce va asigura integritatea datelor în cazul defectării simultane a două discuri, respectiv a unui întreg nod. • Echipamentul ofertat trebuie să includă cel puţin 4 noduri pentru asigurarea unui nivel ridicat de performanţă şi disponibilitate pentru procesele de salvare a datelor precum şi pentru asigurarea unei politici avansate de protecţie şi redundanţă la nivel de nod şi de disc. • Fiecare nod trebuie să fie echipat cu minim 128GB RAM şi 960GB SSD pentru accelerarea datelor.
3.	**Scalabilitate**

	• Echipamentul trebuie să includă toate componentele active de conectare între noduri, în mod redundant și scalabil, pentru a permite conectarea ulterioară online a altor noduri, cu menținerea nivelului de performanță; • Conexiunile de rețea către fiecare nod al echipamentului trebuie să fie redundante și scalabile permițând adăugarea online de noduri suplimentare fără necesitatea de a modifica arhitectura rețelei; • Echipamentul trebuie să permită scalarea, prin adăugarea de noi noduri cu capabilități de procesare și stocare, în timp ce acesta este online, fără întreruperea accesului la date.
4.	**Funcționalități**
	• Echipamentul va permite integrarea cu mecanisme de redistribuție automată a sarcinii de acces la nodurile de stocare în funcție de disponibilitatea și gradul de încărcare al fiecărui nod de stocare; • Echipamentul va permite integrarea cu aplicații multiple în paralel, pentru eficientizarea proceselor de administrare a fișierelor ce aparțin diferitelor aplicații ale sistemului informatic; • Echipamentul trebuie să permită accesul nativ prin protocol S3 fără utilizarea vreunui server fizic sau mașină virtuală externă de tip "gateway"; • Echipamentul va putea oferi servicii de partajare de tip "multi-tenant"; • Echipamentul trebuie să poată susține fluxuri de scriere și citire prin protocoalele solicitate, indiferent de sursa datelor sau a aplicațiilor ce utilizează datele; • Echipamentul trebuie să includă standarde de securitate a datelor prin mecanisme de tip WORM (Write Once, Read Many); • Echipamentul va include un serviciu nativ de indexare a obiectelor cu posibilitatea de căutare după proprietățile acestora; • Toate funcționalitățile software solicitate vor fi incluse în configurația ofertată a echipamentului, licențiate perpetuu, pentru întreaga capacitate de stocare ofertată;
5.	**Replicare**

	• Soluția va oferi mecanisme, licențiate perpetuu, de a replica datele la distanță, către sisteme similare multiple, situate în locații diferite.
6.	**Administrare**
	• Echipamentul va fi prevăzut cu interfața grafică de tip web și va asigura servicii de automatizare, raportare și administrare; • Monitorizarea echipamentului va afișa implicit starea nodurilor, nivelul de performanță, latența la scriere și citire, capacitatea utilizată, eficiența sistemului, alertele critice și starea procesului de replicare; • Echipamentul va integra agenți de tip SNMP pentru servicii externe de monitorizare prin MIB (Management Information Based) și syslog pentru servicii de auditare și alertare; • Echipamentul trebuie să permită integrarea cu aplicații de monitorizare și control prin integrare cu interfețe standard de tip REST API;
7.	**Interfețe de rețea**
	• Fiecare nod component al sistemului de stocare enterprise de tip obiect va include minim 4 x Ethernet 25Gbps SFP28 echipate în configurația ofertată (4 buc Cablu DAC 25Gbps incluse). • Interfața de rețea separată pentru administrare la distanță (1 buc patch CAT6 3m inclusă).
8.	**Conformitate cu standarde europene**
	Conformitate CE cu următoarele standarde europene în vigoare: • Siguranța în exploatare: 014/35/EU; • Echipamente de joasă tensiune: 014/35/EU; • Compatibilitate electromagnetica: 2014/30/EU; • Declarație RoHS: 2011/65/EU.
9.	**Alimentare cu energie electrică**
	• Fiecare nod component al sistemului de stocare enterprise de tip obiect va include minim două surse de alimentare redundante, hot-swap.

	• Cabluri IEC C13 la C14, minim 1,5m, certificate de producătorul echipamentului. Cablurile trebuie să fie prevăzute cu sistem de înlăturare accidentală la ambele capete.
10.	**Format**
	• Sistemul ofertat trebuie să permită montarea într-un rack standard de centru de date, de 19" și va include kit-ul de montaj în rack.
11.	**Accesorii**
	• Sistemul ofertat va fi livrat împreună cu toate accesoriile necesare punerii în funcțiune chiar dacă acestea nu au fost solicitate în mod expres.
12.	**Garanție și suport**
	• Sistemul ofertat trebuie să beneficiaze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia.

	• Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

4.4.6 Switch Distributie

Descriere generală:	Switch de distribuție
Specificații hardware	48 interfețe 1/10/25 Gigabit Ethernet dintre care 10 porturi echipate cu module 10GBase-SR 4 x 40/100 GbE QSFP dintre care 2 porturi echipate cu module QSFP 100GBase-SR4 MTP/MPO MM, OM4 2 x patch FO MTP/MPO MM,850 nm,10m. Posibilitate de stackare, cablurile și interfețele necesare vor fi incluse în ofertă. 1 x port consolă. 1 x port USB.
Performanțe minimale:	Capacitate de switching: 3.2 Tbps MTU configurabil pana la jumbo frames: 9216 bytes Număr adrese MAC: 82000 Număr total rute IPv4: 250000 Număr totsl rute IPv6: 190000
Caracteristici minimale incluse:	4094 VLAN-uri 2000 ACL-uri Auto negociere pe toate porturile Servicii QoS NTP Voice Vlan Private Vlan Autentificare TACACS+ si RADIUS SSH v2 MSTP Criptare MACsec: AES-256 Suport pentru OSPF, VRRP, PBR Suport pentru rute statice IPv4 si IPv6
Protocoale și standarde	IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS Prioritization IEEE 802.1Q VLAN IEEE 802.1s (MSTP)

	IEEE 802.1w IEEE 802.1X IEEE 802.1ab (LLDP) IEEE 802.1AE MACsec IEEE 802.3ae 10G IEEE 802.3ba 40G IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3x 100BASE-TX and 1000BASE-T IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X RMON I and II standards SNMP v1, v2c, and v3 IEEE 802.3az
Management	Configurare CLI, SSH, Web, consola. Nu se accepta echipamente a caror configurare se face exclusiv folosind un client adiacent. Toate functionalitatile echipamentului cerute in prezentul caiet de sarcini se pot configura utilizand metodele de management specificate mai sus. Nu se accepta echipamente de tip "cloud-based".
Licențe și software	Licență pentru toate porturile active simultan la viteza maxima. Licență pentru activarea tuturor porturilor. Licență activă pentru servicii Layer 2. Licență activă pentru servicii Layer 3. Licențele ofertate trebuie să asigure funcționalitățile și suportul pentru protocoalele solicitate in caietul de sarcini.
Alimentare cu energie electrică:	Doua surse de alimentare interne instalate cu suport pentru standarde UE. Sursele de alimentare trebuie sa fie redundante si de tip « hot swappable» .
Răcire	Ventilatoare redundante Un ventilator defect nu va afecta performanțele echipamentului
Dimensiuni	1RU
Servicii suport	Garantie si Suport hardware 8x5:5 ani Update software inclus: 5 ani Acces direct la suportul tehnic al fabricantului: 5 ani Furnizorul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice pe site-ul producătorului echipamentele, având ca și client final beneficiarul. Raportul va trebui să conțină pentru fiecare componentă cel puțin seria și perioada activată de suport

Accesorii:	1 X cablu consolă USB 2 X cablu de alimentare energie electrică tip schuko conform standardelor românești 1 X kit de instalare cu toate cablurile de protecție (împământare), șuruburile, cât și alte accesorii necesare instalării și punerii în funcțiune incluse

4.4.7 Firewall border

Descriere generală	– Echipament integrat de protecție în rețea cu capabilități de scanare antivirus, controlul aplicațiilor și prevenirea intruziunilor destinat folosirii ca o soluție de securitate unificata.
Specificații hardware	– 30 x interfețe 10GbE; – 6 x interfețe 100GbE QSFP28; – 2 x interfețe pentru HA, de minim 10Gbps; – 2 x interfața pentru Management; – 1 x port USB; – 1 x consola;
Performanța sistemului	– Firewall Throughput: 380 Gbps; – IPSec VPN Throughput (AES256-SHA256): 100 Gbps; – IPS Throughput: 35 Gbps; – Throughput combinat scanări de securitate: 30 Gbps; – Tunele IPSec VPN (site to site) concurente: 12000 – Useri SSL-VPN: 25000;

	– Sesiuni concurente: 68 Milioane; – Sesiuni noi/Sec: 800000; – Instanțe virtuale: 20 (echipamentul va permite separarea logica in instanțe virtuale complet independente a tuturor funcționalităților echipamentului); – Sa permită următoarele configurații redundante: Activ/Activ, Activ/Pasiv; – Componentele Hardware si Software ale produsului ofertat trebuie să fie de la același producător, excepție făcând accesoriile (module optice)
Parametri echipament si accesorii	Echipamentul va avea in compunere • 2 perechi QSFP 100Gbps SR si patch-urile necesare interconectarii, de lungime 30m • 2 perechi SFP+ -modulele optice vor avea capabilități de monitorizare a parametrilor optici • stocare interna min 480 GB SSD. • 2 x surse de alimentare redundante Hot-swappable incluse • Alimentare alternativa 100-240V, 50-60Hz. • kit de instalare pentru montarea in rack in rack 19" Spațiu in rack 19" maxim 9U • 2 x cablu alimentare energie electrica pentru conectare in UPS/PDU
Management	Administrare: – Consola, SSH, HTTPS; – Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri stocate intern, grafice, notificări email; – Se vor documenta si livra MIB. Autentificare: – Baza de date locală; – Integrare LDAP/Radius/TACACS+. – Nu se accepta echipamente de tip "cloud-based". – Toate funcționalitățile sa poată fi configurate exclusiv pe echipamentul ofertat, fără necesitatea suplimentara a unui echipament/ unei platforme de management.

	– Soluția trebuie sa permită actualizarea offline a semnăturilor de securitate
Software si Licente	– Licență perpetuă pentru activarea tuturor interfețelor la viteza maximă. – Licență perpetuă pentru activarea echipamentului la capacitate maximă și cu toate funcționalitățile cerute în caietul de sarcini. – Se solicita abonament de activare a capabilităților de tip UTM. – Licențele ofertate trebuie sa asigure toate funcționalitățile cerute in caietul de sarcini – Licență perpetuă pentru număr nelimitat de stații de administrare – Soluția trebuie să continue să funcționeze in parametrii specificați in caietul de sarcini și după expirarea licențelor pentru functionalitatile de securitate care nu necesita interogari in timp real la platforma producatorului. – Licențele care necesită acces periodic la semnăturile de securitate din partea producătorului vor rămâne disponibile la nivelul ultimului update dinaintea expirării acestora. – Licența perpetua pentru un număr de 500 de utilizatori Remote Acess VPN simultani – Nu se accepta produse a căror funcționare se realizează sau depinde de resurse aflate în cloud-uri publice.
Protocoale	Rutare/Rețea: – DHCP; – Policy routing; – Rutare statica; – Rutare dinamica RIP, OSPF, BGP, Multicast; – VLAN Tagging (802.1q); – Rutare între VLAN-uri – Suport multi-zone – Rutare între zone – Suport IPv6 – BFD Traffic Shaping:

	– Bandă Garantată/Maximă – Shaping per-IP – Instanțe Virtuale: – Instanțe Firewall/Rutare separate; High Availability: – Activ/Activ, Activ/Pasiv; – Link failover; – Link status monitor. Servicii de Securitate Firewall: – L3(Routed/NAT)/L2(Bridge/Transparent) ; – Policy-based NAT; – Profile granulare de protecție per-policy; – Protectie DOS; VPN: – Remote access VPN, cu software de la producător (nu se accepta third-party software) - minim 500 utilizatori – IPSec, SSL; – Suport criptare: AES-256 – Autentificare: SHA-2; – Suport DMVPN sau echivalent; – Autentificare cu certificate sau preshared key; – NAT Traversal. Prevenirea Intruziunilor: – Semnături predefinite de producătorul echipamentului – Suport Anomalii de protocoale – Blocare bot – Suport Semnături definite de utilizator Antivirus: – Suport Antimalware; Control Aplicatii si URL filter SSL: – Scanare SSL pentru IPS si antivirus

	DLP: – Suport data leak/loss prevention Traffic Shaping: – Bandă Garantată/Maximă Securitate trafic Web: – Suport filtrare DNS
Garanție și suport tehnic	– Garanție hardware: 5 ani – Update software gratuit: 5 ani – Acces direct la suportul tehnic al fabricantului: 5 ani – Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. – Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată – Garanția va include acces la suportul tehnic al producătorului pe toată durata perioadei de garanție ofertată. – Contractantul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice echipamentele pe site-ul producătorului, având ca și client final beneficiarul. – Raportul va trebui să conțină pentru fiecare componentă cel puțin seria și perioada activată de suport. – Echipamentele livrate vor fi noi și neutilizate. – Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării. În cazul in care in perioada derularii contractului echipamentul ofertat este end-of-life/end of sale/end of support ofertantul il va înlocui cu un echipament echivalent sau superior. – Soluția va fi livrată la ultima varianta de sistem de operare recomandată de producător – Abonament pentru toate serviciile de protecție menționate la categoria „Servicii de securitate” pentru o perioada de 5 ani
Servicii de instalare	– Serviciile de instalare, configurare și punere în funcțiune vor fi incluse în prețul unitar al echipamentelor ofertate, nu vor fi înscrise distinct în ofertă. *) Necesarul efectiv de materiale pentru conectarea în fiecare site se va stabili în urma site survey-ului care se va efectua obligatoriu de catre

	ofertant. Indiferent de cantitățile de materiale utilizate, prețul unitar al echipamentului nu va fi afectat.

4.4.8 Switch LAN tip 1 SPINE (2 per site)

Echipamentele care deservesc zona de retea Data Center vor fi de la acelasi producator si vor fi configurate intr-o topologie de tip Spine-Leaf cu retea de management out of band separata. Interconectarea celor 2 centre de date se va realiza prin intermediul echipamentelor de tip Border Gateway folosind tehnologii de tipul EVPN Multi-Site. Arhitectura completă ce trebuie realizată va fi detaliată cu ofertantul declarat câștigător, în cadrul fazei de implementare a proiectului.

1.	**Descriere generală şi specificaţii hardware**
	- 64 interfeţe QSFP-DD (interfeţele suportă atât module optice 100 Gigabit Ethernet, cât şi module optice 400 Gigabit Ethernet) - 2 surse de alimentare în curent alternativ, redundante - echipament Rackabil 19" Maxim 2U - 1 port 100/1000 Mbps BASE-T pentru management şi consolă - 1 port USB pentru stocare şi boot - Minimum 4 ventilatoare(3+1) înlocuibile instalate astfel încât răcirea echipamentului să se realizeze din faţă spre spate (Front to Rear Airflow), iar un ventilator defect nu va afecta performanţele echipamentului - Procesor minim 4 Core-uri - Memorie sistem minim 32 GB RAM - Disk SSD minim 64 GB - Buffer minim 114 MB
2.	**Performanţa sistemului**
	- 25.6 Tbps switching capacity (51.2 Tbps switching capacity - bidirecţional) - 8.35 Bpps switching capacity - Latenţă maximă 1.5 micro-secunde - Minimum 3900 VLAN-uri - Minimum instanţe RPVST 62 - Minimum 128 instanţe VRF

	- Minimum 64 căi ECMP - Minimum 128 port channel - Minimum 32 link-uri într-un port channel - Minimum 4 sesiuni SPAN active - Minimum 62 instanțe MST - Minimum 800000 rute LPM IPv4 - Minimum 128000 adrese MAC - Minimum 250000 rute multicast - Grupuri IGMP snooping 32000 - Minimum 2300 reguli de filtrare ACL pe intrare și 500 reguli pe ieșire - Host Route/Entries IPv4 minim 500K - Host RouteEntries IPv6 minim 500K
3.	**Standarde și caracteristici minimale incluse**
	- Standarde: • IEEE 802.1D Bridging and Spanning Tree; • IEEE 802.1p QoS/CoS; • IEEE 802.1Q VLAN Tagging; • IEEE 802.1w Rapid Spanning Tree; • IEEE 802.1s Multiple Spanning Tree Protocol; • Rapid Per VLAN Spanning Tree (RPVST+); • IEEE 802.1AB Link Layer Discovery Protocol; • IEEE 802.3ad Link Aggregation with LACP; • IEEE 802.3x Flow Control; • 802.3ba 100 Gigabit Ethernet; • 802.3bs 400 and 200 Gigabit Ethernet; • 802.3cm 400 Gigabit over multimode; • RMON. - Caracteristici minimale: • Imagine pentru servicii Layer 3, OSPF, BGP și VXLAN, EVPN MULTI-SITE • Minimum 4 cozi QoS per port • Class of Service (CoS) • Differentiated Services Code Point (DSCP) • Port security • Acces Control Lists pe port și VLAN

	• Private VLANs • Traffic Storm Control • Control-plane policing • MPBGP • PIM • VXLAN EVPN fabric • BFD, SR(Segment Routing)
4.	**Management**
	- Administrare: • ssh CLI , telnet, consolă • Utilizatori/Administratori cu drepturi configurabile; • Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri interne, grafice; • Se vor documenta și livra MIB; • Nu se accepta echipamente al căror management se realizează în cloud-uri publice; • Nu se accepta echipamente ce se configurează exclusiv cu software adiacent de management; • Toate funcționalitățile echipamentului trebuie să poată fi configurate exclusiv pe echipamentul ofertat fără necesitatea suplimentară a unui echipament/ platforme de management; • Echipamentul să permită folosirea unei platforme de management prin intermediul căreia se pot realiza operațiuni de: automatizarea provizionarii, depanare evenimente, verificare și validare configuratie, monitorizare stare echipamente, monitorizare topologie și alertare (platforma de management anterior menționată trebuie sa fie de la același producător ca și echipamentul). - Autentificare: • Bază de date locală • Integrare Radius/TACACS+ - Platforma de manangement trebuie să asigure următoarele capabilități: • să aibă posibilitatea să dețină un OS repository cu imagini ale sistemelor de operare încărcate manual sau în mod automat; • să aibă dashboard-uri cu evenimente, starea echipamentelor, vizualizare și control topologii logice și fizice, depanare alerte, vizualizare și control configurație echipament;

	• să poată să gestioneze conturile administratorilor (să poată crea conturi nominale de autentificare pe platformă şi să se poată integra cu un mecanism de autentificare de tip SSO/LDAP).
5.	**Licenţe**
	- Toate porturile active la viteză maximă. - Licenţiere inclusă pentru servicii Layer3, OSPF, EVPN, BGP şi VXLAN si EVPN MULTI-SITE, în cazul în care echipamentul necesită licenţiere separată pentru aceste protocoale (să fie posibilă şi suportată crearea unei topologii folosind protocoalele MP-BGP VXLAN EVPN). - Licenţiat pentru utilizarea platformei de management echipament, de la producător (nu compatibil), conform cerinţelor din zona de Management (Licenţiat perpetuu şi cu suport şi update pe toată perioada garanţiei ofertate). - Licenţierea trebuie să asigure funcţionalităţile menţionate în prezentul CS şi după expirarea suportului şi garanţiei.
6.	**Parametri funcţionare**
	- Alimentare cu energie electrică: • 2 Surse de alimentare cu suport pentru standardele româneşti: 230 VAC / 50 Hz internă, iar o sursă de alimentare va suporta consumul total de energie electrică (în cazul defectării unei surse) - Consum maxim de putere: • 3200W - Temperatura de operare: • De la 0 la 40 grade Celsius
7.	**Accesorii**
	- 1 X cablu consolă - 2 X cablu de alimentare energie electrică conector C13 pentru alimentare în PDU - 1 X kit de instalare 19" cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse - 20 module optice QSFPDD-400GB-DR4 SM MPO pentru distanţa de 500 m ** - 20 buc patch FO SM MPO 12 APC - MPO 12 APC compatibil transceiver QSFPDD ofertat, cu o lungime de 3m - 20 buc patch FO SM MPO 12 APC - MPO 12 APC compatibil transceiver QSFPDD ofertat, cu o lungime de 2m

	- 20 buc patch FO SM MPO 12 APC - MPO 12 APC compatibil transceiver QSFPDD ofertat, cu o lungime de 7m - 20 buc patch FO SM MPO 12 APC - MPO 12 APC compatibil transceiver QSFPDD ofertat, cu o lungime de 10m - 20 buc patch FO SM MPO 12 APC – 4*LC SM duplex (Breakout cable) de 3m - 20 buc patch FO SM MPO 12 APC – 4*LC SM duplex (Breakout cable) de 10m - 40 module optice QSFP28-100GB-DR SMF conector LC pentru distanța de 500 m ** - 40 buc patch FO SM-LC compatibil transceiver QSFP28 ofertat, cu o lungime de 2m - 40 buc patch FO SM-LC compatibil transceiver QSFP28 ofertat, cu o lungime de 10m Observație: **(SFP-urile ofertate și patch-urile de FO trebuie să fie capabile să realizeze transformarea de la QSFP-DD 400 GB SM MPO la 4 * 100 GB SM LC)
8.	**Garanție și suport**
	Soluția ofertată trebuie să beneficieze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri.Garanția hardware va fi de minim 60 de luni. Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul ofertat).Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului).

4.4.9 *Switch LAN tip 2* **LEAF**

1.	**Descriere generală şi specificaţii hardware**
	- 48 interfeţe SFP+ (interfeţele SFP+ suportă module optice 25 Gigabit Ethernet, 10 Gigabit Ethernet) - 6 interfeţe QSFP28 (interfeţele QSFP28 suportă module optice 100 Gigabit Ethernet) - 2 surse de alimentare în curent alternativ, redundante - Rackabil 19" 1U - 1 port 100/1000 Mpbs BASE-T pentru management şi consolă - 1 port USB pentru stocare şi boot - Minimum 2 ventilatoare (1+1) înlocuibile instalate astfel încât răcirea echipamentului să se realizeze din spate spre faţă (Rear to Front Airflow), iar un ventilator defect nu va afecta performanţele echipamentului - Procesor minim 4 Core-uri; - Memorie sistem minim 8 GB RAM; - Disk SSD/FLASH minim 8 GB; - Buffer minim 32 MB.
2.	**Performanţa sistemului**
	- 1.8 Tbps switching capacity(3.6 Tbps switching capacity - bidirecţional) - 1 Bpps switching capacity - Latenţă maximă 1.5 micro-secundă - Minimum 3900 VLAN-uri - Minimum instanţe RPVST 510 - Minimum 1000 instanţe VRF - Minimum 64 căi ECMP - Minimum 128 port channel - Minimum 32 link-uri într-un port channel - Minimum 4 sesiuni SPAN active - Minimum 64 instanţe MST - Minimum 360000 rute LPM - Minimum 280000 adrese MAC - Minimum 100000 rute multicast - Grupuri IGMP snooping minim 32000 - Minimum 2000 reguli de filtrare ACL pe intrare şi 2000 reguli pe ieşire - Host Route/Entries IPv4 minim 160K - Host Route/EntriesIPv6 minim 100K
3.	**Standarde şi caracteristici minimale incluse**

	- Standarde: • IEEE 802.1D Bridging and Spanning Tree • IEEE 802.1p QoS/CoS • IEEE 802.1Q VLAN Tagging • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multiple Spanning Tree Protocol • IEEE 802.1AB Link Layer Discovery Protocol • IEEE 802.3ad Link Aggregation with LACP • IEEE 802.3x Flow Control • IEEE 802.3z Gigabit Ethernet • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3by 25 Gigabit Ethernet • IEEE 802.3ba 40 Gigabit Ethernet • IEEE 802.3ba 100 Gigabit Ethernet • RMON - Caracteristici minimale: • Imagine pentru servicii Layer 3, OSPF, BGP, VXLAN, EVPN MULTI-SITE • Minimum 4 cozi QoS per port • Class of Service (CoS) • Differentiated Services Code Point (DSCP) • Port security • Acces Control Lists pe port şi VLAN • Private VLANs • Traffic Storm Control • Control-plane policing • Rapid Per VLAN Spanning Tree (RPVST+) • VRF • MPBGP • PIM • VXLAN EVPN fabric • BFD, SR(Segment Routing)
4.	**Management**
	- Administrare: • ssh CLI , telnet, consolă • Utilizatori/Administratori cu drepturi configurabile; • Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri interne, grafice; • Se vor documenta şi livra MIB;

	• Nu se accepta echipamente al căror management se realizează în cloud-uri publice; • Nu se accepta echipamente ce se configurează exclusiv cu software adiacent de management; • Toate funcționalitățile echipamentului trebuie să poată fi configurate exclusiv pe echipamentul ofertat fără necesitatea suplimentară a unui echipament/ platforme de management; • Echipamentul să permită folosirea unei platforme de management prin intermediul căreia se pot realiza operațiuni de: automatizarea provizionarii, depanare evenimente, verificare și validare configuratie, monitorizare stare echipamente, monitorizare topologie și alertare (platforma de management anterior menționată trebuie sa fie de la același producător ca și echipamentul). - Autentificare: • Bază de date locală • Integrare Radius/TACACS+ - Platforma de manangement trebuie să asigure următoarele capabilități: • să aibă posibilitatea să dețină un OS repository cu imagini ale sistemelor de operare încărcate manual sau în mod automat; • să aibă dashboard-uri cu evenimente, starea echipamentelor, vizualizare și control topologii logice și fizice, depanare alerte, vizualizare și control configurație echipament; • să poată să gestioneze conturile administratorilor (să poată crea conturi nominale de autentificare pe platformă și să se poată integra cu un mecanism de autentificare de tip SSO/LDAP). •
5.	**Licențe**
	- Toate porturile active la viteza maximă - Licențiere inclusă pentru servicii Layer3, OSPF, EVPN, BGP și VXLAN, în cazul în care echipamentul necesită licențiere separată pentru aceste protocoale (sa fie posibilă crearea unei topologii folosind protocoalele MP-BGP VXLAN EVPN) - Licențiat pentru utilizarea platformei de management echipament, de la producător (nu compatibil), conform cerințelor din zona de Management (Licentiat perpetuu și cu suport și update pe toată perioada garanției ofertate) - Licențierea trebuie să asigure funcționalitățile menționate în prezentul CS și după expirarea suport-ului și garanției
6.	**Parametri funcționare**

	- Alimentare cu energie electrică: • 2 Surse de alimentare cu suport pentru standardele româneşti: 230 VAC / 50 Hz internă, iar o sursă de alimentare va suporta consumul total de energie electrică(în cazul defectării unei surse) - Consum maxim de putere: • 600W - Temperatura de operare: • De la 0 la 40 grade Celsius
7.	**Accesorii**
	- 1 X cablu consolă - 2 X cablu de alimentare energie electrică conector C13 pentru alimentare în PDU - 1 X kit de instalare 19" cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse - 10 buc modul optic 25G-LR-S SM Duplex conector LC - 30 buc patch FO SM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m, 10 buc 7m - 10 buc modul optic 25G-SR-S MM Duplex conector LC - 30 buc patch FO MM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m, 10 buc 7m - **6 module optice QSFP28-100GB-DR SMF conector LC Duplex pentru distanţa de 500m - 12 buc patch FO SM-LC Duplex compatibil transceiver QSFP28 ofertat, cu o lungime de 2m - 12 buc patch FO SM-LC Duplex compatibil transceiver QSFP28 ofertat, cu o lungime de 10m - Observaţie: - **(SFP-urile ofertate şi patch-urile de FO trebuie sa fie capabile sa realizeze transformarea de la QSFP-DD 400 GB SM MPO 12 APC la 4 * 100 GB SM LC Duplex)
8.	**Garanţie şi suport**
	Soluția ofertată trebuie să beneficieze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri.Garanția hardware va fi de minim 60 de luni. Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în

	centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcţionare şi solicitarea rezolvării acestora în funcţie de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terţ. De asemenea, se va asigura dreptul de a face update-uri şi upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul ofertat).Toate funcţionalităţile software solicitate vor include licenţiere perpetuă pentru întreaga configuraţie a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. Echipamentele ofertate trebuie să fie noi şi să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricaţie a producătorului).

4.4.10 Switch LAN tip 3 - **MGMT**

1.	**Descriere generală şi specificaţii hardware**
	- 48 interfeţe 1G Base-T(sau port-uri SFP cu module optice SFP-T instalate în fiecare interfaţă), 4 interfeţe 10/25G SFP28 şi 2 interfeţe 40/100G QSFP28 (sau port-uri SFP cu module optice SFP instalate în fiecare interfaţă astfel încât să fie livrată configuraţia propusă de port-uri) - minim 2 surse de alimentare în curent alternativ, redundante - rack-abil 19" 1U - minimum 1 port 100/1000 Mbps BASE-T pentru management şi consolă - minimum 1 port USB pentru stocare şi boot - minimum 2 ventilatoare(1+1) înlocuibile instalate astfel încât răcirea echipamentului să se realizeze din spate spre faţă (BACK to FRONT Airflow), iar un ventilator defect nu va afecta performanţele echipamentului - procesor minim 4 Core-uri; - memorie sistem minim 8 GB RAM; - disk SSD/FLASH minim 4 GB; - buffer minim 22 MB.
2.	**Performanţa sistemului**
	- 0.348 Tbps switching capacity (0.696 Tbps switching capacity - bidirecţional) - 517 mpps switching capacity - Latenţă maximă 2 micro-secunde - Minimum 3900 VLAN-uri - Minimum 1000 instanţe VRF - Minimum 64 căi ECMP - Minimum 64 port channel - Minimum 32 link-uri într-un port channel

	- Minimum 4 sesiuni SPAN active - Minimum 510 instanțe RPVST - Minimum 64 instanțe MST - Minimum 16000 rute LPM - Minimum 97000 adrese MAC - Minimum 8000 rute multicast - Grupuri IGMP snooping minim 8000 - reguli de filtrare ACL pe intrare(2000/slice) și reguli pe ieșire (1000/slice) - Host Route/EntriesIPv4 minim 16K
3.	**Standarde și caracteristici minimale incluse**
	- Standarde: • IEEE 802.1D Bridging and Spanning Tree • IEEE 802.1p QoS/CoS • IEEE 802.1Q VLAN Tagging • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multiple Spanning Tree Protocol • IEEE 802.1AB Link Layer Discovery Protocol • IEEE 802.3ad Link Aggregation with LACP • IEEE 802.3x Flow Control • IEEE 802.3z Gigabit Ethernet • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3by 25 Gigabit Ethernet • IEEE 802.3ba 40 Gigabit Ethernet • IEEE 802.3ba 100 Gigabit Ethernet • RMON - Caracteristici minimale: • Imagine pentru servicii Layer 3, OSPF, BGP, VXLAN, EVPN • Minim 4 cozi QoS per port • Class of Service (CoS) • Differentiated Services Code Point (DSCP) • Port security • Acces Control Lists pe port și VLAN • Private VLANs • Traffic Storm Control • Control-plane policing • Rapid Per VLAN Spanning Tree (RPVST+) • VRF • BGP

	• BFD
4.	**Management**
	- Administrare: • ssh CLI , telnet, consolă • Utilizatori/Administratori cu drepturi configurabile; • Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri interne, grafice; • Se vor documenta şi livra MIB; • Nu se accepta echipamente al căror management se realizează în cloud-uri publice; • Nu se accepta echipamente ce se configurează exclusiv cu software adiacent de management; • Toate funcţionalităţile echipamentului trebuie să poată fi configurate exclusiv pe echipamentul ofertat fără necesitatea suplimentară a unui echipament/ platforme de management; • Echipamentul să permită folosirea unei platforme de management prin intermediul căreia se pot realiza operaţiuni de: automatizarea provizionarii, depanare evenimente, verificare şi validare configuratie, monitorizare stare echipamente, monitorizare topologie şi alertare (platforma de management anterior menţionată trebuie sa fie de la acelaşi producător ca şi echipamentul). - Autentificare: • Bază de date locală • Integrare Radius/TACACS+ - Platforma de manangement trebuie să asigure următoarele capabilităţi: • să aibă posibilitatea să deţină un OS repository cu imagini ale sistemelor de operare încărcate manual sau în mod automat; • să aibă dashboard-uri cu evenimente, starea echipamentelor, vizualizare şi control topologii logice şi fizice, depanare alerte, vizualizare şi control configuraţie echipament; • să poată să gestioneze conturile administratorilor (să poată crea conturi nominale de autentificare pe platformă şi să se poată integra cu un mecanism de autentificare de tip SSO/LDAP).
5.	**Licenţe**
	- Toate porturile active la viteză maximă - Licenţiere inclusă pentru servicii Layer3, OSPF, EVPN, BGP şi VXLAN, în cazul în care echipamentul necesită licenţiere separată pentru aceste protocoale

	(să fie posibilă crearea unei topologii folosind protocoalele MP-BGP VXLAN EVPN) - Licențiat pentru utilizarea platformei de management echipament, de la producător (nu compatibil), conform cerințelor din zona de Management (Licentiat perpetuu și cu suport și update pe toată perioada garanției ofertate) - Licențierea trebuie sa asigure funcționalitățile menționate în prezentul CS și după expirarea suport-ului și garanției
6.	**Parametri funcționare**
	Alimentare cu energie electrică: - 2 Surse de alimentare cu suport pentru standardele românești: 230 VAC / 50 Hz internă, iar o sursă de alimentare va suporta consumul total de energie electrică(în cazul defectării unei surse) **Consum maxim de putere:** - 400W **Temperatura de operare:** - De la 0 la 40 grade Celsius
7.	**Accesorii**
	- 1 X cablu consolă - 2 X cablu de alimentare energie electrică conector C13 pentru alimentare în PDU - 1 X kit de instalare 19" cu toate cablurile de protecție (împământare), șuruburile, cât și alte accesorii necesare instalării și punerii în funcțiune incluse - 24 patch-uri RJ45 CAT6 de lungime : 12 buc 2m, 12 buc 3m - 2 module optice QSFP-40GB LR SM LC-LC duplex - 4 buc patch FO SM-LC compatibil transceiver QSFP ofertat, cu o lungime de 2m - 4 buc patch FO SM-LC compatibil transceiver QSFP ofertat, cu o lungime de 10m - 4 buc modul optic 25G-LR SM conector LC duplex - 16 buc patch FO SM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 4 buc 3m, 4 buc 2m, 4 buc 7m, 4 buc 10m - 4 buc modul optic 25G-SR MM conector LC duplex - 16 buc patch FO MM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 4 buc 3m, 4 buc 2m, 4 buc 7m, 4 buc 10m
8.	**Garanție și suport**
	Soluția ofertată trebuie să beneficieze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii

	de mentenanţă, folosind un canal de comunicare între centrul de date al autorităţii contractante şi centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modului defect şi înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri.Garanţia hardware va fi de minim 60 de luni. Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcţionare şi solicitarea rezolvării acestora în funcţie de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terţ. De asemenea, se va asigura dreptul de a face update-uri şi upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul ofertat).Toate funcţionalităţile software solicitate vor include licenţiere perpetuă pentru întreaga configuraţie a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia.Echipamentele ofertate trebuie să fie noi şi să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricaţie a producătorului).

4.4.11 **SWITCH Border Gateway(2 per site)**

1.	**Descriere generală şi specificaţii hardware**
	- 48 interfeţe SFP+ (interfeţele SFP+ suportă module optice 25 Gigabit Ethernet, 10 Gigabit Ethernet) - 6 interfeţe QSFP28 (interfeţele QSFP28 suportă module optice 100 Gigabit Ethernet) - 2 surse de alimentare în curent alternativ, redundante - Rackabil 19" 1U - 1 port 100/1000 Mpbs BASE-T pentru management şi consolă - 1 port USB pentru stocare şi boot - Minimum 2 ventilatoare (1+1) înlocuibile instalate astfel încât răcirea echipamentului să se realizeze din spate spre faţă (Rear to Front Airflow), iar un ventilator defect nu va afecta performanţele echipamentului - Procesor minim 4 Core-uri; - Memorie sistem minim 8 GB RAM; - Disk SSD/FLASH minim 8 GB; - Buffer minim 32 MB.
2.	**Performanţa sistemului**
	- 1.8 Tbps switching capacity(3.6 Tbps switching capacity - bidirecţional)

	- 1 Bpps switching capacity - Latență maximă 1.5 micro-secundă - Minimum 3900 VLAN-uri - Minimum instanțe RPVST 510 - Minimum 1000 instanțe VRF - Minimum 64 căi ECMP - Minimum 128 port channel - Minimum 32 link-uri într-un port channel - Minimum 4 sesiuni SPAN active - Minimum 64 instanțe MST - Minimum 360000 rute LPM - Minimum 280000 adrese MAC - Minimum 100000 rute multicast - Grupuri IGMP snooping minim 32000 - Minimum 2000 reguli de filtrare ACL pe intrare și 2000 reguli pe ieșire - Host Route/Entries IPv4 minim 160K - Host Route/EntriesIPv6 minim 100K
3.	**Standarde și caracteristici minimale incluse**
	- Standarde: • IEEE 802.1D Bridging and Spanning Tree • IEEE 802.1p QoS/CoS • IEEE 802.1Q VLAN Tagging • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multiple Spanning Tree Protocol • IEEE 802.1AB Link Layer Discovery Protocol • IEEE 802.3ad Link Aggregation with LACP • IEEE 802.3x Flow Control • IEEE 802.3z Gigabit Ethernet • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3by 25 Gigabit Ethernet • IEEE 802.3ba 40 Gigabit Ethernet • IEEE 802.3ba 100 Gigabit Ethernet • RMON - Caracteristici minimale: • Imagine pentru servicii Layer 3, OSPF, BGP, VXLAN, EVPN MULTI-SITE • Minimum 4 cozi QoS per port • Class of Service (CoS) • Differentiated Services Code Point (DSCP) • Port security

	• Acces Control Lists pe port și VLAN • Private VLANs • Traffic Storm Control • Control-plane policing • Rapid Per VLAN Spanning Tree (RPVST+) • VRF • MPBGP • PIM • VXLAN EVPN fabric • BFD, SR(Segment Routing)
4.	**Management**
	- Administrare: • ssh CLI , telnet, consolă • Utilizatori/Administratori cu drepturi configurabile; • Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri interne, grafice; • Se vor documenta și livra MIB; • Nu se accepta echipamente al căror management se realizează în cloud-uri publice; • Nu se accepta echipamente ce se configurează exclusiv cu software adiacent de management; • Toate funcționalitățile echipamentului trebuie să poată fi configurate exclusiv pe echipamentul ofertat fără necesitatea suplimentară a unui echipament/ platforme de management; • Echipamentul să permită folosirea unei platforme de management prin intermediul căreia se pot realiza operațiuni de: automatizarea provizionarii, depanare evenimente, verificare și validare configuratie, monitorizare stare echipamente, monitorizare topologie și alertare (platforma de management anterior menționată trebuie sa fie de la același producător ca și echipamentul). - Autentificare: • Bază de date locală • Integrare Radius/TACACS+ - Platforma de manangement trebuie să asigure următoarele capabilități: • să aibă posibilitatea să dețină un OS repository cu imagini ale sistemelor de operare încărcate manual sau în mod automat; • să aibă dashboard-uri cu evenimente, starea echipamentelor, vizualizare și control topologii logice și fizice, depanare alerte, vizualizare și control

	configuraţie echipament; • să poată să gestioneze conturile administratorilor (să poată crea conturi nominale de autentificare pe platformă şi să se poată integra cu un mecanism de autentificare de tip SSO/LDAP). •
5.	**Licenţe**
	- Toate porturile active la viteza maximă - Licenţiere inclusă pentru servicii Layer3, OSPF, EVPN, BGP şi VXLAN, în cazul în care echipamentul necesită licenţiere separată pentru aceste protocoale (sa fie posibilă crearea unei topologii folosind protocoalele MP-BGP VXLAN EVPN) - Licenţiat pentru utilizarea platformei de management echipament, de la producător (nu compatibil), conform cerinţelor din zona de Management (Licentiat perpetuu şi cu suport şi update pe toată perioada garanţiei ofertate) - Licenţierea trebuie să asigure funcţionalităţile menţionate în prezentul CS şi după expirarea suport-ului şi garanţiei
6.	**Parametri funcţionare**
	- Alimentare cu energie electrică: • 2 Surse de alimentare cu suport pentru standardele româneşti: 230 VAC / 50 Hz internă, iar o sursă de alimentare va suporta consumul total de energie electrică(în cazul defectării unei surse) - Consum maxim de putere: • 600W - Temperatura de operare: • De la 0 la 40 grade Celsius
7.	**Accesorii**
	- 1 X cablu consolă - 2 X cablu de alimentare energie electrică conector C13 pentru alimentare în PDU - 1 X kit de instalare 19" cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse - 10 buc modul optic 25G-LR-S SM Duplex conector LC - 30 buc patch FO SM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m, 10 buc 7m - 10 buc modul optic 25G-SR-S MM Duplex conector LC - 30 buc patch FO MM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m, 10 buc 7m

	- 10 buc modul optic 10G-LR-S SM Duplex conector LC - 30 buc patch FO SM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m, 10 buc 7m - 10 buc modul optic 10G-SR-S MM Duplex conector LC - 30 buc patch FO MM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m, 10 buc 7m - 6 module optice QSFP28-100GB MMF conector LC Duplex - 18 buc patch FO MM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 6 buc 3m, 6 buc 2m, 6 buc 7m - **6 module optice QSFP28-100GB-DR SMF conector LC Duplex pentru distanța de 500m - 12 buc patch FO SM-LC Duplex compatibil transceiver QSFP28 ofertat, cu o lungime de 2m - 12 buc patch FO SM-LC Duplex compatibil transceiver QSFP28 ofertat, cu o lungime de 10m - Observație: - **(SFP-urile ofertate și patch-urile de FO trebuie sa fie capabile sa realizeze transformarea de la QSFP-DD 400 GB SM MPO 12 APC la 4 * 100 GB SM LC Duplex)
8.	**Garanție și suport**
	Soluția ofertată trebuie să beneficieze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri.Garanția hardware va fi de minim 60 de luni. Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul ofertat).Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia.Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului).

4.4.12 Load Balancer

Descriere generală	Echipament de balansare, accelerare și protejare a aplicațiilor din infrastructura centrului de date. Se vor instala câte 2 echipamente în configurație redundantă în fiecare centru de date din cadrul proiectului.
Specificații hardware	- 8 x 10 Gigabit Ethernet SFP+: echipate cu 8 perechi transceivere 10 Gbps SMF Short-range conector LC; - 2 x 100 Gigabit Ethernet QSFP28: echipate cu 2 perechi transceivere 100 Gbps SMF SR cu conector LC; - Capacitate de stocare interna tip SSD; - Memorie RAM: 128 GB; - Procesor: 18vCPU ; - Instanțe virtuale: 18;
Performanța sistemului	Fiecare echipament de balansare va fi configurat si echipat pentru a asigura următoarele funcționalități: - 95 Gbps throughput, in regim de procesare generală L4; - 85 Gbps throughput, in regim de procesare generală L7; - 45 Gbps procesare criptografica hardware interna integrata; - 80.000 tranzacții pe secunda procesare SSL hardware internă integrată de tip RSA (cu chei 2048bit); - 50.000 tranzacții pe secunda procesare SSL hardware internă integrată de tip ECC (ECDSA P-256); - Protectie Hardware pentru atacuri DDoS:80M SYN/sec - HTTP/2 full-proxy support; - Optimizare TCP WAN; - Suport pentru TLS 1.3; - Protocoale de rutare: BGP, OSPFV2 si V3, ISIS; - Procesarea de trafic cel puțin 1.4M cereri pe secunda L4; - Procesarea de trafic cel puțin 2.4M cereri pe secunda L7;

	- Echipamentul va dispune de multipli algoritmi sau metode statice de balansare a traficului: round-robin, ratio si priority (cu un număr minim de membri activi); - Echipamentul va dispune de multipli algoritmi sau metode dinamice de balansare a traficului: fastest-response, least-connections, combinaţia fastest-response least-connections, precum şi bazate pe resursele serverelor de aplicaţii (ex: utilizare CPU, încărcare memorie, gradul de încărcare al reţelei); Proxy: - Echipamentul va putea funcţiona ca proxy hardware, putând fi configurat pentru funcţionare strictă în mod "reverse proxy" şi va integra funcţionalităţi de tip syn cookie protection; - Echipamentul va putea funcţiona in full proxy mode şi în reverse proxy mode; Monitorizare: - Echipamentul va monitorizara aplicaţii "content based", cum ar fi: HTTP/HTTPS, FTP (passiv/activ), POP3, IMAP, SIP, SMTP, RADIUS, LDAP, MSSQL, SNMP DCA, WMI, RPC si SOAP; Echipamentul va permite: - Procesarea cererilor în funcţie de adresa IP sursa/destinaţie, SSL, hashpersistence; - Utilizarea metodelor de "cookie persistence": pasiv, insert, rewrite; - Utilizarea metodelor de persistenta a sesiunilor în funcţie de orice variabilă din header-ul pachetelor TCP/UDP sau din payload; - NAT (network address translation) si NAPT (network address port translation) bazat pe IP sursa şi/sau IP destinaţie; - Capabilitate de filtrare a pachetelor OSI L3-L7; - Direcţionarea traficului in funcţie de URL, method, HTTP host, version, cookie, tipul browser-ului folosit de client; - Inserţie XFF in header-e HTTP, cu adresa IP originară a clientului; - Redirectare URL către mai multe servere virtuale în funcţie de HTTP response code sau URL pattern; - Agregarea si refolosirea de multiple sesiuni client într-o singură sesiune server-side;

	- Inspecția cererilor/răspunsurilor HTTP; - Blocarea codurilor de eroare generate de anumite servere de aplicații; - Filtrarea informațiilor despre serverele de aplicații și mesajele generate de acestea ("Resource cloaking"); - Capabilitatea de a detecta și bloca anomaliile de protocol TCP/UDP, pentru protecție DoS; - Capabilitatea de definire a politicilor de blocare pentru atacuri tip DoS; - Capabilitate de monitorizare a aplicațiilor protejate pentru prevenirea, detectarea și raportarea anomaliilor de trafic precum și pentru protecția împotriva atacurilor L7 DoS; - Capabilitatea de logging granular per aplicație; Web Application Firewall: - Permite realizarea granulara a politicilor de securitate; - Permite definirea de politici de securitate utilizând semnături predefinite de producător; - Permite definirea unor diferite politici de securitate specifice aplicațiilor implementate; - Permite contruirea de politici de securitate real-time, cu functie de auto-invatare - Permite protecția aplicațiilor utilizând capabilități de tip threat intelligence furnizate de producătorul echipamentului; - Semnaturile de securitate predefinite de producatorul echipamentului ofertat vor include minim urmatoarele categorii: • Baze de date: Microsoft SQL, ORACLE, MySQL, PostgreSQL, Sybase. • Sisteme de operare: Windows, Linux, UNIX. • Limbaje si contexte de aplicatie: .NET, PHP, Java. • Servere web: Apache, Nginx, Microsoft IIS.
Parametri echipament si accesorii	- 2 x surse de alimentare redundante - Alimentare alternativa 100-240V, 50-60Hz. - Kit de instalare pentru montarea in rack 19" - Dimensiune rack: 1U; - 2 x cablu alimentare energie electrica pentru conectare in UPS/PDU
Managemen	**Administrare:**

t	Consola, SSH, HTTPS; Syslog, SNMP, log-uri stocate intern, grafice, notificări email; Se vor documenta si livra MIB. **Autentificare:** Baza de date locală; Integrare LDAP/Radius/TACACS+. Nu se accepta echipamente de tip "cloud-based". Toate funcționalitățile sa poată fi configurate exclusiv pe echipamentul ofertat, fără necesitatea suplimentara a unui echipament/ unei platforme de management.
Software și Licențe	Licențele ofertate trebuie să asigure toate funcționalitățile cerute în caietul de sarcini pentru o perioadă de 5 ani; Se solicita activarea tuturor licențelor de securitate necesare pentru a asigura funcționalitățile solicitate in caietul de sarcini pe o perioada de 5 ani;
Garanție și suport tehnic	Garanție hardware: 5 ani Update software gratuit: 5 ani Acces direct la suportul tehnic al fabricantului: 5 ani Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată Garanția va include acces la suportul tehnic al producătorului pe toată durata perioadei de garanție ofertată. Contractantul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice echipamentele pe site-ul producătorului, având ca și client final beneficiarul. Raportul va trebui să conțină pentru fiecare componentă cel puțin seria și perioada activată de suport. Echipamentele livrate vor fi noi și neutilizate. Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării. În cazul in care in perioada derularii contractului echipamentul ofertat este end-of-life/end of sale/end of support ofertantul il va înlocui cu un echipament echivalent sau superior. Soluția va fi livrată la ultima varianta de sistem de operare recomandată de producător.

Servicii de instalare	Serviciile de instalare, configurare și punere în funcțiune vor fi incluse în prețul unitar al echipamentelor ofertate, nu vor fi înscrise distinct în ofertă. *) Necesarul efectiv de materiale pentru conectarea în fiecare site se va stabili în urma site survey-ului care se va efectua obligatoriu de catre ofertant. Indiferent de cantitățile de materiale utilizate, prețul unitar al echipamentului nu va fi afectat.

Cerințe tehnice balansor Global Server Load Balancing

Sistemul va fi prevazut cu o soluția de balansare GSLB care va fi compusă din minim doua echipamente instalate la sediul din CESTRIN și minim doua echipamente identic instalate în locația de back-up dedicate pentru GSLB si DNS firewall. Echipamentele vor forma un cluster geografic și vor asigura o disponibilitate înaltă a soluției printr-o arhitectură performantă și redundantă (mecanisme și sisteme de back-up) cât și prin proceduri de continuitate utilizate în cazuri de incidente tehnice.

Soluția de balansare GSLB va contine toate licențele, ansamblele, subansamblele și echipamentele necesare realizării balansării globale a traficului din cele două centre de date si pastrarea continuitatii furnizarii serviciilor in caz de nefunctionare a unuia dintre cele doua centre de date.

Soluția de balansare va contine toate licențele, ansamblele, subansamblele și echipamentele necesare realizării balansării globale a traficului din cele două centre de date.

Soluția GSLB va fi responsabilă de distribuirea traficului între cele două data centere prin utilizarea de algoritmi inteligenți DNS. De asemenea soluția de GSLB va asigura mutarea traficului in cazul in care unul dintre nodurile sistemului devine indisponibil.

Pentru uniformitate în administrare și optimizarea integrării funcționalităților cu balansorul local soluția GSLB va fi furnizată de la același producator ca și echipamentele de balansare trafic.

Soluția GSLB va fi concepută astfel încât să beneficieze de caracteristica de înaltă disponibilitate (arhitectură redundantă) de care beneficiază toate componentele din prezentul caiet de sarcini și va fi capabilă de luarea unor decizii bazate pe algoritmi inteligenți de distribuire a traficului pentru asigurarea continuitătii functionarii serviciilor:

- Distribuția traficului în funcție de distanța dintre utilizator și cel mai apropiat data center prin facilitarea accesului unui utilizator la resursa optima
- metode avansate de balansare globala :
    - disponibilitate Globala
    - Round robin
    - persisitenta LDNS
    - Least connections
    - Packets per second
    - Round trip time
    - Hops
    - QoS definite de utilizator
    - Dynamic ratio
    - LDNS
    - Ratio
    - Kilobytes per second
- platforma ofertata va trebui sa suporte un MINIM de 1.000.000 (un milion) de RPS pentru cereri de DNS
  DNSSEC- capabilitatea de a semna digital si a cripta raspunsurile la ceririle DNS in vederea prevenirii atacurilor de tip DNS hijacking si cache poisoning
  DNS over HTTPS (DOH)
- DNS over TLS (DoT)
- se va integra cu solutia de balansare locala pentru monitorizarea statusului VS-urilor,va dispune de functii de descoperire a serviciilor si va genera statistici legate de functionarea serviciilor
- Imbunatatirea performatei aplicatiei prin directionarea traficului bazat pe geolocatie si conditiile de trafic si incarcare a retelei.
- blocarea domeniilor IP malitioase
- prevenirea atacurilor DNS DDoS sau volumetrice
- posibilitate de a utiliza servicii de filtrare DNS de la thrid-party;
- rezolvarea cererilor DNS corespunzătoare dimensionării echipamentelor de balansare trafic, NGFW și aplicații;
- DNS Caching pe baza de profile;
- DNS Security
-

Nu se acceptă solutii on-cloud, soluția ofertată va trebui să fie de tip on-premise.

Arhitectura unui nod

Fiecare nod al sistemului va fi compus, din punct de vedere al subsistemului de comunicatii, dintr-un cluster de firewall, un cluster de balansare locala, un cluster de balansare GSLB și un stack de switch-uri cu capabilități L3 extinse, care vor asigura conectivitatea WAN privat si internet. Conectivitatea dintre centrele de date va fi asigurata prin intermediul echipamentelor de tip Border Gateway dedicate, cu capabilități de tip EVPN Multi-Site care vor permite implementarea unei infrastructuri L2 unificate la nivelul celor 2 noduri ale sistemului Contractantul va asigura conectarea si interoperabilitatea prin Border gateway cu reteaua din centrul de date de la Cristian deja existenta si aflata in administrarea Serviciului de Telecomunicatii Speciale.Topologia de retea a fiecarui centru de date va fi de tip Spine-Leaf folosind suita de protocoale MP-BGP-VXLAN-EVPN, topologiile fiind independent functionale.

Pentru nodul secundar, infrastructura de retea de tip centre de date se va integra cu infrastructura existenta in centrul de date din Cristian si va fi administrata exclusiv de catre Serviciul de Telecomunicatii Speciale.

Solutia finala va fi stabilita in urma sedintelor de lucru dintre Autoritatea contractanta si Contractant impreuna cu specialistii desemnati si va fi implementata dupa acordul Autoritatii contractante.

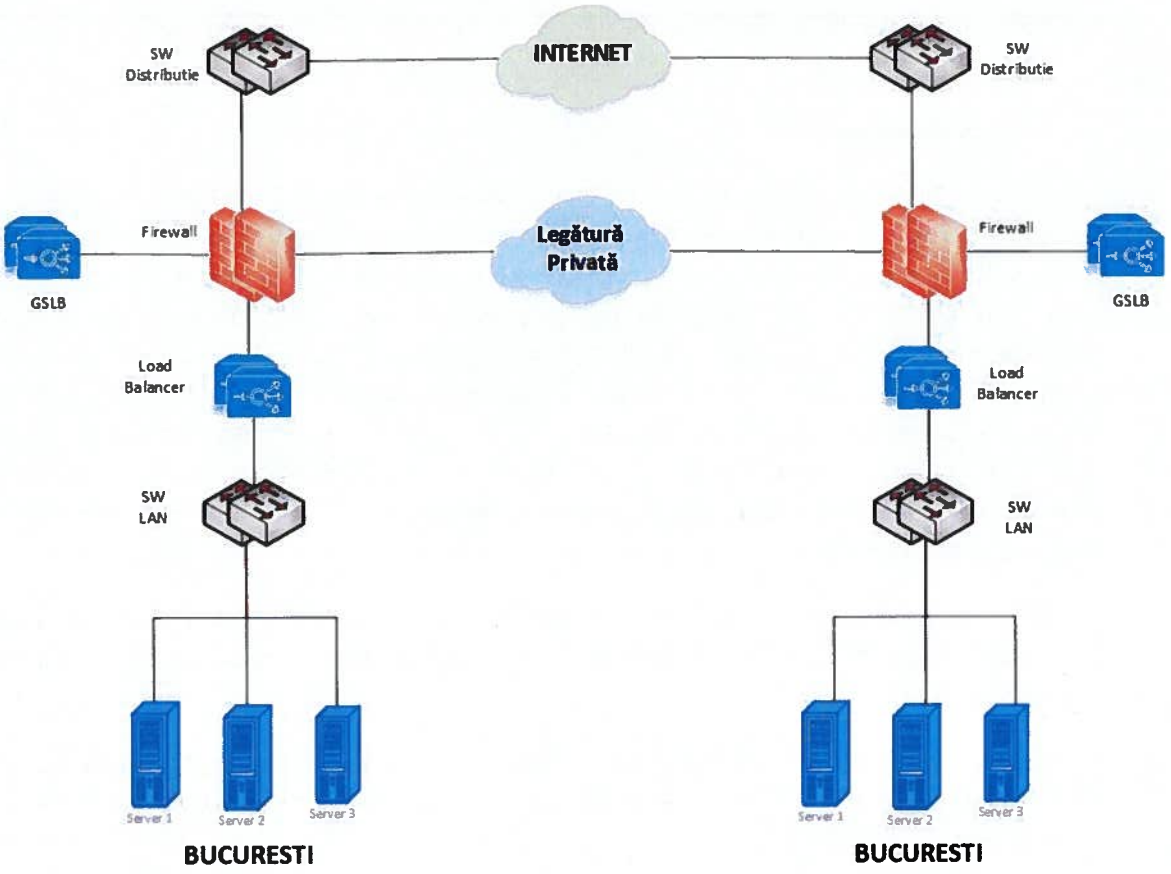


Fig. 2. Schema GSLB

Arhitectura rețelei de comunicații pentru un nod al sistemului

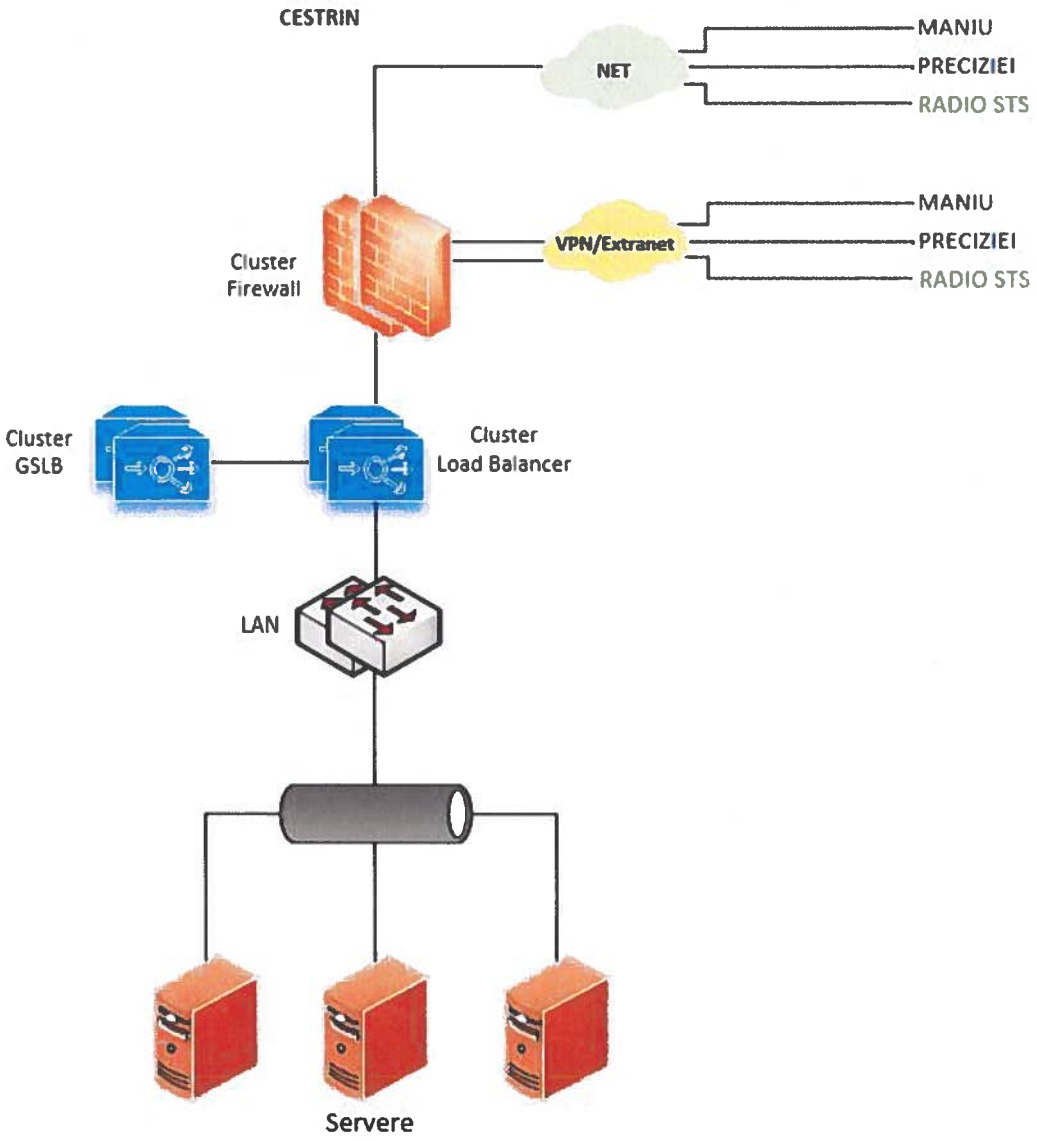


Fig 3. Schema de principiu a unui nod

Arhitectura sistemului trebuie să asigure, pentru toate modulele pe care le conține, un grad înalt de disponibilitate prin asigurarea redundanței atât la nivel hardware, cât și la nivelul legăturilor.

Interfețele echipamentele descrise în prezentul caiet de sarcini vor fi echipate cu SFP-uri corespunzătoare soluției tehnice alese astfel încât să fie capabile să susțină valorile de trafic prezentate în document, inclusive cazul WCS (Worst Case Scenario).

Totodată, la nivel tehnic, sistemul trebuie să îndeplinească următoarele cerinţe:

Orice echipament trebuie să poată fi înlocuit, după expirarea perioadei de garanţie, cu unul cu funcţionalităţi similare comercializat de alt producător. În aceeaşi idee, extinderea sistemului informatic trebuie să se poată realiza cu echipamente de la producători diferiţi, fără nicio constrângere, să implementeze tehnologii de virtualizare care optimizează utilizarea infrastructurii hardware.

Ofertanţii au posibilitatea de a-şi formula propunerea tehnică, adaptată specificului soluţiilor ofertate, incluzând în propunerea tehnică, pe lângă echipamentele precizate în caietul de sarcini, orice echipamente si accesorii pe care le consideră necesare pentru funcţionarea soluţiei. În cazul în care, pentru realizarea soluţiei tehnice sunt necesare şi alte materiale, echipamente, licenţe sau software, decât cele prevăzute în prezentul caiet de sarcini, acestea vor face parte integrantă din ofertă, fără costuri suplimentare din partea Autorităţii/entităţii contractante.

Echipamentele ofertate nu trebuie să fie declarate de producător ca fiind end-of-life, end-of-sale, end-of-support, la data depunerii ofertelor.

Specificaţiile tehnice care eventual fac referire la/indică un anumit model de produs vor fi interpretate în mod obligatoriu ca fiind urmate de menţiunea "sau echivalent".Scopul unor astfel de referinţe este în mod exclusiv sprijinirea potenţialilor ofertanţi în identificarea cu uşurinţă a tipului de produs şi NU favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse.

Specificaţiile tehnice care indică o anumită origine, sursă, producţie, un procedeu special, o marcă de fabrică sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie, sunt menţionate doar pentru identificarea cu uşurinţă a tipului de produs şi NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificaţii vor fi considerate ca având menţiunea de «sau echivalent» şi vor fi considerate specificaţii minimale din punct de vedere al performanţei, indiferent de marcă sau producător. Echivalenţa va fi demonstrată de ofertant.

Dacă în perioada desfăşurării achiziţiei/implementării prezentului contract apar echipamente/software ca şi end-of-life / end-of-sale / end-of-support care să ducă la imposibilitatea furnizării acestora de către Contractant, se vor accepta variante superioare sau echivalente cu acestea. Echivalenţa va fi demonstrată de către Contractant.

Garanţia va include acces la suportul tehnic al producătorului, pe toată durata perioadei de garanţie ofertată. Contractantul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice echipamentele pe site-ul producătorului, având ca şi client final beneficiarul. Raportul va trebui să conţină pentru fiecare componentă cel puţin seria şi perioada activată de suport.

Cerinte infrastructura :

Infrastructură hardware a nodului central va fi instalată în două locații: site principal, situat în București locatia CESTRIN și site secundar, situat în Brașov, cel de al doilea aparținând STS. Atât site-ul principal, cât și cel secundar vor fi constituite din sisteme structural identice din punct de vedere funcțional și vor fi dimensionate în conformitate cu necesitățile de procesare, stocare și arhivare ale sistemului informatic, ținând cont de cerințele de disponibilitate a serviciilor.

De asemenea în cazul unei avarii la unul din site-uri, celălalt site trebuie să susțină , fără întreruperea serviciilor și fără intervenție umană, întreaga încărcăre.

Sistemul din site-ul secundar va fi implementat folosind arhitectura de replicare a datelor din site-ul principal pentru toate componentele funcționale și va fi implementat astfel încât, în cazul nefuncționării site-ului principal, sistemul să fie funcțional din această locație, la întreaga capacitate proiectată și cu toate funcționalitățile și licențierile existente în site-ul principal. Din acest motiv, licențele propuse vor da posibilitatea ca sistemul din site-ul secundar să fie instalat și să funcționeze în mod activ-activ la nivel aplicatie.

Pentru a atinge nivelul de disponibilitate toate componentele funcționale principale vor trebuie să fie asigurate în sisteme de tip cluster.

Componenta de comunicații și securitate trebuie să asigure o lățime de bandă de minim 10 Gbps pentru a asigura accesul rapid la date, precum și între site-ul primar și cel secundar, astfel că, traficul agregat de la utilizatorii finali către sistemul central va fi expus simultan către cele două noduri componente prin conexiuni de minim 10 Gbps într-o arhitectură redundantă și, în același timp, replicarea între cele două noduri ale sistemului central se va realiza printr-o conexiune care să ofere o bandă garantată de minim 10 Gbps. La proiectarea sistemului trebuie avut în vedere o arhitectură cu legături redundante asigurate atât la interconectarea echipamentelor dintr-un nod (cu redundanță locală și la nivelul echipamentelor, și a surselor de alimentare), la nivelul legăturilor nodului și la nivel geo-redundant conform regulilor de bune practici.

Pentru a asigura disponibilitatea și accesul la sistem, întreaga soluție trebuie să fie construită în regim de înaltă disponibilitate (24 de ore pe zi, 7 zile pe săptămână). Soluția trebuie să asigure un regim de înaltă disponibilitate la nivelul fiecărui tip de componentă hardware cât și a fiecărui tip de componentă software atât din nodul principal, cât și din nodul secundar. Arhitectura sistemului proiectat trebuie să asigure înaltă disponibilitate prin asigurarea redundanței la nivel hardware și software, atât din punct de vedere al echipamentelor cât și al conexiunilor de la nivelul unui nod cât și la nivelul nodurilor (No single point of failure). Echipamentele utilizate trebuie să aibă capabilități de configurare a protocoalelor care să permită îndeplinirea cerințelor de înaltă disponibilitate (protocoale de tunelare, de rutare dinamică, de agregare a legăturilor, de sincronizare, VRRP, mecanisme HA etc.)

- Servere de aplicații și baze de date în clustere activ - activ;

- Redundanță locala și geografică la nivelul echipamentelor de rețea (switch-uri, balansoare, firewall);

- Sistemul de operare trebuie să suporte failover și /sau load balancing pentru serviciile instalate care asigură accesul concurențial.

Instalarea echipamentelor:

Echipamentelor vor fi instalate in site principal, situat în București locatia CESTRIN și site secundar situat în Brașov sub supravegherea personalului desemnat de catre autoritatea contractantă. Vor fi incluse orice echipamente si accesorii pe care le consideră necesare pentru funcționarea soluției, fara costuri suplimentare. La implementarea soluției contractantul va eticheta corespunzator, în funcție de tipul de trafic pe care acestea il gestionează echipamentele si cablurile folosite.

4.4.13 Soluție de backup

Această componentă va fi compusă dintr-un echipament dedicat de backup și o soluție software de backup prin care să se administreze toate procesele de backup aferente întregului sistem informatic. Echipamentul dedicat de backup trebuie să îndeplinească următoarele cerințe minimale:

1.	**Descriere generală**
	• Sistem hardware dedicat de stocare a datelor deduplicate având rol de backup. • Sistemul ofertat trebuie să permită montarea într-un rack standard de centru de date, de 19". • Sistemul hardware trebuie să asigure protecția si securitatea datelor și să se integreze cu aplicația software de backup ofertată. • Toate funcționalitățile software solicitate vor fi incluse în configurația ofertată a echipamentului, licențiate perpetuu, pentru întreaga capacitate de stocare ofertată;
2.	**Capacitate instalată**

	• Solutia ofertata va fi echipata cu cel putin 2 module de stocare dedicate pentru rularea sistemului de operare specializat al echipamentului si care nu vor fi parte din spatiul unde vor fi stocate datele salvate. • Echipamentul hardware va avea instalată o capacitate de stocare brută de min. 750 TB. Capacitatea de stocare utilă totală rezultată în urma configurării în RAID (sau echivalent) cu dublă paritate trebuie să fie de minim 500 TiB. • Echipamentul hardware trebuie să includă o capacitate de stocare de tip SSD, minim 18 TB, destinată exclusiv memorării si accesării rapide a indecșilor procesului de deduplicare indiferent de capacitatea utilizată.
3.	**Deduplicare**
	• Procesul de deduplicare va fi global indiferent de tipul sau dimensiunea datelor, de protocolul de tranfer utilizat sau de numărul de sesiuni de salvare; • Sistemul trebuie să includă mecanisme de protecție și corecție a segmentelor de date deduplicate prin care asigură verificarea acestora și disponibilitatea de restaurarea granulară sau completă a fiecărui proces de salvare anterior finalizat cu succes; • Sistemul hardware propus trebuie să susțină deduplicarea globală inline a datelor, prin procese paralele concurente, utilizând interfețe multiple de rețea fără a afecta integritatea datelor. • 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. • Procesul de deduplicare 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 sau protocol. • Solutia ofertata va include suport atat pentru deduplicarea la destinatie, cat si pentru deduplicarea la sursa a datelor pentru cel putin 3 vendori de solutii software de backup. • Rata minimă de deduplicare: 20:1.
4.	**Performanță**

	• Sistemul trebuie să susțină o funcționare continuă a procesele de scriere și citire, în același timp, inclusiv a proceselor de expirare și eliminare a segmentelor de date conform politicilor de retenție; • Procesul de deduplicare a datelor trebuie să fie inline, la momentul scrierii, fără nici un alt proces tampon la nivelul sistemului sau ca opțiune separată de deduplicare; • Procesul de expirare a seturilor de date salvate și cel de stergerea a acestora nu vor afecta operațiunile de salvare și restaurare, funcționarea sistemului va fi continuă; • Backup Throughput: minim 57 TB/oră.
5.	**Replicare**
	• Sistemul va include un mecanism de replicare inteligent a datelor deduplicate într-un sistem hardware identic transmițând doar segmentele unice de date noi; • Politicile de replicare a datelor deduplicate vor fi granulare, automatizate și integrate în politicile de protecție a soluției propuse cu posibilitatea de definire a unor perioade de retenție diferite.
6.	**Securitate**
	• Soluția va include capabilități de securizare și compliență prin criptarea și sigilarea datelor salvate conform politicilor de protecție și a perioadelor de retenție definite. • Segmentele de date deduplicate și compresate trebuie să poată fi securizate prin mecanisme de tip WORM, securizate fata de eventuale 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). • Echipamentul trebuie să utilizeze funcții de criptare conforme cu FIPS 140-2.
7.	**Interfețe de rețea**
	• Minim 8 x Ethernet 25Gbps SFP28 echipate în configurația ofertată (8 buc Cablu DAC 25Gbps 3m incluse). • Toate porturile trebuie sa fie active si sa poata fi folosite in traficul de date de backup. • Interfața de rețea separată pentru administrare la distanță (1 buc patch CAT6 3m inclusă).

8.	**Conformitate cu standarde europene**
	Conformitate CE cu următoarele standarde europene în vigoare: • Siguranța în exploatare: 014/35/EU; • Echipamente de joasă tensiune: 014/35/EU; • Compatibilitate electromagnetica: 2014/30/EU; • Declarație RoHS: 2011/65/EU.
9.	**Alimentare cu energie electrică**
	• Surse de alimentare interne redundante (1+1) AC, 220V, 50 Hz • Cabluri IEC C13 la C14, minim 1,5m, certificate de producătorul echipamentului. Cablurile trebuie să fie prevăzute cu sistem de înlăturare accidentală la ambele capete.
10.	**Accesorii**
	Sistemul ofertat va fi livrat împreună cu toate accesoriile necesare punerii în funcțiune chiar dacă acestea nu au fost solicitate în mod expres.
11.	**Format**
	• Rackmountable 19", maxim 12U (12 rack unit).
11.	**Garanție și suport**
	• Soluția ofertată trebuie să beneficieze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță, folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate

	(firmware, drivere componente, pachete software de la producător incluse în echipamentul ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri şi au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiţionale. • Toate funcţionalităţile software solicitate vor include licenţiere perpetuă pentru întreaga configuraţie a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi şi să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricaţie a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

Soluţia software de backup trebuie să îndeplinească următoarele cerinţe minimale:

Soluţia trebuie sa asigure protecţia sistemelor de producţie, a datelor si aplicaţiilor ce vor rula pe aceste sisteme, sa monitorizeze aplicarea politicilor de protecţie si recuperare a datelor, sa utilizeze mecanisme de deduplicare si compresie şi sâ permită replicarea continua a maşinilor virtuale.

- Licenţierea soluţiei trebuie sa fie calculata fie după numărul de procesoare fizice in utilizare pe sistemele de calcul ale infrastructurii de producţie, fie per maşină virtuală (VM) sau capacitate

- Licenţierea trebuie sa fie de tip perpetua, nu se accepta cea pe baza de abonament, tip subscripţie.

- Soluţia trebuie sa asigure protecţia sistemelor virtualizate si fizice, a sistemului de operare, a fişierelor si aplicaţiilor ce rulează pe aceste sisteme prin politici de protecţie unitare sau distincte.

- Administratorul trebuie sa utilizeze o singura interfaţa de administrare a politicilor de protecţie si restaurare a datelor pentru toate politicile de protecţie indiferent de sistemele de protejat.

- Soluţia trebuie sa permită configurarea politicilor de protecţie in mod independent pentru protecţia unui fisier, a sistemului de operare, a imaginii întregului sistem sau pentru o aplicaţie specifica.

- Sursa datelor, sistemul sau aplicaţia de protejat, trebuie sa comunice in mod direct si securizat cu sistemul dedicat pentru protecţia datelor folosind mecanisme de autentificare.

- Soluţia va permite protecţia unui număr nelimitat de maşini virtuale si de aplicaţii ce rulează pe sistemele licenţiate conform matricei de complianţa a producătorului.

- Soluția susține de duplicarea globala a datelor, la sursa sau destinație, prin segmentare variabila pentru fiecărui proces de protecție indiferent de rețea sau protocolul de transfer utilizat.

- Procesul de de duplicare trebuie sa se desfășoare fără stocare temporara si fără sisteme de calcul intermediare intre sursa si destinație, utilizând un algoritm global de deduplicare.

- Soluția va permite ca procesele de salvare sa transmită peste rețea numai segmentele de date noi, sau cele modificate fata de procesul de salvare anterior, având întotdeauna disponibil ultimul set de date, tip full backup, in echipamentul dedicat protecției datelor fără a inița trafic adițional în rețea.

- Soluția va include capabilități de protecție la nivel de bloc de date pentru sisteme fizice si pentru mașinile virtuale. Restaurarea acestor date fiind disponibila atât ca imagine completa cat si granular.

- Soluția trebuie să ofere posibilitatea de a crea backup-uri în modul complet (full), sintetic full și incremental.

- Transferul datelor de la sursa la destinație trebuie sa poată fi criptat, la fel si stocarea segmentelor de date deduplicate in echipamentul dedicat, indiferent de politicile de retenție aplicate.

- Soluția trebuie sa permită protecția mediilor virtuale la nivel de bloc de date fără agenți instalați in mașinile virtuale cu posibilitatea de a transfera datele peste o rețea IP sau Fibre Channel.

- Administratorul va putea rula simultan mai multe mașini virtuale direct din echipamentul dedicat protecției datelor cu posibilitatea de a le transfera către mediul de producție fără oprirea acestora sau acționarea unui proces de restaurare.

- Soluția trebuie sa protejeze sisteme de calcul de tipul Microsoft Windows, Linux Debian, Red Hat, SuSE, Oracle Linux.

- Soluția trebuie sa utilizeze module dedicate pentru protecția aplicațiilor ca Microsoft SQL, Oracle, PostgreSQL.

- Soluția va permite protecția bazelor de date, integrat politicilor de protecție păstrând eficienta procesului de deduplicare si a consistentei datelor prin politicile de protecție centralizate.

- Soluția va permite definirea si rularea unor rutine automate, înainte sau imediat după desfășurarea procesului de salvare a datelor, in funcție de cerințele specifice ale aplicației de protejat.

- Monitorizarea tuturor componentelor soluției, software si hardware, într-o singura interfața grafica ce va permite personalizarea informațiilor in funcție de cerințele administratorului.

- Soluția trebuie sa ofere posibilitatea de a rula rapoarte combinate cu informații aferent desfășurării proceselor de protecție de la toate componentele software si hardware ale soluției.

- Soluția trebuie sa includă mecanisme automatizate de replicare a datelor salvate astfel încât catalogul actualizat sa utilizeze datele replicate la distanta in cazul in care va fi solicitat.

- Soluția va permite ca o singura operațiune de protecție sau restaurare sa fie împărțita in fluxuri de date paralele pentru același client sursa îmbunătățind indicatorii de performanta ai procesului.

- Soluția trebuie sa permită notificări tip SNMP traps v3.

- Acest jurnal se va putea păstra local sau in locația secundara pentru o restaurare rapida a mașinii virtuale din momentul anterior apariției erorii sau coruperii acesteia.

- Replicarea mașinilor virtuale trebuie sa utilizeze capabilități de deduplicare si compresie ce vor rula in mod continuu pentru a eficientiza transferul datelor de la un centru de date la altul.

- Licențierea soluției trebuie sa fie pentru toate procesoarele fizice ofertate.In functie e licentiere soluția trebuie sa fie licențiată la nivelul fiecarui site pentru toate mașinile virtuale, toate procesoarele fizice sau tot spatiul de stocare și să includă minim 60 de luni de suport;

-

4.4.14 HSM

Dispozitivul Hardware Security Module trebuie sa acomodeze următoarele funcționalități:

- Generare si persistenta chei PKI (online and offline CA keys)
- SSL/TLS
- Code Signing
- Certificate Signing & Validation
- Document signing
- HSMaaS – Private & Public Cloud Environment
- Transaction processing
- Database encryption
- Smart card issuance
- Hardware root of trust for the Internet of Things (IoT)
- Compliannta GDPR, PCI-DSS, HIPAA, eIDAS
- Funcționare in mod cluster Activ-Activ
- Licențierea dispozitivului HSM trebuie sa acopere necesitatea de conectare a unui număr de cel puțin 6 servere per locatie.

- Autentificarea la HSM trebuie sa se realizeze cu ajutorul unui dispozitiv fizic de tip PED cu autentificare multi-factor.
- Din considerente de disponibilitate este nevoie de cate 2 dispozitive de tip PED per locatie.

Specificații modul HSM:

Caracteristica	Detaliu
Suport Sistem de Operare	Windows, Linux
	Virtual: VMware, KVM
Criptografie	Full Suite B support
	Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more
	Symmetric: AES, AES-GCM, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST, and more
	Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3, and more
	Key Derivation: SP800-108 Counter Mode
	Key Wrapping: SP800-38F
	Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG
API cryptography	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
	REST API for Administration
Montare in Rack	Standard 1U 19" rack mount appliance
Certifications	FIPS 140-2 Level 3 – password and multi-factor (PED) Certificate #3205
	QSCD for eIDAS compliance
	Common Criteria Certification (PP 419 221-5)
Complianta	UL, CSA, CE
	FCC, CE, VCCI, C-TICK, KC Mark
	RoHS2, WEEE
	TAA

Interfete network	4 Gigabit Ethernet ports with Port Bonding IPv4 and IPv6
Monitorizare	SNMP

Backup HSM

- Materialul criptografic prezent pe HSM trebuie sa fie stocat in scop de back-up pe un mediu securizat de date, de tip hardware HSM.
- Cu ajutorul dispozitivului de backup HSM, trebuie sa se poata duplica cu ușurință materialul criptografic către celelalte HSM-uri din productie cat si păstrarea acestuia în siguranță în caz de urgență sau dezastru.
- Cu un singur dispozitiv de Backup, un administrator sa poata salva și restaura cheile de pe cel putin 100 partitii.
- Autentificare pe dispozitiv cu ajutorul tokenelor si port dedicat USB.
- Sisteme de operare suportate: Windows, Linux.
- LCD touch screen
- Host interface: USB 3.0 Type C connector
- Token interface: USB 3.0 Type C connector + USB-C (M) to USB-A (F) adapter
- Din considerente de disponibilitate este nevoie de cate 1 dispozitiv de tip backup HSM per locatie.

4.4.15 Rack și accesorii

Sistemul trebuie să includă minim următoarele echipamente și accesorii:

- Rack 42U 1070 x 600, echipat cu uși frontale și dorsale, precum și panouri laterale detașabile. Pentru a optimiza circuitul aerului rece și a disiparea căldurii ușile vor avea suprafața perforată. De asemenea pentru securitate sporită ușile vor fi prevăzute cu încuieturi cu cheie. Va suporta instalarea de echipamente cu o greutate totală de până la 1000 kg, respectiv 20kg pe orizontală per unitate de rack (1U).
- Switch KVM ce permite conectarea serverelor
- Consola TFT retractabilă și este echipată cu un ecran de minim 15 inch și tastatură cu touchpad și butoane pentru mouse.
- UPS minim 8kVA / 8kW rackabil monofazat.
- Accesorii:
  - 2 bucăți PDU cu prize conectate la UPS;
  - organizatoare laterale verticale;
  - patch-uri Fiber Channel și Ethernet de dimensiuni optime pentru interconectarea redundantă a echipamentelor sistemului (acolo unde este permisă);
  - kit-uri de montare în rack pentru toate echipamentele sistemului.

4.5 CERINȚE FUNCȚIONALE

4.5.1 Funcționalități Modul Nucleu central (core system)

Modulul Nucleu central (core system) reprezintă nucleul central al sistemului de tarifare rutiera si va îngloba atât funcționalitățile existente la acest moment in zona emiterii de roviniete si peaj – autovehicule cu masa totala maxima autorizata mai mica de 3,5 tone, precum si noile funcționalități legate de tarifarea bazata pe distanta parcursa - autovehicule cu masa totala maxima autorizata mai mare de 3,5 tone.

Fața de soluția existenta in prezent, modulul central va suferii următoarele modificări:

- Se păstrează funcționalitățile existente pentru autovehiculele cu masa totala autorizata de pana la 3,5 tone inclusiv
- Se vor adăuga funcționalități noi ca urmare a introducerii unui nou mod de tarifare având la baza distanta parcursa pentru autovehiculele cu masa totala autorizata de peste 3,5 tone.

Diagrama funcțională a fluxurilor ce au la baza procesul de tarifare bazat pe distanta parcursa a autovehiculelor este prezentata astfel:

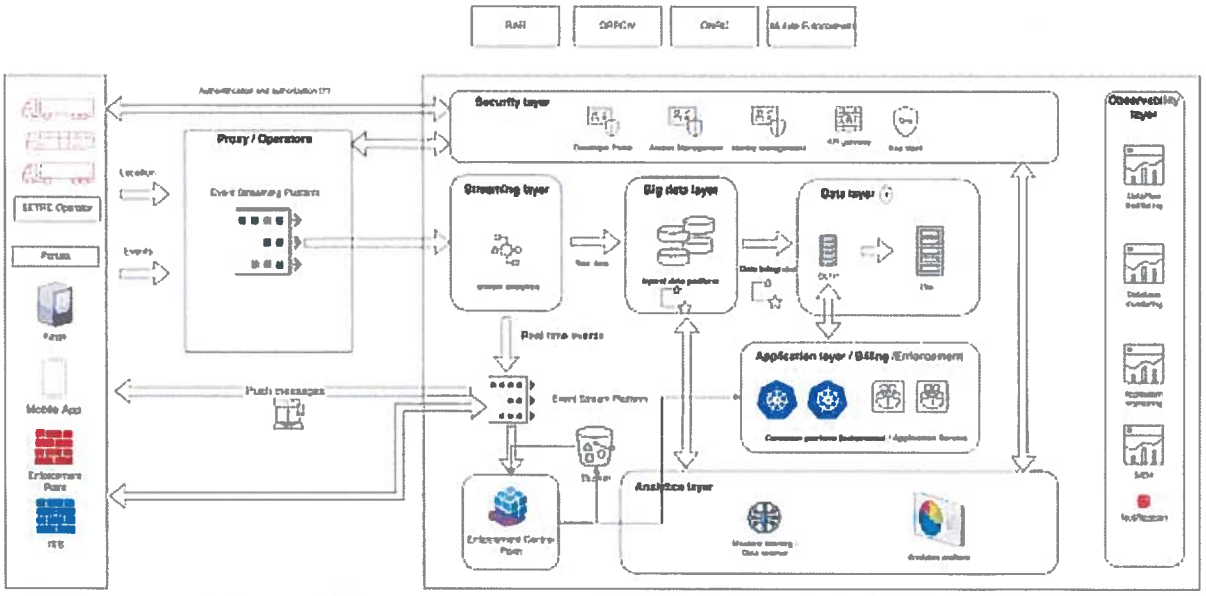


Figura 3 - Diagrama flux tarifare bazata pe distanta parcursa

Modulul nucleu central va conține următoarele funcționalități:

- Gestiune nomenclatoare

- Gestiune clienți (persoane fizice si juridice)
- Gestiune tarife pentru roviniete , peaj sau tarif per km
- Evidenta si gestiune roviniete emise si peaj
- Gestiune porți virtuale (virtual gates) pentru segmente de drum
- Gestiune parteneri si punct de lucru parteneri
- Gestiune scutiri la plata rovinietei sau a tarifului de utilizare a infrastructurii rutiere
- Gestiune tarif pre-paid si post-paid tarif de utilizare infrastructura rutiera
- Gestiunea emiterilor de roviniete si peaj (inclusiv gestiunea trecerilor efectuate prin obiectivele cu tarif special)
- Determină totalul sumelor de plata pentru distanța parcursă în cazul tarifului de utilizare a infrastructurii în mod distanță parcursă si transmite datele aferente pentru facturare
- Oferă funcționalități de tip servicedesk pentru rezolvare incidente si/sau modificări legate de tarifarea rutiera

Modulul nucleu central se integrează cu:

- Modulul GIS
- Modulul de facturare
- Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)
- Modulul de contravenții
- Sistem ERP al CNAIR

Modulul nucleu central expune servicii către:

- Portal extern pentru înrolare in sistem a persoanelor fizice si juridice, emitere si evidenta roviniete si peaj, achiziție in regim pre-paid tarif utilizare infrastructura rutiera având la baza distanta parcursa
- Aplicație mobilă emitere roviniete si peaj
- Aplicație mobilă urmărire traseu in vederea stabilirii tarifului rutier avand ca baza de calcul distanta parcursa de un autovehicul (>3,5 tone)
- Servicii tarifare pre-paid pentru dispozitive multifuncționale (kiosk) atât pentru emiterea de roviniete si peaj cat si pentru tarifarea bazata pe distanta parcursa
- Sistem ERP al CNAIR
- Inspectoratul de Stat pentru Controlul în Transportul Rutier - I.S.C.T.R.
- Agenția Națională de Administrare Fiscala
- Alte instituții ale statului

Modulul nucleu central consuma servicii de la:

- Procesator de plăti prin internet
- DRPCIV
- Institutul Național de Cercetare - Dezvoltare în Informatică – Registrul Operatorilor SETRE
- Registrul Auto Roman
- Oficiul National Registrul Comerțului
- Sistemul Național de Evidenta a Persoanelor
- Banca Națională a României – Curs Valutar

4.5.2 Funcționalități modul contravenții

Modulul de contravenții va conține următoarele funcționalități:

-
- Gestiune nomenclatoare specifice zonei de contravenții
- Gestiune puncte de control
- Gestiune certificate digitale necesare securizării pachetelor ce conțin informații despre autovehiculele care tranzitează punctele de control sau sistemele ITS (captura imagini de la camerele web si metadate)
- Oferă servicii web pentru captarea informațiilor oferite de către punctele de control si/sau sistemele ITS. Serviciile web vor fi securizate
- Configurează modul de captare a informațiilor despre autovehiculele care tranzitează punctele de control sau sistemele ITS - in mod integral (se înregistrează întreg fluxul de autovehicule tranzitat) sau doar a celor care sunt considerate
- Poate procesa informații despre autovehicule fie din imagini in format static , fie flux continuu de înregistrare video
- Stochează informațiile primite de la punctele de control sau sisteme ITS in sistemul de stocare tip Object Storage (compatibil API S3 Object Storage)
- Procesează imaginile recepționate si efectuează o noua identificare a numerelor auto înglobând un sistem de tip ALPR – Automatic License Plate Recognition. Sistemul de tip ALPR va fi livrat de ofertant si poate fi o solutie dezvoltata personalizat sau una de tip COTS.
- Grupează pachete de contravenții pe agenți constatatori
- Întocmește documente de contravenții specifice

Modulul de procesare contravenții se integrează cu:

- Modulul GIS
- Modulul nucleu central

Modulul de procesare contravenţii expune servicii către:

- Modulul central
- Puncte de control si sisteme ITS
- Echipaje mobile de control in trafic

Modulul de procesare contravenţii consuma servicii de la:

- DRPCIV
- Registrul Auto Roman
- Oficiul National Registrul Comerţului
- Sistemul Naţional de Evidenta a Persoanelor
- Banca Naţionala a României – Curs Valutar

4.5.3 Funcţionalităţi servicii web pentru colectare date de la operatorii SETRE

Pentru achiziţia datelor transmise de catre operatorii SETRE despre poziţia si deplasarea autovehiculelor înregistrate in sistem se vor dezvolta interfeţe specializate.

Arhitectura funcţionala a sistemelor integrate se va dezvolta având la baza standardul STN ISO 17573-1, Electronic fee collection.

4.5.4 Funcţionalităţi servicii web pentru emitere roviniete si peaj

Pentru emiterea rovinietelor si a tarifului de obiectiv (peaj) se vor reimplementa serviciile existente in acest moment. La acest moment serviciile web sunt construite pe protocoale SOAP. Se doreşte trecerea către servicii REST si un model de securitate mai avansat. Detalii despre implementare se vor stabilii in faza de analiza si proiectare a sistemului.

Arhitectura funcţionala a sistemelor integrate se va dezvolta având la baza standardul STN ISO 17573-1.

4.5.5 Funcţionalităţi aplicaţie mobila pentru înregistrare si transmitere date privind traseul parcurs de un autovehicul

Pentru a oferii soluţii alternative proprietarilor de autovehicule cu masa totala autorizata de peste 3,5 tone si care se încadrează la modul de tarifare având ca baza de calcul distanta

parcursa, se dorește realizarea unei aplicații mobile care sa fie utilizata de către conducătorii auto care nu dețin si nu doresc sa dețină un contract cu un operator SETRE.
Aplicația va oferii date similare cu cele oferite de către operatorii SETRE si trebuie sa aibă următoarele minime caracteristici si funcționalități:

- Sa fie disponibila pe dispozitive de tip smartphone Android sau IOS
- Sa înregistreze pozițiile geografice având la baza coordonatele GPS

4.5.6 Funcționalități servicii web pentru achiziție roviniete , peaj si mod pre-paid distanta parcursa

CNAIR dorește sa ofere posibilitatea de achiziție a rovinietelor si tarifului de obiectiv (peaj), precum si achiziția pre-paid a tarifului de utilizare a infrastructurii rutiere având la baza distanta parcursa. In acest scop se vor dezvolta servicii specializate care sa ofere următoarele funcționalități:

- Emiterea de roviniete si tarif de obiectiv
- Afișare si selecție harți pentru traseu propus - in cazul tarifarii pe baza de distanta parcursa - având ca si coordonate sursa si destinație itinerar
- Calcul si achitare tarif de utilizare pentru traseul selectat avand ca si parametrii minimi categoria auto, distanta parcursa si norma de poluare a autovehiculului
- Plata prin card bancar

4.5.7 Managementul utilizatorilor și accesul la sistem

Pentru asigurarea managementului utilizatorilor și accesului la sistem, se vor avea în vedere următoarele:

- identificarea în mod unic a fiecărui utilizator în sistem prin crearea de conturi unice și personalizate de acces;
- accesul la sistem se va putea realiza doar prin autentificarea utilizatorilor, excepție făcând doar acele informații de interes public publicate în portal.
- gestionarea centralizată și unitară a accesului utilizatorilor în sistem prin autorizarea utilizatorului doar la componentele și modulele funcționale ale sistemului conform cu drepturile de acces și atribuțiile specifice;
- utilizatori de tip administrator, cu drepturi privilegiate / acces extins și în unele cazuri, nelimitat (de tip root) la sisteme și date.

Asigurarea accesului la sistem se va realiza diferențiat pe diferitele tipuri de utilizatori și conform atribuțiilor structurilor din care fac parte astfel:

- controlul accesului la date şi servicii trebuie să ia în considerare cerinţele referitoare la politicile instituţiilor cu atribuţii privind actualizarea informaţiilor despre persoană şi accesul la date cu caracter personal;
- în scopul realizării şi menţinerii unui nivel adecvat de acces la date şi servicii, se vor lua în considerare cel puţin următoarele:
- soluţie de tip Single-Sign-On pentru autentificarea unitară şi managementul sesiunilor utilizatorilor din sistem;
- cerinţele de securitate ale aplicaţiilor;
- politicile departamentale şi de instituţii publice privind diseminarea informaţiilor;
- cerinţele contractuale şi legale ale organizaţiilor nonguvernamentale, în vederea protejării împotriva accesului neautorizat la date şi servicii.
- capabilitatea de a înregistra operaţiile/tranzacţiile realizate de fiecare utilizator autentificat în vederea realizării unui audit;
- capabilitatea de a seta durata sesiunii unui utilizator în cazul în care acesta nu mai utilizează aplicaţia, pentru a preîntâmpina accesul neautorizat la sistem al altor persoane;
- capabilitatea de a înregistra evenimente definite de securitate şi să transmită mesaje de alertă administratorilor de securitate;
- să permită prin monitorizarea accesului şi limitarea/blocarea temporară sau permanentă a accesului unor utilizatori sau scripturi, pe baza unor reguli prestabilite.

4.5.8 Integrarea cu alte sisteme externe

Sistemul va permite schimbul de date unidirecţional sau bidirecţional pe protocoale standardizate cu respectarea cerinţelor de securitate prin interfeţe de acces programatic, de tip API / WebServices (transfer de date / mesaje via XML, JSON, SOAP, standarde de tip openAPI).

Cadrul Naţional de Interoperabilitate (CNI) cuprinde mai multe niveluri de interoperabilitate: juridic, organizaţional, semantic, tehnic. Proiectul va trebui adaptat din punct de vedere semantic şi tehnic cu CNI/EIF.

Sistemul se va integra cu următoarele entităţi:

- Registrul Auto Roman
- D.R.P.C.I.V.
- Sistemul National Integrat de Evidenta a Populaţiei
- Oficiul National Registrul Comerţului
- Institutul Naţional de Cercetare - Dezvoltare în Informatică

4.6 CERINŢE NON-FUNCŢIONALE

Toate soluţiile ofertate cu excepţia celor dezvoltate personalizat trebuie să fie de tip COTS (commercial off the shelf), modulare, integrate, consacrate şi recunoscute pe plan internaţional. Ele trebuie să aducă valoare adăugată sistemului informatic prin cele mai bune practici internaţionale specializate şi dedicate proceselor specifice ale proiectului.

Toate echipamentele IT și software-ul de infrastructură ofertate vor fi conforme cu structura solicitată și specificațiile din capitolele dedicate, toate cerințele prezente în acest document fiind minime și obligatorii. Sistemul furnizat trebuie să fie unul scalabil, furnizorul având obligația să furnizeze limitele superioare ale scalabili tații, și care să funcționeze în arhitecturi cu disponibilitate ridicată.

Cerințele non-funcționale acoperă condițiile care nu sunt direct legate de comportamentul sau funcționalitatea soluției, ci descriu condițiile de mediu în care soluția trebuie să rămână funcțională sau calitățile pe care aceasta trebuie să le dețină.

5 ETAPELE DE IMPLEMENTARE

Activitățile de analiză, proiectare, realizare, testare și implementare a sistemului trebuie să fie realizate în conformitate cu următoarele prevederi:

5.1 ANALIZA ȘI PROIECTAREA

Rolul principal al fazei de analiză este de a înțelege corect nevoile utilizatorilor înainte de proiectarea și implementarea unui sistem care să le îndeplinească.
În vederea implementării sistemului, Prestatorul va trebui 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 implementat sistemul.
Analiza se va efectua după caz la sediul Beneficiarului sau la Prestator și va avea ca finalitate un pachet de specificații funcționale agreat 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 și a organizațiilor partenere prin ședințe de analiză, chestionare etc. Se vor identifica procesele operaționale care vor fi impactare prin implementarea soluției dezvoltate în cadrul contractului;
- Definirea cerințelor informaționale pentru noul sistem. Se va contura astfel, imaginea viitorului sistem informațional prin stabilirea proceselor operaționale care să precizeze participanții, momentul intervenției acestora, locația sau contextul, modalitatea de intervenție și informația procesată. 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);
- Stabilirea actorilor de business care vor interacționa în viitorul sistem;
- Se vor evidenția activitățile care urmează a fi automatizate dacă este cazul, astfel încât să se identifice clar funcțiile viitorului sistem informatic;

- Identificarea utilizatorilor, a nivelurilor și drepturilor de acces, a modului de securizare a accesului la diversele module/componente ale sistemului;
- Se vor analiza sistemele operaționale existente (inclusiv structurile de date, aspecte legate de consistența și coerența datelor) pentru identificarea posibilităților și a modului în care se va face preluarea datelor din soluțiile existente.

Rolul principal al fazei de proiectare este de a descrie la un nivel suficient de detaliu sistemul care urmează a fi implementat.

În vederea implementării sistemului, Prestatorul va trebui să execute activități de proiectare care să asigure premisele unei implementări eficiente.

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

- Arhitectura de sistem - va prezenta cel puțin următoarele niveluri: hardware, comunicații, componente software instalate (sisteme de operare, produse COTS), arhitectura logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate și caracteristicile funcționale și non-funcționale ale acestora;
- Scenarii de utilizare - din care să reiasă modul de utilizare a sistemului informatic din perspectiva utilizatorului, 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. De asemenea, scenariile de utilizare vor fi însoțite de o listă a actorilor sistemului și maparea acestora cu actorii de business. Pentru prezentarea cazurilor de utilizare se vor folosi instrumente în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent);
- Modelul de securitate - la nivel logic (organizarea pe roluri, grupuri, drepturi, poziția în structura organizatorică etc.) și la nivel fizic (servere, comunicații, aplicații etc.);
- 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.;
- Scenarii/modele de scalare (orizontală/verticală) ulterioară a componentelor platformei.

Proiectarea sistemului trebuie să ofere o soluție optimă, urmărindu-se ușurința și eficiența realizării și implementării soluției, în cadrul restricțiilor de ordin tehnic, organizatoric sau financiar.

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 de acceptanță.

În urma activităților de analiză și proiectare, pentru a se obține un sistem final operațional se vor desfășura activități de configurare, testare și implementare (deployment).

5.2 DEZVOLTAREA

Se vor derula activități de configurare, personalizare și dezvoltare a componentelor soluției informatice (definire fluxuri, dezvoltare module/component, dezvoltare interfețe, dezvoltare proceduri/procese preluare date istoric, dezvoltare proceduri/procese arhivare/backup/restaurare soluție și date, etc).

Având in vedere faptul ca autoritatea contractanta – CNAIR – deține parte din proprietatea intelectuala a soluției de emitere si gestiune a rovinietelor si integral in zona de emitere si gestiune peaj (tarifare per obiectiv) , pentru optimizarea timpilor de dezvoltare si păstrarea competentelor existente, se dorește continuarea dezvoltărilor sistemului in aceeași direcție si anume bazat pe **tehnologii JAVA**.

Soluțiile dezvoltate personalizat vor fi realizate într-o arhitectura de tip microservicii.

Pe toata durata fazei de dezvoltare depozitarele de cod sursa vor fi găzduite la sediul beneficiarului in sistemele special instalate in scopul acestui proiect.

La finalul fazei de dezvoltare va rezulta o soluție informatica completa, dezvoltata în conformitate cu cerințele menționate în Caietul de Sarcini, și detaliate în cadrul fazei de analiza.

Ofertanții vor lua în calcul ca activitățile de dezvoltare se vor desfășura pe mediul achiziționat. Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de dezvoltare/ configurare și testare internă și vor demonstra integrarea acestor proceduri cu procedurile de analiză și proiectare.

5.3 IMPLEMENTAREA

Se vor derula activități de instalare și configurare a echipamentelor, a produselor software livrate, și activități de testare internă pe mediul de producție.

Activitățile de implementare (deployment) sunt activitățile necesare pentru a face sistemul informatic gata de folosire de către utilizatori.

Tot în aceasta etapa va fi finalizata și implementarea soluției pe mediul de dezvoltare/testare.

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de implementare.

5.4 TESTAREA ȘI ASIGURAREA CALITĂȚII

Beneficiarul (cu asistența Prestatorului) va rula toate scenariile pentru testele de acceptanță ale întregului sistem sau componentă livrată. Testele de acceptanță se vor derula în conformitate cu Planul de Teste realizat de Prestator și agreat de Beneficiar, plan ce va fi în concordanță cu întregul ciclu de realizare al contractului: etape de testare distribuite pe iterații, seturi de funcționalități sau alte tipuri de teste.

Planul de testare pentru acceptanță va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerințelor din prezentul caiet de sarcini. Astfel, se va avea în vedere faptul că sistemul funcționează corect din punct de vedere al respectării cerințelor, consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor, inclusiv pentru funcționalitățile

existente care au fost extinse sau modificate. Criteriul de succes - sistemul trece toate testele definite în planul de testare agreat împreună cu Beneficiarul.
O primă variantă a planului de testare va fi prezentată odată cu oferta. Planul detaliat de testare, însoţit de scenariile de testare, va fi realizat de către Prestator şi aprobat de Beneficiar înainte de fiecare etapă de testare agreată prin planul de proiect.
Ofertantul trebuie să descrie modalitatea în care va realiza testarea sistemului şi testele de acceptanţă specifice. Ofertantul trebuie să prezinte metodologia de testare după care se vor realiza activităţile de testare în timpul desfăşurării proiectului. Ofertantul trebuie să prezinte instrumentele de testare folosite.

5.5 MIGRAREA DATELOR ISTORICE

Se vor derula activităţi de preluare a datelor din sistemele operaţionale existente şi încărcare a lor în noua soluţie, urmata de verificarea şi validarea încărcării corecte (testare).
Vor fi considerate dezvoltarea de scripturi dedicate pentru preluarea datelor din sistemele operaţionale existente şi încărcarea lor în modulele corespunzătoare din noua soluţie.
Vor fi considerate activităţi de analiza, de mapare/proiectare, de dezvoltare, testare şi implementare.
Vor fi considerate şi proceduri/procese de roll-back în cazul în care apar erori la migrarea datelor.
Ofertantul trebuie să prezinte modalitatea prin care va realiza migrarea datelor din aplicaţiile existente la Beneficiar precum şi să ţină cont de un plan de migrare automată a datelor în noul sistem integrat.

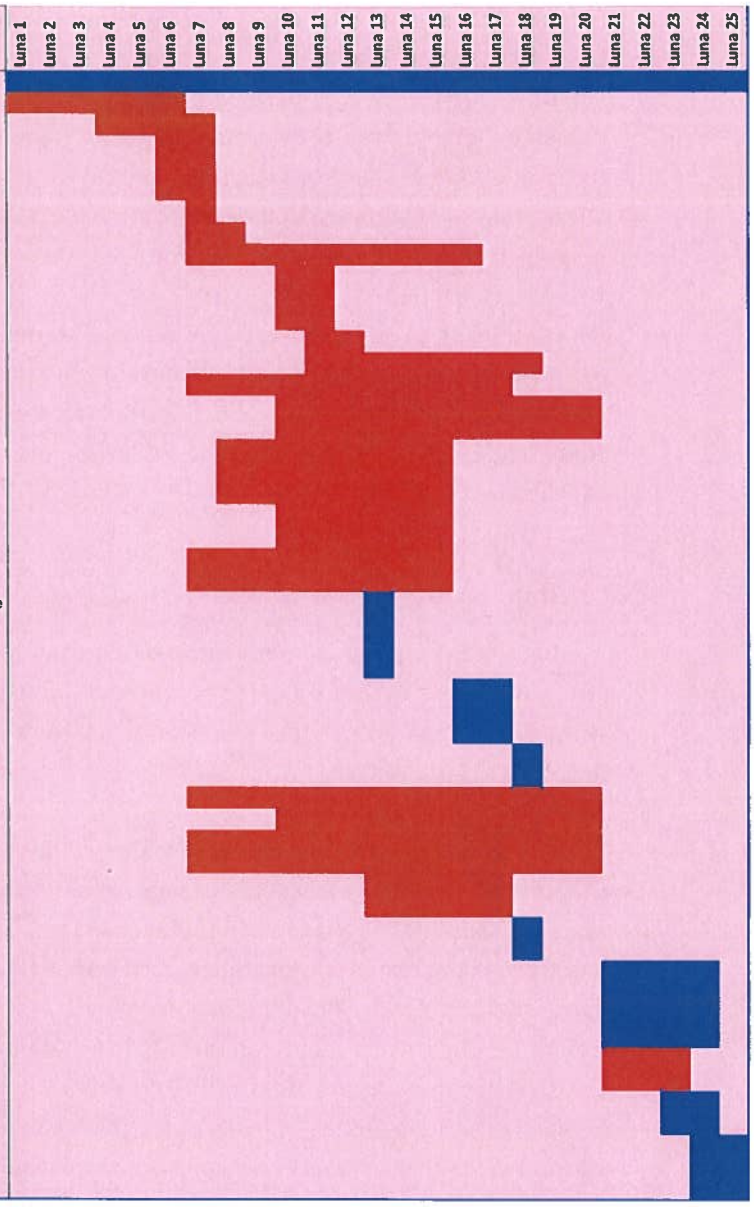
5.6 PUNEREA ÎN PRODUCŢIE

Ofertanţii trebuie să prezinte planul care va fi utilizat la trecerea în producţie a sistemului, ataşat procedurii de acceptanta.
Planul de trecere în producţie trebuie să ţină cont de legăturile logice între subsisteme/componente ale sistemului astfel încât să se asigure o trecere în producţie coerentă şi cu impact minim asupra activităţilor zilnice a angajaţilor Beneficiarului.
Înainte de trecerea efectivă în producţie, va avea loc pilotarea sistemului pentru o perioadă de minim 4 săptămâni.
Concluziile rezultate în urma pilotării vor fi utilizate pentru ajustarea proceselor şi fluxurilor implementate şi va avea ca obiectiv optimizarea funcţionării şi exploatării sistemului.
Codul sursă al aplicaţiei informatice dezvoltate pentru funcţionarea sistemului integrat rămâne în proprietatea Beneficiarului, pentru fiecare versiune a sistemului din producţie.
Data trecerii în producţie este considerata data la care se semnează Procesul Verbal de Acceptanta Finala.

5.7 GRAFICUL DE IMPLEMENTARE

Graficul de implementare al sistemului informatic este prezentat in figura de mai jos:

Nr. Crt.	Faza a proiectului
1	Implementare sistem informatic
2	Analiza de business
3	Proiectare sistem informatic
4	Servicii de livrare, instalare si punere in functiune echipamente Hwardware si infrastructura software site principal
5	Instalare mediu de testare
6	Instalare componente software site principal
7	Incarcare date sistem GIS cu domeniile de tarifare
8	Servicii de livrare, instalare si punere in functiune echipamente Hwardware si infrastructura software site secundar
9	Instalare componente software site secundar
10	Configurarre infrastructura - backup, replicare, comutare
11	Dezvoltare sistem de baza nucleu sistem (backoffice)
12	Dezvoltare in portal mixt modul tarifarare per distanta parcursa (vehicule >3,5 tone)
13	Dezvoltare servicii web pentru dispozitive tip kiosk
14	Dezvoltare servicii web pentru operatorii SETRE si aplicatie mobila de inregistrare traseu parcurs
15	Dezvoltare servicii web pentru inregistrarea datelor si imaginilor aferente contraventiilor de la punctele de
16	Dezvoltare rapoarte aferente modulelor de tarifare per kilometru
17	Publicare servicii web pentru operatorii SETRE pe mediul de testare
18	Publicare servicii web captura date si imagini puncte de control , Sisteme ITS si echipaje mobile
19	Instruire personal module tarifare per kilometru
20	Testare non-functionala module tarifare per kilometru
21	Testare UAT module tarifare per kilometru
22	Punere in productie module tarifare per kilometru (servicii web, aplicatie mobila, portal)
23	Dezvoltare modul central contraventii
24	Dezvoltare in portal mixt modul emitere roviniete si peaj
25	Dezvoltare rapoarte module emitere roviniete/peaj si module contraventii
26	Dezvoltare Servicii Web pentru emitere roviniete si peaj pentru parteneri
27	Publicare servicii emitere roviniete si peaj pe mediul de testare pentru parteneri
28	Testate non-functionala module emitere si peaj
29	Testare UAT module emitere roviniete/peaj
30	Testare UAT module contraventii - integral pentru ambele moduri de tarifare
31	Pregatire Mediu de productie si Migrare Date module emitere rovniete si peaj
32	Instruire module emitere roviniete/peaj , module contraventii si module raportare
33	Pornire in regim de productie module emitere roviniete/peaj si module contraventii (integral pentru ambele moduri de tarifare)



Perioadele aferente fiecărei etape sunt consecutive și dau posibilitatea prestatorului să implementeze etapa următoare de îndată ce a îndeplinit condițiile și livrabilele impuse de etapa anterioară. Prestatorul va avea în vedere să respecte graficul de implementare.

Graficul de implementare nu exclude posibilitatea desfășurării simultane a unor activități în situația în care premisele obiective de începere a acestora sunt realizate.

Activitățile de migrare a datelor de istoric pot fi cuprinse și detaliate în cadrul celorlalte etape de proiect.

Cerințe:

- Ofertanții vor prezenta în cadrul ofertei și un plan de proiect, cu includerea diagramei Gantt, care va conține, în detaliu, atât activitățile pe care Ofertantul le considera necesare a fi prestate pentru

îndeplinirea obiectivului proiectului, cât și tipul de resurse umane care vor fi implicate pe fiecare tip de activitate.

- Planul de proiect va considera calendarul de derulare detaliat mai sus ca fiind unul maximal. În planul de proiect vor fi clar menționate și dependențele între activități, fiind menționate și milestone-urile propuse (atât cele tehnice cât și cele financiare).
- Ofertanții vor prezenta și tipurile de resurse alocate pentru îndeplinirea activităților, menționând responsabilitățile pe care aceștia le vor avea, și vor fi menționate și tipurile de resurse necesare a fi implicate din partea Beneficiarului.
- Ofertanții vor prezenta detalierea resurselor umane alocate cuprinzând descrierea rolurilor acestora, atribuțiilor și efortului (zile om) folosite pentru fiecare activitate menționată în Gantt.
- Ofertanții vor prezenta, în detaliu, metodologia de management de proiect care va fi utilizata, cu toate componentele sale (plan de riscuri și management al riscurilor, plan de comunicare, escaladare, etc).

6 INSTRUIRE

Instruirea cuprinde administrarea și operarea sistemului informatic. Scopul instruirii este de a furniza cunoștințele necesare pentru operarea sistemului informatic și administrarea componentelor software de bază, baze de date și a aplicației. Instruirea va fi coordonată și prestată de către experții prestatorului soluției, astfel:

Sesiuni de instruire a utilizatorilor:

- se vor organiza circa 50 sesiuni de instruire, cu durata de 1 zi, la sediul Beneficiarului, pentru circa 20 persoane/sesiune, în total pentru aproximativ 1000 utilizatori.

Instruirea utilizatorilor va avea în vedere familiarizarea cunoștințelor privind:

- utilizării generale a interfeței grafice a sistemului (GUI);
- funcționalitățile cheie ale modulelor aplicative;
- definirii/generării de rapoarte în funcție de rol (definire rapoarte/generare rapoarte).

Sesiuni de instruire pentru administratorii de aplicație:

- se va organiza o sesiune de instruire, cu durata de 2 zile, la sediul Beneficiarului, pentru circa 20 persoane/sesiune, în total pentru aproximativ 20 administratori de aplicație.

Instruirea administratorilor de aplicație are în vedere dobândirea cunoștințelor necesare:

- utilizării generală a sistemului;
- administrării utilizatorilor și permisiunilor asociate acestora în cadrul aplicației;
- administrării design-ului interfețelor;
- administrării și particularizării sistemului;
- consultării jurnalelor de auditare a accesului și operațiunilor desfășurate în cadrul sistemului;
- întreținerii aplicației;
- adăugării/modificării/ștergerii de date din cadrul sistemului;
- definirii/generării de rapoarte în funcție de rol (definire rapoarte/generare rapoarte);

- cunoștințe necesare administrării, configurării și extinderii funcționalităților componentelor deja existente fără intervenția furnizorului.

Sesiuni de instruire pentru administratorii de sistem:

- se va organiza o sesiune de instruire, cu durata de 5 zile, la sediul Beneficiarului, pentru circa 20 persoane/sesiune, în total pentru aproximativ 20 administratori de sistem.

Instruirea administratorilor de sistem informatic va avea în vedere familiarizarea cunoștințelor privind:

- utilizării generală a sistemului;
- administrării componentelor software și hardware de bază;
- întreținerii și operării în bune condiții a componentelor sistemului.

Instruirea va începe odată cu finalizarea implementării sistemului și se va finaliza înainte de trecerea efectivă a soluției în producție. Durata estimată a perioadei de instruire este de 3 luni.

Limba de predare pentru instruirea utilizatorilor și a administratorilor de aplicație este limba română.

Limba de predare pentru instruirea administratorilor de sistem este limba română sau limba engleză.

Ofertantul va propune o soluție astfel încât să asigure instruirea tuturor utilizatorilor prevăzuți mai sus.

7 DURATA DE EXECUTIE

Durata de execuție a proiectul este de **24 de luni** de la data de incepere a contractului

7.1 Conformitatea realizarii fazelor sistemului are ca punct de referinta punerea in productie a modulelor tarifare per kilometru (servicii web, aplicatie mobila, portal), asa cum este prevazut la pct. 22 din graficul de implementare, in termen maxim de 18 luni de la data inceperii contractului.

In cazul in care Prestatorul nu reuseste sa atinga punctul de referinta prevazut la pct. 7.1 la termenul stabilit, Beneficiarul va fi indreptatit sa aplice o penalitate in cuantum de 15% din valoarea aferenta realizarii aceastei faze a sistemului .

De menționat faptul că există etape intermediare în proiect, etape care au fost evidențiate în cadrul graficului de execuție.

8 GARANȚIA

Ofertantul va oferi detalii suficiente despre modul de asigurare a garanției, a sistemul de tichete pentru preluare și rezolvare incidentelor, a resursele umane alocate și a calificării acestora.

Din punct de vedere al garanției, se are în vederea asigurarea următoarelor:

- componente hardware: 5 ani de la data punerii in funcțiune a acestora

- componente software de tip COTS: 5 ani de la data livrării
- modulele si aplicațiile dezvoltate în cadrul proiectului: 5 ani de la data punerii în producție

În cadrul perioadei de garanție se vor asigura de către Furnizor, fără nici un cost suplimentar pentru Beneficiar:

- garanția de buna funcționare, calitatea și performanțele soluției și componentelor livrate în conformitate cu cerințele Caietului de Sarcini;
- rezolvarea bug-urilor care nu au fost identificate în timpul implementării și care apar în faza de producție;
- întreținerea și buna funcționare a sistemului furnizat în parametrii agreați (funcțional, performanță, disponibilitate, integritatea datelor, securitate etc.);
- instalarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- actualizarea manualelor de utilizare și a altor documente în urma efectuării modificărilor, corecțiilor;
- Instalarea, testarea și punerea în mediul de producție de actualizări software datorate modificărilor legislative survenite pe parcursul implementării proiectului și în perioada de garanție.
- toate incidentele vor fi gestionate prin intermediul aplicației software de gestionare a tichetelor.

În situația în care este necesară transportarea echipamentelor în afara sediilor beneficiarului, toate mijloacele de stocare a datelor vor fi reținute de către beneficiar (hard-discurile vor fi scoase din echipamente și păstrate la sediul beneficiarului).

Descriere SLA (Service Level Agreement)

În cadrul SLA-ului, pe perioada garanției, prestatorul va acorda următoarele servicii de suport:

- Servicii de Help Desk;
- Fault Management;
- Suport în caz de urgență;
- Rapoarte de deranjamente și corelare a erorilor;

Pentru a permite o identificare pro activă a unor posibile soluții, se va asigura permanent (pe durata garanției) acces la o bază de cunoștințe tehnice și/sau documentație tehnică care sunt actualizate de fiecare dată când apar modificări în Soluția implementată sau când apar noi erori și/sau modalități noi de rezolvare/identificare a erorilor.

În acest sens, va fi desemnat un singur punct de intrare pentru toate incidentele legate de Soluția informatică furnizată și anume către Administratorul de Servicii al Prestatorului (de exemplu, acest rol poate fi îndeplinit de către Expertul software soluție de asistență tehnică)

Administratorul de Servicii al Prestatorului va:

- administra și monitoriza incidentele;
- lua legătura cu persoana desemnată ca punct de contact din partea beneficiarului, pentru analiza stărilor incidentelor deschise;
- răspunde tuturor întrebărilor legate de incidente.

Problemele ridicate de către beneficiar vor fi înregistrate de către specialiști ai Prestatorului, în cadrul unei aplicații de tip HELPDESK / e-Ticketing pusă la dispoziție de către Prestator pe perioada garanției.

Suportul va fi furnizat în intervalul orar [09:00 - 18:00] ora locală a României, de Luni până Vineri, cu excepția sărbătorilor legale.
Se va asigura diagnosticarea unui incident pentru determinarea problemei de bază.
Se va monitoriza în permanență incidentul până la închiderea acestuia.
Beneficiarul va avea acces la aplicația de tip HELPDESK/e-Ticketing pentru a monitoriza modul de rezolvare al incidentelor.
Aplicația trebuie să îndeplinească minim următoarele caracteristici:

- înregistrarea solicitărilor de suport și alocarea unui identificator unic fiecărei solicitări;
- posibilitatea de definire și de încadrare a solicitărilor în categorii: defect, eroare, solicitare de informații, cerere de schimbare;
- posibilitatea de înregistrare a descrierii problemei și de atașare a unor documente suplimentare. Aplicația software să permită atașarea oricăror tipuri de fișiere (doc, xls, jpg, xml, sau altele în funcție de necesități) precum și postarea a unor capturi de ecran din aplicații;
- posibilitatea de alocare a unui criteriu de urgență. Aplicația software să permită clasificarea incidentelor în funcție de tipul stabilit, putând să emită notificări pe mail privind alocarea incidentelor către persoanele implicate în incident;
- înregistrarea automată a datei și a orei primirii unei solicitări de asistență;
- posibilitatea de atenționare automată în momentul depășirii unor praguri temporale de rezolvare a diferitelor categorii de solicitări de asistență;
- posibilitatea de escaladare a cererilor de suport;
- posibilitatea de înregistrare a datelor de contact pentru responsabilii pentru activitățile de suport pentru diferitele componente ale sistemului informatic;
- posibilitatea de definire a unor rapoarte personalizate folosind cel puțin criteriile: tipul de incident, nivelul de urgență, timpul de rezolvare, persoana și locația de unde a fost semnalat un incident, modulul sau funcția care a cauzat incidentul, numărul de incidente.

Urmărirea incidentelor

Persoana desemnată ca punct de contact din partea Beneficiarului va lansa un incident, Administratorul de Servicii al Prestatorului primind o notificare pe e-mail sau fax. Fiecare incident va avea atașat un nivel de prioritate (ca în exemplele de mai jos) care să reflecte impactul problemei asupra funcționării sistemului. Inițial, atașarea nivelului de prioritate se va face cu ajutorul Administratorului de Servicii al Prestatorului, ulterior acesta putând fi modificat, cu acordul părților, în funcție de evoluția incidentului. Remedierea se face prin depanare sau înlocuire de echipamente sau subansamble ale acestora (pentru defectele hardware) sau prin actualizări de cod sau aplicare de soluții software recomandate de către producător (în cazul defectelor software). Remedierea defectelor se va face cu păstrarea, eventual creșterea, în niciun caz diminuarea caracteristicilor tehnice ale echipamentului original. Costurile apărute pentru remedierea defectelor apărute în perioada de garanție vor fi suportate integral de către Furnizor.

Niveluri de Prioritate

Nivel Prioritate	Descriere
Urgent	Impact Major asupra funcţionării sistemului Problema împiedică desfăşurarea activităţii instituţiei, procesul de activitate este serios afectat şi nu mai poate continua, pierderea funcţionalităţilor devenind critică. Sistem total nefuncţional
Critic	Impact Semnificativ asupra funcţionării sistemului Problema împiedică desfăşurarea în condiţii normale a activităţii utilizatorilor. Nicio soluţie alternativă nu este disponibilă iar activitatea utilizatorilor poate totuşi continua, însă într-un mod restrictiv. Eroare ce afectează majoritatea funcţionalităţilor sistemului
Major	Impact Mediu asupra funcţionării sistemului Problema afectează minor funcţionalităţile sistemului. Impactul reprezintă un inconvenient care necesită soluţii alternative pentru refacerea funcţionalităţilor. Eroare apărută la o funcţie, proces sau componentă, sistem parţial nefuncţional.
Minor	Impact Minim asupra funcţionării sistemului Problema nu afectează funcţionalităţile sistemului. Rezultatul este o eroare minoră care nu împiedică desfăşurarea în bune condiţii a activităţii utilizatorilor. Eroare care afectează o funcţie dar funcţionarea întregului sistem nu este afectată semnificativ.

Asistenţa este de tipul on site la sediul unde este instalat sistemul central.

În toate tipurile de incidente cu orice nivel de prioritate, asistenţa va fi asigurată 24x7, fiind disponibilă până când problema va fi rezolvată. Pentru aceasta, beneficiarul va furniza o persoană de contact, disponibilă 24x7, care să furnizeze informaţii, să testeze soluţiile de remediere şi să aplice soluţiile furnizate.

Timpi de răspuns şi rezoluţii

Prestatorul va respecta următorii timpi de răspuns, în corelaţie cu nivelul de prioritate:

Nivel prioritate	Timp de răspuns	Timp maxim soluţie provizorie / temporară	Timp maxim de remediere
Urgent	Maxim 1 oră	4 ore	1 zi
Critic	Maxim 1 oră	8 ore	1 zile
Major	Maxim 4 ore	1 zi	2 zile
Minor	Maxim 8 ore	2 zile	3 zile

Timpii de mai sus sunt calculaţi din momentul în care Prestatorul a fost înştiinţat de apariţia problemelor.

La sfârşitul fiecărui caz deschis, Prestatorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului şi o va include în recomandarea finală. Fiecare intervenţie în sistem va fi documentată de către Prestator prin elaborarea unei fişe de intervenţie care va conţine cel puţin următoarele detalii: data intervenţiei, descrierea intervenţiei, modalitatea de rezolvare a intervenţiei, durata intervenţiei; fişa va fi transmisă Beneficiarului.

Produsele/componentele/funcționalitățile reparate sau înlocuite în timpul perioadei de garanție vor fi testate din punct de vedere funcțional de către Beneficiar și se vor semna documente de recepție și/sau acceptanță cantitativă/calitativă (după caz). Garanția pentru produsele reparate sau înlocuite în perioada de garanție se prelungește cu durata imobilizării acestora în reparație.

În cazul în care sunt identificate defecte la acele componente ale soluției care au fost dezvoltate/customizate, Beneficiarul va asigura accesul Prestatorului la Soluția care este instalată și funcțională pe mediul de dezvoltare/testare și unde acesta va face modificările necesare pentru rezolvarea incidentului. După rezolvarea incidentului, noua versiune de soluție va fi testată de către echipa Beneficiarului și, în cazul în care defectele au fost remediate, noua versiune se va instala pe mediul de producție.

Prestatorul va garanta că SLA-ul mai sus menționat se bazează pe servicii de suport pentru Soluția software furnizată în cadrul acestui contract. În cazul în care apare un deranjament hardware, timpii de răspuns vor fi calculați, de asemenea, pe baza tabelului de mai sus.

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;
- Timp de Remediere: Durata de timp până la oferirea soluției finale;
- Remediere Temporară: O modificare în cadrul procedurilor sau datelor care să evite erorile fără folosirea defectuoasă a produselor;
- SLA (Service Level Agreement): identifică funcționalitățile și definește procesele care implică livrarea de către Prestator a diferitelor servicii de suport către Beneficiar;
- Suport: Modalitatea prin care Prestatorul oferă asistență Beneficiarului pentru rezolvarea problemelor apărute și poate fi telefonul de suport tehnic, asistență web și asistență prin e-mail; Suportul este oferit la un Major Release al produsului și la un Release Secvențial Anterior (versiune anterioară) a produsului. Prestatorul va oferi, de asemenea, asistență tehnică pentru versiunile mai vechi ale produsului, dar rezolvarea problemei ar putea fi limitată la instalarea unui Major Release;
- 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 integrate furnizate.

Timpii de răspuns măsurați în zile se referă la zile lucrătoare.

Aceste servicii vor realiza prevenirea și remedierea defecțiunilor și anomaliilor apărute la echipamentele hardware și produsele software ce compun sistemul integrat. Sistemul de suport va asigura rezolvare minimal, fără a se limita, pentru următoarele tipuri de probleme:

- Întrebări de natură tehnică;
- Preluare și remediere de bug-uri (erori la nivel soluție livrată) și defecte în conformitate cu tabelul de răspuns la incidente;
- Asigurare de soluții provizorii valide inclusiv, după caz, înlocuirea de părți, componente hardware defecte cu componente funcționale în vederea restaurării rapide a sistemului functional;

- Informarea permanenta a beneficiarului privind demersurile de remediere şi termenele de rezolvare defecte, erori, etc. care se afla în lista activa de incidente nerezolvate (inclusiv cele aflate în rezolvare la producător);
- Informarea beneficiarului privind noile versiuni de produse, noi service-pack-uri şi upgrade-uri ce includ funcţionalităţi, îmbunătăţiri şi performante, lansate oficial de către producătorii acestora.

Ofertanţii trebuie să descrie în detaliu metodologia după care vor derula activităţile de suport.
Ofertanţii trebuie să prezinte împreună cu oferta procedurile suport din cadrul propriei organizaţii.

9 METODOLOGIA ŞI PLANUL DE LUCRU

Metodologia şi planul de lucru sunt componente-cheie şi obligatorii ale ofertei tehnice.
Oferta tehnică trebuie prezentată în următoarea structură:

- metodologia pentru realizarea serviciilor;
- planul de lucru pentru realizarea serviciilor;
- personalul utilizat pentru realizarea serviciilor şi organizarea acestuia.

9.1 METODOLOGIA

În această secţiune Ofertantul va prezenta modul în care înţelege:

- obiectivele contractului şi sarcinile stabilite prin caietul de sarcini;
- abordarea ce va fi urmată în prestarea serviciilor, inclusiv descrierea conceptului utilizat pentru atingerea obiectivelor contractului;
- metodologia de realizare a activităţilor în scopul obţinerii rezultatelor aşteptate.

Cel puţin următoarele informaţii vor fi prezentate:

- prevederile legale în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit, ce pot avea incidenţă asupra derulării/implementării acestuia;
- identificarea şi explicitarea aspectelor-cheie privind îndeplinirea obiectivelor contractului şi atingerea rezultatelor aşteptate;
- modalitatea de abordare a activităţilor ce corespund rezultatului final al contractului şi a rezultatelor intermediare aferente, în raport cu serviciile şi responsabilităţile stabilite prin caietul de sarcini. Activităţile descrise la acest capitol trebuie reprezentate ca durată, la capitolul aferent din planul de lucru şi trebuie reflectate în propunerea financiară sub aspect valoric la nivel de activitate şi la nivel de pachet de activităţi;
- descrierea soluţiei propriu-zise propuse pentru îndeplinirea obiectivelor stabilite prin caietul de sarcini.

Ofertanţii vor prezenta, în detaliu, metodologiile pe care le vor considera pentru:

- Managementul de Proiect
- Managementul Schimbării
- Dezvoltarea de soluţii software
- Testare
- Management al Riscurilor şi Asigurarea Calităţii

- Instruire
- Punere în producție
- Suport

Metodologiile vor fi referite acolo unde este cazul în Oferta Tehnică.

9.2 PLANUL DE LUCRU

Vor fi prezentate cel puțin următoarele informații:

- denumirea și durata activităților și pachetelor de activități din cadrul contractului, așa cum sunt acestea prezentate la capitolul "Metodologie";
- succesiunea și inter-relaționarea acestor activități;
- punctele-cheie de control - "jaloanele" proiectului;
- durata fiecărei activități din cadrul contractului
- dată estimată de început și finalizare a fiecărei activități
- resursele Prestatorului implicate în realizarea activității

Planul de lucru propus trebuie să fie:

- conform cu abordarea și metodologia propusă;
- să demonstreze:
  - înțelegerea prevederilor din caietul de sarcini;
  - abilitatea de a transpune prevederile într-un plan de lucru fezabil;
  - încadrarea activităților în timp de așa manieră încât să se asigure finalizarea serviciilor în termenul specificat în caietul de sarcini;
- realizat utilizând un software de planificare a timpului.

Planul de lucru sumarizat (cuprinzând toate principalele activități ale fiecărei faze de proiect, durata, dependențele și resursele cheie implicate în derularea fiecărei faze) va fi prezentat ca Anexa la Oferta Tehnică.

Planul de lucru va fi livrat de către Furnizor, în format editabil, la momentul semnării contractului (și va fi detalierea planului de proiect sumarizat depus ca și Anexa la Oferta Tehnică).

Planul de lucru va fi actualizat pe parcursul fiecărei faze/etape a proiectului, fiind un livrabil al fiecărei faze. Orice modificare a Planului de Proiect trebuie să fie validată/acceptată de către managerii de proiect ai Prestatorului și Beneficiarului înainte de a fi transmisă spre validare/acceptare de către responsabilii de proiect ai Prestatorului și Beneficiarului.

9.3 ORGANIZAREA ȘI PERSONALUL

Vor fi prezentate cel puțin următoarele informații:

- 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 (la fiecare fază de proiect și la finalizarea proiectului);

Vor fi prezentate:

- modul de abordare a activității de identificare a riscurilor ce pot apărea pe parcursul derulării contractului și măsuri de diminuare a riscurilor în raport cu prevederile caietului de sarcini;
- modul de abordare a activității de prevenire/atenuare/eliminare sau minimizare a efectelor, după caz, a riscurilor identificate în caietul de sarcini;
- modul de abordare a activităților corespunzătoare îndeplinirii cerințelor privind sănătatea și securitatea în muncă, inclusiv modul în care Ofertantul devenit Prestator 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);

9.3.1 Cerințe privind experții

Se va prezenta lista cu personalul propus pentru desfășurarea contractului, conform cerințelor, conținând minim pozițiile de experți cheie de mai jos, iar pentru restul experților non-cheie lista putând fi extinsa în perioada de analiză de business. Lista completa cu personalul propus, atat pentru pozitiile de experti cheie cat si pentru pozitiile de experti non-cheie va fi prezentata in oferta propusa.
Toți experții trebuie să respecte condițiile prevăzute în caietul de sarcini. Este în sarcina operatorului economic să se asigure de acest lucru.
Referitor la cerințele de certificare oferite de către producători, se acceptă certificarea doar dacă producătorul soluției ofertate este o instituție / organizație / organism de drept public sau privat care respectă standardele naționale sau internaționale de certificare.
Contractantul va asigura experții non-cheie (secundari) necesari pentru desfășurarea activităților pe specialități, și va demonstra în cadrul propunerii tehnice că dispune de resursele de a-i mobiliza atunci când este necesară prezența lor. Experții non-cheie vor completa și sprijini echipa de experți cheie (principali); cerință este îndeplinită prin prezentarea de declarație de disponibilitate ori a oricărui alt document doveditor

Pentru demonstrarea îndeplinirii cerințelor minimale în cazul fiecărui expert cheie, Prestatorul va atașa ofertei tehnice următoarele documente:

- CV Europass, aferent fiecărei persoane propuse în cadrul echipei, semnat de către fiecare titular în parte și datat, care sa ateste îndeplinirea cerințelor solicitate de Autoritatea Contractantă;
- declarațiile de disponibilitate semnate de experții cheie pentru perioada în care urmează să efectueze activități în cadrul prezentului Contract.
- documente suport din care sa rezulte deținerea pregătirii și competențelor/calificărilor profesionale ale personalului de specialitate propus în cadrul echipei, astfel cum sunt acestea menționate, respectiv diplome, atestate, certificări, contracte/cărți de munca/REVISAL, referințe emise de angajatori sau beneficiari care să probeze experiența și durata de lucru în domeniile/specializările cerute, alte documente pentru dovedirea experienței profesionale.

Este în sarcina operatorului economic să se asigure că diplomele/certificările/atestările/acreditările sau alte documente similare, în domeniu, sunt eliberate de către o organizație/organism de drept public sau privat care respecta standardele naționale sau internaționale de certificare.
În cazul în care certificatele/diplomele/documentele care confirmă experiența profesională indicată sunt emise în altă limbă decât română, acestea vor fi transmise in limba de origine, însoțite de o traducere autorizată a acestora în limba română.
Precizăm că autoritatea contractantă nu solicită prezentarea documentelor experților non-cheie în cadrul documentației de participare.
Ofertantul va avea in vedere ca pentru expertii non-cheie trebuie descris in propunerea Tehnica modul in care ofertantul si-a asigurat accesul la serviciile acestora si momentul in care acestia vor interveni in implementarea contractului.
Schimbarea/înlocuirea experților cheie se va efectua numai cu notificare prealabilă comunicată în scris și înregistrată la sediul Beneficiarului (cu minim 10 zile înainte de data propusă pentru înlocuire) și cu acceptul Beneficiarului, prin încheierea unui act adițional, numai în cazuri excepționale (de exemplu în caz de deces, caz de boală sau accidente, demisie sau ineficiență în implementare) și numai cu respectarea acelorași condiții de eligibilitate solicitate în documentația de atribuire. În cazul experților cheie care au făcut obiectul evaluării (factori de evaluare, sunt incidente prevederile art 162 dn HG 395/2016.
Notificarea va fi in mod obligatoriu însoțită de documentele justificative asociate noului expert, așa cum au fost acestea solicitate prin documentația de atribuire a contractului. Prestatorul are obligația de a se asigura că expertul nou propus îndeplinește cel puțin toate cerințele minime solicitate de către Autoritatea Contractantă pentru expertul înlocuit (precum și toate calificările sau experiența suplimentară care a facut obiectul evaluării ofertelor), inclusiv condițiile și cerintele cu privire la inexistența unui conflict de interese.
Autoritatea Contractantă are dreptul de a respinge motivat noul expert propus, în situația în care constată că acesta nu îndeplinește cerințele minime prevăzute în documentația de atribuire sau constata existența unui conflict de interese.
Prestatorul își asumă responsabilitatea exclusivă în ceea ce privește eventualele întârzieri care ar putea interveni în implementare ca urmare a notificării unui nou expert care nu întrunește cerințele minime sau este în conflict de interese. Prestatorul nu poate solicita prelungirea termenelor de prestare a contractului din aceste motive. Prestatorul se va asigura că va duce la îndeplinire obligațiile asumate în prezentul caiet de sarcini.
Experții sunt obligați să respecte confidențialitatea informațiilor pe parcursul implementării proiectului, potrivit dispozițiilor contractului de achiziție publică.

9.3.2 Experții cheie

9.3.2.1 Manager de proiect – 1 persoana

Cerinte experienta si calificare:

- Studii finalizate cu diploma de licenta
- Cunoștințe privind coordonarea proiectelor IT într-o manieră standardizată, dovedite prin certificare profesională de management de proiect eliberată de o organizație / organism de drept public sau privat care respecta standardele naționale sau internaționale de certificare.
- Experienta detinuta in pozitia de Manager proiect/contract si/sau Adjunct Manager proiect/contract si/sau Coordonator proiect/contract si/sau Adjunct Coordonator proiect/contract si/sau Director proiect/contract si/sau Adjunct Director proiect/contract si/sau Project Manager si/sau Project Manager Adjunct si/ sau Sef echipa proiectare si/ sau Adjunct Sef Echipa proiectare si/ sau Sef Proiect si/ sau Adjunct Sef Proiect in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract.

Responsabilități:

- Activități specifice de management de proiect (legat de obiectul contractului, dezvoltare software)
- Punct principal de contact in relația cu beneficiarul
- Managementul contractului
- Managementul proiectului in ansamblul sau, managementul ariei de cuprindere, managementul schimbărilor, planificarea generala a proiectului, managementul riscurilor, managementul problemelor, managementul comunicării
- Asigurarea resurselor proiectului
- Managementul, organizarea, alocarea si planificarea echipei de proiect
- Identificarea riscurilor si propunere de soluții pentru diminuarea/evitarea riscurilor
- Rezolvarea problemelor in scopul evitării situațiilor de criza
- Urmărirea respectării tuturor termenelor conform planului de proiect
- Analiza modalității prin care livrabilele proiectului corespund cerințelor de business
- Realizarea rapoartelor periodice/ad-hoc ale proiectului.
- Elaborează planurile de calitate
- Verifica si asigura calitatea livrabilelor

9.3.2.2 Arhitect de sistem – 1 persoana

Cerinte experienta si calificare:

- Studii finalizate cu diploma de licenta
- Deținerea de cunoștințe în domeniul arhitecturilor de aplicații de nivel Enterprise dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel național/ internațional (TOGAF sau echivalent).
- Experienta detinuta in pozitia de Arhitect de sistem sau similar*) in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic la nivel national in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract.

Responsabilități:

- Este responsabil pentru imaginea, comunicarea și evoluția arhitecturii întregului sistem de tarifare rutiera
- Definește împreuna cu ceilalți coordonatori proiectarea sistemului
- Urmărește respectarea cu strictețe a obiectivelor asumate in documentele de proiectare
- Are rol de mediator intre membrii echipelor proiectului pe teme tehnice si rol decizional in alegerea soluțiilor informatice legate de sisteme , framework-uri si standarde implementate
- Întreține si livrează documentul de arhitectura al sistemului de tarifare rutiera
- Colaborează cu specialiștii autorității contractante pe teme legate de arhitectura sistemului informatic

9.3.2.3 Arhitect de soluție – 1 persoana

Cerinte experienta si calificare:

- Studii finalizate cu diploma de licenta
- Deţinerea de cunoştinţe în domeniul arhitecturii produselor software dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel naţional/internaţional
- Experienta detinuta in pozitia de Arhitect de solutie sau similar*) in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic la nivel national in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract.
- Certificare la nivel cel putin Professional(activa) pe vendorul solutiei de switching

Responsabilități:

- Definirea, împreuna cu Expertul Integrare si coordonare dezvoltare aplicații software, a soluțiilor detaliate pentru noile subsisteme
- Definirea arhitecturii de integrare a componentelor sistemului
- Activități de implementare, asistenta si suport tehnic
- Identificarea riscurilor si problemelor tehnice si a soluțiilor de rezolvare

9.3.2.4 Coordonator Analiza – 1 persoana

Cerinte experienta si calificare:

Studii finalizate cu diploma de licenta

- Deținerea de cunoștințe în domeniul dezvoltării software dovedite prin prezentarea unei certificări recunoscută național/internațional.
- Detinerea de cunostinte in domeniul analizei de business dovedite prin certificare/de tip Certified Business Analysis Professional sau echivalent;
- Detinerea de cunostinte referitoare la modelarea proceselor de business, dovedite prin certificare de tip Certified Unified Modeling Language Professional sau echivalent;

- Experienta detinuta in pozitia de Coordonator analiza sau similar*) in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităţilor ce urmează să le îndeplinească în viitorul contract.

Responsabilităţi:

- Coordonează activităţile de analiza a cerinţelor de business, elaborare a documentelor de specificaţii funcţionale si a scenariilor de testare
- Activităţi de implementare, asistenta si suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanta a sistemului

Nota: *) pentru expertii Arhitect de sistem, Arhitect de solutie si Coordonator Analiza experienta in pozitii similare va fi analizata raportat la responsabilitatile expertului din acest contract

9.3.3 Experţii non-cheie

9.3.3.1 Expert Analist de business – 3 persoane

- Absolvent studii superioare finalizate cu diploma de licenţa
- Competente privind analiza de business dovedite prin certificare in domeniu
- Experienţa specifica in cel puţin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităţilor ce urmează să le îndeplinească în viitorul contract

9.3.3.2 Expert Analist date – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenţa
- Competente privind tehnici de analiza multi-dimensionala utilizate in analiza datelor dovedite prin diploma/certificare in domeniu
- Experienţa specifica in cel puţin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităţilor ce urmează să le îndeplinească în viitorul contract

9.3.3.3 Coordonator dezvoltare software – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licenţa;
- Competente privind o metodologie de dezvoltare software, recunoscuta la nivel naţional/ internaţional, dovedite prin certificare in domeniu
- Competente privind dezvoltarea de software dovedite prin certificare in domeniu obţinute la nivel naţional sau internaţional (pentru absolvenţii de studii superioare la facultăţi cu profil informatic/calculatoare, este suficientă diploma de absolvire).
- Competente privind dezvoltarea de aplicaţii bazate pe tehnologii BigData (precum Hadoop, Spark, etc) dovedite prin certificare recunoscuta la nivel naţional/internaţional

- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.4 Specialist Dezvoltare software – 18 persoane

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind dezvoltarea de software dovedite prin certificare in domeniu obținute la nivel național sau internațional (pentru absolvenții de studii superioare la facultăți cu profil informatic/calculatoare, este suficientă diploma de absolvire).
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.5 Expert Coordonator testare – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.6 Specialist testare – 6 persoane

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.7 Expert integrare – 2 persoane

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente in domeniul modulelor de integrare in proiecte cu arhitectura de tip Enterprise
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.8 Expert baze de date relaționale – 2 persoane

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind administrarea bazelor de date in configurație cluster dovedite prin certificare in domeniu recunoscuta la nivel național/ internațional

- Competente privind optimizarea performantei bazelor de date dovedite prin certificare in domeniu recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.9 Expert replicare/ETL – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind implementarea sistemelor de replicare a datelor sau a instrumentelor ETL dovedite prin certificare recunoscuta la nivel național/internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.10 Specialist infrastructura/virtualizare - 2 persoane

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente in domeniul sistemelor de operare de tip Enterprise, dovedite prin certificare recunoscuta la nivel național/ internațional
- Competente privind sistemul de virtualizare ofertat in cadrul acestei proceduri, dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.11 Specialist DEVOPS - 1 persoana

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente in domeniul DEVOPS, dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.12 Specialist sistem management aplicații containerizate (Kubernetes) - 1 persoane

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind sisteme de orchestrare aplicații containerizate (Kubernetes sau echivalente), dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.13 <u>Specialist comunicații și rețea</u> – 2 persoane

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind implementarea, administrarea si depanarea tehnologiilor avansate de rutare si switching, dovedite prin certificare recunoscuta la nivel național/ internațional
- Competente privind administrarea si gestiunea securitatea rețelelor dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract
- Certificare la nivel cel puțin Professional(activa) pe producătorul soluției de Firewall
- Certificare la nivel cel puțin Professional(activa) pe producătorul soluției de switching
- Dovada implementării a cel puțin unui proiect cu redundanta geografica(intern sau internațional)

9.3.3.14 Specialist testare de securitate – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind testarea de securitate a sistemelor informatice, dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.15 Expert securitatea* cibernetică *– 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind securitatea datelor si a sistemelor informatice, dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.16 Expert instruire – 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind instruire, dovedite prin diploma de formator;
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.17 Expert instrumente Big Data - 1 persoana

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind instalarea si administrarea de instrumente BigData, dovedite prin certificare (pentru soluțiile ofertate) recunoscuta la nivel național/ internațional

- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.18 Expert infrastructura procesare/stocare - 2 persoane

- Studii finalizate cu diploma de licența
- Competente privind infrastructura hardware: platforma de procesare aplicații sau platforma de stocare dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

9.3.3.19 Expert infrastructura de securitate - 1 persoana

- Studii finalizate cu diploma de licența
- Competente privind infrastructura de securitate: infrastructura firewall sau ADC/WAF dovedite prin certificare recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în viitorul contract

Certificare la nivel cel puțin Professional(activa) pe producătorul soluției de Firewall

- Certificare la nivel cel puțin Professional(activa) pe producătorul soluției de Balansare ofertata.
- Dovada implementării a cel puțin unui proiect cu redundanta geografica(intern sau internațional)

10 MANAGEMENTUL CONTRACTULUI

10.1 ASPECTE ORGANIZATORICE

Autoritatea contractantă

CNAIR va îndeplini rolul de Autoritate Contractantă în prezenta procedura de achiziție publică și va fi responsabilă cu organizarea acestei proceduri. Totodată, CNAIR îndeplinește și rolul de Beneficiar al serviciilor ce urmează a fi contractate.

Managementul Contractului, inclusiv implementarea administrativă și procedurală aferente Contractului, va fi asigurat de către o echipa de proiect din partea CNAIR (Echipa de Proiect), care va gestiona totodată și documentele elaborate de prestator (analize, livrabile ale fazelor de proiect, rapoarte de progres, rapoarte, facturi, alte documente justificative etc.).

Autoritatea Contractantă este responsabilă pentru:

- punerea la dispoziția Prestatorului a tuturor informațiilor disponibile pentru obținerea rezultatelor așteptate, cum ar fi: date de intrare, raportări, situații specifice;
- punerea la dispoziția Prestatorului, dacă este cazul, a unui spațiu de lucru mobilat;
- desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit Prestatorului;

- asigurarea tuturor resurselor care sunt în sarcina să pentru buna derulare a Contractului.

Prestatorul

Prestatorul serviciilor este responsabil pentru execuția conformă și la timp a tuturor activităților și pentru furnizarea livrabilelor prevăzute în prezentul Caiet de Sarcini, corespunzătoare Proiectului.

Prestatorul va răspunde întocmai tuturor cerințelor prevăzute în prezentul Caiet de Sarcini, respectând și aplicând cele mai bune practici în domeniu.

Prestatorul este direct și integral responsabil pentru activitatea experților săi și pentru îndeplinirea scopului Contractului și obținerea rezultatelor Proiectului.

Prestatorul este pe deplin responsabil pentru:

- asigurarea planificării resurselor în raport cu graficul estimat pentru derularea contractului și prezentat în cadrul acestui Ofertei;
- îndeplinirea obligațiilor sale, cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale relevante precum și cu deplina înțelegere a complexității legate de derularea cu succes a Contractului, astfel încât să se asigure îndeplinirea obiectivelor stabilite, inclusiv prin furnizarea - prin intermediul Planului de management al calității - a asigurării că activitățile și rezultatele sunt realizate la parametrii calitativi solicitați;
- asigurarea valabilității tuturor autorizațiilor și certificatelor (atât pentru organizația sa, cât și pentru personalul/echipamentul propus pentru realizarea serviciilor) care sunt necesare (conform legislației în vigoare) pentru prestarea serviciilor;
- prestarea serviciilor în conformitate cu cerințele Caietului de Sarcini;
- prezentarea rezultatelor în formatul/formatele care să respecte cerințele Autorității Contractante;
- colaborarea cu personalul Autorității Contractante alocat pentru serviciile desfășurate conform Contractului (monitorizarea progresului activităților în cadrul Contractului, coordonarea activităților în cadrul Contractului, feedback).

Principalele atribuții și responsabilități ale Prestatorului:

- Implementarea soluției informatice:
  - Analiza necesităților;
  - Proiectarea soluției informatice;
  - Servicii de livrare, instalare și punere în funcțiune echipamente hardware, de comunicații și licențe software;
  - Dezvoltarea aplicației informatice;
  - Testarea aplicației;
  - Pilotare la nivel național;
- Instruirea administratorilor și utilizatorilor.

10.2 FACILITĂȚI OFERITE DE PRESTATOR

Prestatorul va asigura experților săi sprijin administrativ, de secretariat și traducere, după caz, care să le permită experților desfășurarea în bune condiții a activităților din acest contract.

Printre altele, Prestatorul va fi responsabil pentru (și va suporta costurile):

- Asigurarea cazării, serviciilor de masă, și transportului (local și internațional dacă este cazul) pentru personalul său;
- Cheltuieli de relocare, asigurări de sănătate, după caz;
- Asigurarea spațiului necesar pentru desfășurarea activităților experților (suplimentar față de cel pus la dispoziție de Autoritatea Contractantă), dotat cu mobilier și toate echipamentele și materialele necesare;
- Cheltuieli de comunicare;
- Serviciile de secretariat;
- Orice cost legat de interpretare și traduceri, imprimarea sau multiplicarea rapoartelor;
- Costurile pentru angajarea experților;
- Costurile elaborării și transmiterii rapoartelor;
- Orice alte cheltuieli legate de activitatea Prestatorului.

Echipamente

Prestatorul va fi responsabil și va suporta costurile pentru toate echipamentele necesare în executarea obligațiilor asumate prin Contractul de prestări servicii.

Niciun fel de echipamente nu vor fi achiziționate în numele Autorității Contractante/Beneficiar ca parte a serviciilor din cadrul Contractului sau transferate Autorității Contractante/ Beneficiarului la finalizarea Contractului.

10.3 METODOLOGIE DE LUCRU ȘI RAPORTARE

10.3.1 Metodologia de lucru

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

În termen de 3 zile lucrătoare de la data începerii contractului, va fi organizată o întâlnire de lucru la care vor participa reprezentanți ai Beneficiarului (membrii echipei de proiect) și ai Prestatorului (directorul de proiect, experții cheie).

În cadrul acestei întâlniri vor fi stabilite următoarele:

- principiile de comunicare reciprocă;
- 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.

10.3.2 Cerințe privind raportarea

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

Raportul Inițial

Va fi întocmit în maxim 2 săptămâni de la data începerii executării 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.

Rapoarte lunare

Prestatorul va elabora un raport lunar prin care să prezinte evoluția lunară a activităților și întârzierile, dacă acestea sunt semnificative. Rapoartele lunare vor detalia:

- Progresele înregistrate;
- Activități aflate în derulare cu data estimativă a finalizării acestora și cu rezultatele anticipate;
- Dificultățile întâmpinate în cursul implementării proiectului și soluțiile propuse pentru a depăși respectivele dificultăți;
- Rezultatele realizate în cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente, și planificarea activităților pentru perioada următoare;
- alte documente solicitate de către beneficiar prevăzute în instrucțiuni.

Rapoartele lunare vor fi transmise spre aprobare Autorității Contractante până în data de 5 a următoarei luni pentru care se face raportarea (de ex. Raportul aferent activității din luna ianuarie se va transmite până pe data de 5 februarie). În cazul în care data de 5 a lunii respective este o zi nelucrătoare, prestatorul va anticipa transmiterea raportului lunar.

Raportul final

Varianta preliminară a Raportului final trebuie să fie transmisă Echipei de Proiect cu cel puțin o luna înainte de sfârșitul perioadei de execuție a Contractului pentru a fi analizată. Acest raport trebuie să descrie întreg procesul de execuție și va înlesni evaluarea rezultatelor obținute atât în termeni calitativi, cât și cantitativi.

Raportul 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 CNAIR în acest sens.

Varianta preliminară a acestui raport va fi revizuită cu observațiile/comentariile primite din partea Autorității Contractante, în termen de 5 zile lucrătoare de la data primirii observațiilor/comentariilor.

Autoritatea Contractantă va transmite observațiile/comentariile în termen de 15 zile lucrătoare de la data primirii variantei preliminare a Raportului final.
Alte rapoarte: Autoritatea Contractantă poate cere Prestatorului să elaboreze pe parcursul derulării Contractului și alte rapoarte, în măsura în care acestea sunt legate de buna desfășurare a Contractului.

10.3.3 Transmiterea și aprobarea rapoartelor

Raportul inițial, Rapoartele lunare și Raportul final trebuie transmise, în trei exemplare, spre aprobare, în atenția Managerului de Proiect al Echipei de proiect din partea Autorității Contractante.
Toate rapoartele vor fi redactate în limba română. Variantele intermediare, de lucru, pot fi transmise Autorității Contractante doar în format electronic editabil. Variantele finale vor fi transmise atât în format electronic editabil cât și pe hârtie. Aprobarea rapoartelor se face de către Comisia de recepție desemnată de Autoritatea Contractantă.
Autoritatea Contractantă, în urma recepției, va aproba rapoartele sau va prezenta observațiile sale în termen de maxim 10 zile lucrătoare de la data depunerii rapoartelor inițial, lunare, respectiv 15 zile lucrătoare pentru raportul final.
În cazul unor modificări, Prestatorul are obligația de a răspunde pozitiv solicitărilor Autorității Contractante de modificare/ completare a rapoartelor, corespunzător cu observațiile Autorității Contractante, în termen de maxim 5 zile lucrătoare de la data primirii acestora. Autoritatea Contractantă, prin recepție, va proceda la aprobarea sau respingerea rapoartelor, după caz, în termen de 15 zile lucrătoare de la data primirii acestora în forma revizuită, termen care poate fi prelungit în funcție de situațiile specifice.

10.3.4 Indicatori de performanță

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 va avea în vedere:

Indicator privind calitatea livrabilelor proiectului

- Categorie indicator: Nivelul de calitate;
- Indicator de performanță al contractului: Livrabil adecvat pentru scopul utilizării;
- Nivelul de performanță așteptat conform Caiet de sarcini: Documentele elaborate sunt conforme cerințelor stabilite în Caietul de Sarcini;
- Ce se măsoară: Nivelul de acurateţe al livrabilelor după "peer review" (sub nivelul de calitate, agreat conform cerințelor stabilite în Caietul de Sarcini și/sau prezentat în oferta tehnică).
- Modalitatea de evaluare:
  - 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 agreat. Au fost necesare doar ajustări nemateriale.

- Acceptabil (3 puncte) - Livrabilele nu includ neconformități/inexactități față de nivelul agreat însă nu includ nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului. Nu au existat întârzieri semnificative ca urmare a efectuării eventualelor remedieri.
- Nesatisfăcător (2 puncte) - Livrabilele prezinta neconformități / inexactități față de nivelul agreat iar aceste aspecte nu au putut fi corectate în totalitate într-o perioada rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost remediate de către Furnizor.
- Foarte nesatisfăcător (1 punct) - Livrabilele prezinta neconformități / inexactități majore față de nivelul agreat iar aceste aspecte nu au putut fi corectate de către Furnizor. 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.

Indicator privind termenele de predare a livrabilelor proiectului

- Categorie indicator: Nivelul de calitate;
- Indicator de performanță al contractului: Livrabil/rezultat final predat în termenul agreat;
- Nivelul de performanță așteptat conform Caiet de sarcini: Livrabilul/rezultatul final este predat conform termenului agreat în contract;
- Ce se măsoară: Livrarea la timp a rezultatelor;
- Modalitatea de evaluare:
  - Foarte satisfăcător (5 puncte) - livrate în termenele convenite în contract,
  - Satisfăcător (4 puncte) - livrate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului
  - Acceptabil (3 puncte) - livrate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate.
  - Nesatisfăcător (2 puncte) - livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului pentru mai mult de 60 de zile.
  - Foarte nesatisfăcător (1 puncte) - livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului pentru mai mult de 90 de zile.

10.4 CONFLICTUL DE INTERESE

Se aplică prevederile legii nr. 98/2016 privind achizițiile publice, cu completările și modificările ulterioare.

Pentru a se asigura independența Ofertantului, acesta va semna o declarație prin care certifică 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.

10.5 DREPTURI DE PROPRIETATE INTELECTUALĂ

Toate documentele ce vor fi elaborate în executarea Contractului (Livrabile, studii, analize, rapoarte, planuri, proceduri, metodologii, materiale de instruire şi prezentare etc) vor face obiectul dreptului exclusiv de proprietate (inclusiv, dar fără a se limita la drepturi de autor şi/sau orice alte drepturi de proprietate intelectuală) al Autorităţii 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 soluţiei tehnice create de către Prestator (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, CNAIR (cf. art. 12, alin. (1) din Ordonanţa de urgenţă nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administraţiei publice centrale şi pentru modificarea şi completarea unor acte normative: "Instituţiile publice şi organele de specialitate ale administraţiei publice centrale au obligaţia de a prevedea explicit în caietele de sarcini şi în contractele aferente procedurilor de achiziţie publică demarate de la dat intrării în vigoare a prezentei ordonanţe de urgenţă, care includ dezvoltări de programe informatice la solicitarea instituţiei sau autorităţii, 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".

Pe toata durata desfăşurării proceselor de dezvoltare a soluţiilor informatice, se vor utiliza depozitare de cod sursa aflate in patrimoniul CNAIR. Codul sursa nu va fi stocat, sub nici o forma in alta locaţie decât cea indicate de către autoritatea contractanta.

Înainte de plata facturii finale, autoritatea contractanta preia integral codul sursă al aplicaţiilor informatice dezvoltate, documentaţia aferentă şi kit-urile de instalare.

11 ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI

11.1 CONŢINUTUL PROPUNERII TEHNICE

CNAIR va îndeplini rolul de Autoritate Contractantă în prezenta procedura de achiziţie publică şi va fi Ofertantul va descrie în detaliu modul de îndeplinire a cerinţelor de realizare a activităţilor.

Oferta tehnică va cuprinde următoarele:

1. <u>Metodologia de prestare a serviciilor constituie acea parte a propunerii tehnice care prezintă strategia propusă de ofertant pentru prestarea serviciilor solicitate prin specificaţiile tehnice incluse în documentaţia de atribuire.</u>

Metodologia trebuie să cuprindă minimum următoarele informaţii:

- descrierea de ansamblu a abordării propuse de ofertant pentru prestarea serviciilor, precum şi a riscurilor aferente implementării proiectului;
- descrierea cât mai detaliată a activităţilor propuse de ofertant pentru prestarea serviciilor solicitate, cu indicarea oricăror etape / stadii considerate ca esenţiale, a rezultatelor şi efectelor aşteptate şi estimate ale fiecărei activităţi, precum şi a riscurilor specifice fiecărei activităţi;

- descrierea contribuției ofertantului, în termeni de resurse umane specializate, cunoștințe etc., necesare pentru ducerea la îndeplinire în cele mai bune condiții a activităților respective și obținerea rezultatelor;
- în cazul în care oferta este depusă de o asociere, o descriere a implicării fiecărui asociat în prestarea serviciilor solicitate, a modului de colaborare între asociați în vederea executării contractului, inclusiv prin delimitarea sarcinilor și responsabilităților individuale în prestarea serviciilor;
- descrierea oricăror aranjamente de subcontractare a unei părți a serviciilor solicitate, a interacțiunii dintre ofertant și subcontractor/i, precum și o descriere detaliată a serviciilor ce vor fi subcontractate.

Ofertanții vor prezenta, în detaliu, ca Anexă/Anexe la propunerea tehnică, metodologiile pe care le vor considera, dar nu se vor limita la:

- Managementul de Proiect
- Managementul Schimbării
- Automatizarea proceselor de instalare a infrastructurii hardware
- Dezvoltarea de soluții software
- Testare
- Management al Riscurilor și Asigurarea Calității
- Instruire
- Punere în producție
- Suport

2. Graficul de prestare a serviciilor constituie acea parte a propunerii tehnice care prezintă calendarul propus de ofertant pentru prestarea serviciilor solicitate prin specificațiile tehnice incluse în documentația de atribuire.

Metodologia va include Diagrama Gantt pentru toate activitățile proiectului, în ordinea și succesiunea logică a acestora, precizând momentele de pornire și finalizare ale fiecărei activități precum și relațiile dintre ele, alocarea tipurilor de resurse pe fiecare activitate (experți cheie și non cheie), corelate cu planurile de acțiune și respectând constrângerile din prezentul caiet de sarcini. Se va prezenta drumul critic al întregului proiect precum și punctele cheie (milestones) ale planului. Diagrama va fi prezentată la o scară care să permită vizualizarea cel puțin la nivel de lună calendaristică.

Graficul este un calendar al activităților ce vor fi derulate în cadrul contractului, conform metodologiei de prestare a serviciilor, a modului în care activitățile respective sunt reflectate în rapoarte, a legăturilor și relațiilor dintre activități și secvențialitatea acestora. Etapele de raportare pe fiecare activitate vor fi evidențiate ca activități separate.

Calendarul propus trebuie să se încadreze în termenele indicate în caietul de sarcini. Beneficiarul a indicat pentru fiecare activitate și rezultat așteptat termenul maxim la care acestea trebuie realizate, fiind în sarcina Prestatorului să propună termenele de execuție, în funcție de legăturile și condiționalitățile existente între etape și să asigure corelarea acestora din punct de vedere al secvențialității și resurselor implicate.

3. Lista licenţelor ofertate, specificând în clar numele licenţei de la producător, ediţia, producătorul, cantitatea şi unităţile de licenţiere specifice producătorului precum „User" sau „Processor Core" precum şi corelarea acestora cu cerinţele caietului de sarcini.

Lista licenţelor trebuie să cuprindă toate licenţele propuse de ofertant. Toate componentele ofertate vor trebui să fie regăsite în oferta financiară.

Produse software propuse

Nr. Crt.	Denumire componentă (*)	Producător	Nume produs propus (**)	Descriere produs	Cantitate	Unitate de măsură	Modul de licenţiere (***)	Garanţie şi/sau mentenanţă

(*) Denumirea componentei conform Caietului de Sarcini.

(**) Denumirea completă dată de producător, inclusiv ediţia (exemplu „Standard", „Enterprise", dacă este cazul). Se va insera câte un singur produs pe un rând.

(***) Va conţine detalierea modului de licenţiere al producătorului cu explicaţii privind modalitatea de îndeplinire a cerinţelor caietului de sarcini.

4. Lista echipamentelor hardware specificând în clar identificatorul unic producător (part-number) asociat fiecărui echipament şi componenta, numărul de echipamente ofertate pentru fiecare tip de echipament, configuraţia acestora, precum şi corelarea acestora cu cerinţele caietului de sarcini. Toate componentele ofertate vor trebui să fie regăsite în oferta financiară.

Infrastructura de calcul (echipamente hardware)

Nr. Crt.	Denumire componentă (*)	Producător	Echipament propus (**)	Cod echipament (***)	Descriere produs	Cantitate	Garanţie şi/sau mentenanţă

(*) Denumirea componentei de infrastructură conform Caietului de Sarcini.

(**) Denumirea completă dată de producător. Se va insera câte un singur produs pe un rând.

(***) Va conţine codul echipamentului provenit de la producător care permite identificarea unică a echipamentului.

5. Oferta financiara a serviciilor ce vor fi prestate in proiect avand ca reper Oferta Financiara Servicii.

6. Fişele tehnice ale tuturor materialelor, instrumentelor şi utilajelor propuse de ofertant pentru desfăşurarea activităţilor proiectului din care să reiasă conformitatea cu cerinţele documentaţiei de atribuire.

7. Propunerea tehnica va fi elaborata punctual, într-o anexă sub forma de tabel de conformitate (în format *pdf editabil) in care va fi înscris, in partea stingă, cerinţele tehnice din caietul de sarcini (cu precizarea capitolului şi a paginii) iar, in partea dreapta modul concret de îndeplinire a cerinţelor din caietul de sarcini (comentariul ofertantului), prezentate cat mai detaliat care sa

demonstreze corespondenta propunerii tehnice cu cerințele conținute in caietul de sarcini cat si prin indicarea documentelor tehnice (document, paragraf, pagina etc).

Cerință caiet de sarcini (cu precizarea capitolului și a paginii)	Modul concret de îndeplinire a cerinței	Referință la documentația tehnică

Nu se acceptă descrierea detaliată a modului în care este îndeplinită cerința **prin copierea conținutului cerinței**.

8. Planul de instruire, inclusiv precizarea experților responsabili propuși pentru instruire.

Ofertantul are obligația să respecte toate cerințele prezentate în caietul de sarcini și să dezvolte într-o manieră proprie și originală punctele prezentate.
Omisiunea sau neîndeplinirea corespunzătoare a oricăreia dintre cerințele prezentului caiet de sarcini poate duce la respingerea ofertei ca neconformă. Astfel, lipsa unui răspuns sau prezentarea unor descrieri nerelevante prin raportare la cerințele prezentului caiet de sarcini, ori care nu demonstrează înțelegerea contextului și obiectivelor/rezultatelor așteptate ale proiectului poate duce la descalificarea ofertantului. În acest sens se solicită din partea ofertanților și intră în răspunderea acestora prezentarea dovezilor concrete în sprijinul oricăror afirmații care se pot încadra în categoria exemplului anterior menționat.
Nerespectarea cerințelor din caietul de sarcini sau absența din cadrul conținutului propunerii tehnice a serviciilor ofertate pentru fiecare din cerințele din caietul de sarcini poate atrage încadrarea 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. Propunerea tehnică trebuie să reflecte modul în care Ofertantul înțelege să îndeplinească în integralitatea lor, cerințele prevăzute în Caietul de sarcini.

11.2 PROPUNEREA FINANCIARĂ

Propunerea financiară va fi prezentată în lei, atât în sumă globală pe fiecare activitate/subactivitate și a valorilor unitare, conform anexei la formularul de ofertă financiară
Nu există suprapuneri între costurile logistice

12 MODALITĂȚI ȘI CONDIȚII DE PLATĂ

Plata se va face eșalonat în funcție de livrări și recepții parțiale sau recepție finală, astfel:

Plata	% din valoarea contractului [lei fara TVA]	Descriere	Corespondenta grafic de implementare
1	10.00%	Avans	
2	10.00%	Plata partiala servicii analiza si proiectare	Poz 2 si 3
3	10.00%	Plata echipamente hardware site principal	Poz. 4
4	10.00%	Plata produse COTS site principal	Poz. 4 si poz. 6
5	10.00%	Plata integrala servicii analiza si proiectare	Poz 2 si 3
6	10.00%	Plata echipamente hardware site secundar	Poz. 8
7	10.00%	Plata produse COTS site secundar	Poz 8 si 9
8	10.00%	Dezvoltare module tarifare per km	Poz. 22
9	20.00%	Rest de plata	Poz. 33

Documentele tip, necesare pentru efectuarea plăților din cadrul contractului (aplicabile fiecărui livrări în parte), sunt prezentate mai jos:

1. Aviz de însoțire a mărfii (dacă este cazul);
2. Certificate de garanție și declarație conformitate (dacă este cazul);
3. Set de proceduri și mecanisme pentru coordonare și consultare factori interesați;
4. Manuale de utilizare a aplicației;
5. Suport de curs format electronic;
6. Chestionare evaluare instruire;
7. Certificate de participare;
8. Raport al activității;
9. Proces verbal de recepție calitativ și cantitativ al produselor/serviciilor cât și a raportului aferent activității;
10. Factura fiscală.

Orice obiecțiune de natură financiară sau privind calitatea rezultatelor atinse poate determina diminuarea valorii de plată. Decizia Beneficiarului de diminuare a sumei de plată va fi motivată și comunicată în scris Prestatorului.

Factura se va emite de către Prestator după recepționarea echipamentelor/serviciilor de către Autoritatea Contractantă.

13 IPOTEZE ȘI RISCURI

13.1 RISCURILE

Riscurile avute în vedere sunt:

În elaborarea ofertelor tehnice, operatorii economici trebuie să ia în calcul următoarele riscuri, care pot interveni în derularea contractului:

- Surse de ordin instituțional - factori care aparțin organizației CNAIR sau altor organizații;
- Surse de mediu legislativ - factori care provin din contextul legislativ național/comunitar/ internațional (legislația actuală aplicabilă) și evoluția legislației naționale/comunitare/internaționale;
- Surse externe (la nivel european, național) - factori ce sunt determinați de specificațiile stabilite pentru platforme
- Surse de ordin tehnic - factori care provin din constrângeri (limitări) de tip tehnic, inclusiv la nivelul datelor existente sau al formatului acestora.

Prin urmare, prezentăm o analiză calitativă a riscurilor aferente proiectului, în care s-a identificat riscul, precum și măsurile de atenuare a riscului, având în vedere impactul estimat (mic, mediu, semnificativ) și consecințele materializării riscului.

În ceea ce privește riscurile de mediu și legate de schimbările climatice, precizăm că nu există o vulnerabilitate a proiectului referitor la aceste aspecte.

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
1	Se schimba Project Managerul din echipa proiectului pe durata derulării acestuia Probabilitate: mică	Impact: semnificativ Consecințe: apariția unor disfuncționalități în gestionarea proiectului și în coordonarea echipei de proiect. Acțiuni preventive: La formarea echipei se desemnează un PM care a mai fost implicat în proiecte din același domeniu sau cel puțin din aceeași sfera și care are o stabilitate cunoscută în cadrul structurii organizatorice a CNAIR. Desemnarea unui adjunct care să cunoască toate aspectele operaționale ale proiectului și care să poată prelua aceasta funcție în cazul indisponibilității managerului de proiect desemnat inițial. Responsabili: Director General CNAIR
2	Descompletarea echipelor pe durata ciclului de viața al proiectului Probabilitate: medie	Impact: mediu Consecințe: un posibil impact semnificativ asupra activităților proiectului, livrabilelor cheie, finalizării etapelor proiectului. Pierderea unor abilitați cheie în momente critice. Acțiuni corective: Înlocuirea personalului cât mai curând posibil, permiterea unei perioade de tranziție, atunci când este posibil. Acțiuni preventive: Pregătirea și derularea unui program intern de instruire.

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
		Responsabili: manager de proiect CNAIR, Director General CNAIR
3	Rezistenta personalului beneficiarului la schimbare Probabilitate: medie	Impact: mediu Consecinţe: Probleme operaţionale. Beneficiile sistemului nu pot fi valorificate complet din cauza folosirii practicilor vechi de lucru. Acţiuni corective: problema va fi escaladată către Comitetul Director al Proiectului. Ar putea fi necesare programe de instruire suplimentare. Acţiuni preventive: obţinerea angajamentului conducerii beneficiarului că personalul său va fi informat despre importanta proiectului. Responsabili: manager de proiect CNAIR, Director General CNAIR
4	Modificări în aria de cuprindere a proiectului Probabilitate: medie	Impact: mediu Consecinţe: Posibile reevaluări ale obiectivului, costurilor şi/sau etapelor proiectului. Acţiuni corective: Reprogramarea componentelor non-critice ale proiectului pentru etapa ulterioara. Acest proces va fi desfăşurat în concordanta cu procedura de control a modificărilor. Acţiuni preventive: Asigurarea acordului tuturor factorilor decizionali importanţi în privinţa acoperirii sistemului din faza iniţială a proiectului. Responsabili: manager de proiect CNAIR / manager de proiect prestator
5	Lipsa cooperării din partea utilizatorilor Probabilitate: mica	Nivelul de implicare a utilizatorilor este esenţial atât pentru succesul sistemului cât şi pentru acceptanţa finală. Impact: mediu Consecinţe: costuri suplimentare pentru proiect, cauzate de eventuala apariţie a unor noi cerinţe. Definirea eronată a unor cerinţe funcţionale. Acţiuni corective: Escaladarea către nivelurile conducerii superioare şi obţinerea unui angajament puternic din partea Comitetului Director. Acţiuni preventive: Utilizatorii trebuie implicaţi în activităţile proiectului. Dacă este necesar se vor efectua analize ale proiectului. Responsabili: manager de proiect CNAIR / manager de proiect prestator
6	Nu se respecta termenul de	Impact: mediu

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
	implementare tehnică al proiectului. Probabilitate: medie	Consecințe: imposibilitatea respectării termenului de implementare specificat în Contractul de finanțare Acțiuni preventive: Respectarea perioadei de analiză pentru stabilirea tuturor detaliilor pentru desfășurarea dezvoltării în parametri stabiliți. Verificarea periodica a taskurilor în derulare. Acțiuni corective: stabilirea măsurilor pentru recuperarea timpului pierdut în etapele anterioare. Încheierea de acte adiționale la contractul de finanțare. Responsabili: manager de proiect CNAIR / manager de proiect prestator
7	Produsul nu respectă întocmai cerințele clientului Probabilitate: medie	Riscul apare atunci când Prestatorul nu a înțeles exact ce dorește clientul sau când nu sunt respectate specificațiile funcționale ale proiectului. Impact: Semnificativ Acțiuni preventive: Validarea etapelor intermediare astfel încât să se poată observa cât mai rapid orice deviație și pentru a se putea lua măsurile necesare pentru corectarea acestora. Responsabili: manager de proiect CNAIR / manager de proiect prestator
8	Produsul final conține bug-uri Probabilitate: medie	Impact: Mediu Acțiuni preventive: stabilirea unei etape de testare internă a fiecărei componente, apoi a unei testări integrate. Acțiuni corective: Asigurarea unei marje de timp pentru rezolvarea bug-urilor, existenta unei echipe de testare care să descopere toate bug-urile existente. Responsabili: manager de proiect CNAIR / manager de proiect prestator
9	Domeniu nou pentru dezvoltatori Probabilitate: medie	Fiind un produs inovator pe piață, dezvoltatorii sistemului pot avea dificultăți în a-și desfășura munca. Impact: Mare Acțiuni preventive: Se vor căuta dezvoltatori sau consultanți care au mai lucrat pe proiecte asemănătoare. Se va asigura buna înțelegere a procesului general de către dezvoltatori. Responsabili: manager de proiect CNAIR / manager de proiect prestator
10	Neagrearea unui plan formal pentru testarea funcțională a sistemului informatic, bazat pe scenarii clare de	Impact: Mediu Acțiuni preventive: Stabilirea unei strategii de testare și acceptanță imediat după demararea proiectului de

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
	testare, ceea ce poate duce la prelungirea excesiva a perioadei de testare, sau la apariția unor noi cerințe introduse sub formă de observații de testare. Prelungirea perioadelor de testare afectează și planificarea activităților experților pentru managementul proiectului. Probabilitate: medie	implementare a soluției informatice. Planul de contingenta pentru protejarea proiectului dacă acțiunile preventive eșuează: Întocmirea unor scenarii de testare și acceptanță agreate de ambele părți, care să ușureze activitatea de testare. Validarea de către CNAIR a strategiei de testare și acceptanță pentru sistemul informatic. Responsabili: manager de proiect CNAIR / manager de proiect prestator
11	Existența unor divergențe de opinie de natură tehnică între experții CNAIR și experții tehnici ai Prestatorului, care să determine întârzierea finalizării unor activități din proiect. Probabilitate: medie	Impact: Mediu Acțiuni preventive: Stabilirea exacta a responsabilităților și a nivelului de autoritate pentru fiecare din experții / specialiștii celor două organizații. Derularea unor întâlniri în care să fie prezentate și discutate opiniile experților și specialiștilor celor două organizații. Derularea unei sesiuni de instruire preliminare pentru prezentarea tehnologiilor utilizate în proiect. Acțiuni corective: Implicarea managerului de proiect al CNAIR și a managerului de proiect al prestatorului pentru medierea eventualelor dispute. Responsabili: manager de proiect CNAIR / manager de proiect prestator
12	Criza financiară provocată de situația geopolitica poate afecta capacitatea de derulare a achizițiilor internaționale de echipamente și produse software. Probabilitate: medie	Impact: Mare Consecințe: Dacă Ofertanții nu reușesc să obțină finanțări naționale/internaționale nu se vor putea plasa comenzile de echipamente. Acțiuni preventive: Derularea procedurilor de achiziție echipamente fără întârzieri în etapa de recepție, pentru a diminua nevoia de finanțare a proiectului. Diminuarea sumei de finanțat între momentul recepției și plata finală. Responsabili: manager de proiect CNAIR / manager de proiect prestator / Director General CNAIR

Riscurile care pot fi identificate la momentul elaborării Caietului de Sarcini și riscurile care pot apărea în derularea contractului sunt următoarele:

- dificultăți de colaborare și comunicare între factorii interesați implicați;
- datele și informațiile necesare desfășurării serviciilor comunicate de către Autoritatea Contractantă nu sunt suficiente pentru îndeplinirea cerințelor solicitate prin Caietul de Sarcini;
- adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților.

Aceste riscuri vor fi gestionate de către echipa de management a proiectului, din partea Autorității Contractante.

Ofertantul va introduce în propunerea tehnică:

- descrierea ipotezelor pe care Ofertantul trebuie să le aibă în vedere în pregătirea Ofertei și în derularea serviciilor;
- descrierea riscurilor care pot apărea pe parcursul derulării Contractului, astfel cum au fost identificate de către Autoritatea Contractantă în procesul de elaborare a Caietului de Sarcini și pe care Prestatorul trebuie să le aibă în vedere, astfel încât să propună măsuri pentru diminuarea efectelor sau eliminarea riscurilor - în cazul în care strategia de abordare a riscurilor este, în totalitate, sub controlul Prestatorului sau când și dacă Prestatorul poate contribui la diminuarea efectelor riscurilor.

Ofertantul va identifica și alte riscuri față de cele principale, arătate mai sus. În oferta se vor prezenta recomandări/propuneri de reducere sau eliminare a riscurilor care ar putea afecta implementarea proiectului (inclusiv a riscurilor prezentate mai sus).

13.2 IPOTEZELE

Ipotezele avute în vedere sunt:

- conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
- corelația dintre resursele necesare și rezultatele așteptate este realistă;
- începerea serviciilor se va realiza în perioada preconizată;
- nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
- toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Prestatorului;
- Prestatorul va semna un acord de confidențialitate la momentul semnării Contractului și va respecta toate instrucțiunile privind utilizarea informațiilor confidențiale.

În pregătirea Ofertei, Ofertantul trebuie să aibă în vedere cel puțin riscurile și ipotezele descrise mai sus. În acest sens, la întocmirea ofertei, Ofertantul trebuie să ia în considerare resursele necesare (de timp, financiare și de orice alta natură), pentru implementarea strategiilor de risc propuse.

14 ALTE MENȚIUNI

Limba de lucru este limba română. Ofertele care se vor prezenta numai pentru anumite activități sau care nu vor respecta toate condițiile prevăzute în prezentul caiet de sarcini vor fi eliminate. Prezentul caiet de sarcini, oferta tehnică și oferta financiară se constituie ca anexă la contractul încheiat între Autoritatea Contractantă și Ofertant.

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. Informații privind reglementările în vigoare la nivel național în acest

domeniu se pot obține de la Inspecția Muncii sau de pe site-ul http://www.inspectmun.ro/Legislație/legislație.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.

Avizat,
SEF DEPARTAMENT COOPERARE
INTERINSTITUTIONALA TRAFIC RUTIER
Lucian Silviu ILINA

Avizat,
SEF SERVICIU IT
Liviu CHERBIS

Sef Serviciu Administrare SIEGMCR
Bogdan RADULESCU