# 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 ..... 9
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 ..... 11
1.3.6 Compatibilitatea cu infrastructura IT a clientului ..... 11
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 ..... 16
3.4 Sisteme de virtualizare ..... 17
3.5 Sisteme de automatizare aplicații containerizate ..... 17
3.6 Sisteme de operare ..... 17
3.7 Componente hardware ..... 17
3.8 Licențe perpetue componente software ..... 17
3.9 Volumetrie ..... 19
**4 DESCRIEREA TEHNICĂ A PROIECTULUI ..... 20**
4.1 PREVEDERI DE SECURITATE ..... 20
*4.1.1 Prevederi generale de Securitate* ..... 20
*4.1.2 Nivelurile de asigurare a încrederii prin mijloace de autentificare* ..... 22
4.2 ARHITECTURA TEHNICĂ ȘI FUNCȚIONALĂ ..... 23
*4.2.1 Arhitectura funcțională* ..... 23

*4.2.2 Module necesare realizării sistemului informatic* ....28

*4.2.3 Arhitectura tehnică* ....38

4.3 CERINȚE TEHNICE PENTRU COMPONENTELE SOFTWARE DE BAZĂ ....47

*4.3.1 Componenta portal* ....47

*4.3.2 Componenta server de aplicații* ....52

*4.3.3 Componenta server web* ....53

*4.3.4 Componenta de baze de date relationale* ....54

*4.3.5 Componenta de replicare date baze de date relaționale* ....58

*4.3.6 Componenta Platforma de procesare a fluxurilor de date si analiza in timp real (stream analytics)* 59

*4.3.7 Componenta Platforma de gestiune fluxuri de date (streaming engine)* ....62

*4.3.8 Componenta de integrare și gateway pentru servicii web* ....63

*4.3.9 Componenta Big Data* ....66

*4.3.10 Componenta de analiză și prognoză* ....69

*4.3.11 Componenta GIS* ....74

*4.3.12 Stocare centralizata profile utilizatori* ....77

*4.3.13 Componenta de gestiune acces utilizatori* ....78

*4.3.14 Componenta de management centralizat echipamente firewall* ....80

*4.3.15 Componenta de virtualizare și containerizare* ....80

*4.3.16 Componenta de disaster recovery* ....82

*4.3.17 Componenta de analiză și detecție atacuri cibernetice* ....84

*4.3.18 Componenta SIEM* ....87

*4.3.19 Componenta PKI* ....92

*4.3.20 Componenta de monitorizare infrastructură și aplicații* ....94

4.4 CERINȚE TEHNICE PENTRU COMPONENTELE HARDWARE CENTRALE ....96

*4.4.1 Echipament server tip 1* ....96

*4.4.2 Echipament server tip 2* ....103

*4.4.3 Echipament stocare tip 1* ....109

*4.4.4 Echipament stocare tip 2* ....112
*4.4.5 Echipament stocare tip 3* ....116
*4.4.6 Router internet* ....118
*4.4.7 Router WAN* ....120
*4.4.8 DNS Firewall* ....122
*4.4.9 Firewall tip 1* ....126
*4.4.10 Firewall tip 2* ....131
*4.4.11 Firewall tip 3* ....136
*4.4.12 Switch LAN tip 1* ....141
*4.4.13 Switch LAN tip 2* ....144
*4.4.14 Switch LAN tip 3* ....148
*4.4.15 Switch SAN tip 1* ....151
*4.4.16 Switch SAN tip 2* ....155
*4.4.17 ADC / WAF* ....159
*4.4.18 Load Balancer* ....163
*4.4.19 Soluție de backup* ....167
*4.4.20 HSM* ....170
*4.4.21 Rack și accesorii tip 1* ....172
4.5 CERINȚE FUNCȚIONALE ....173
*4.5.1 Funcționalități Modul Nucleu central (core system)* ....173
*4.5.2 Funcționalități modul contravenții* ....175
*4.5.3 Funcționalități servicii web pentru colectare date de la operatorii SETRE* ....176
*4.5.4 Funcționalități servicii web pentru emitere roviniete si peaj* ....176
*4.5.5 Funcționalități aplicație mobila pentru înregistrare si transmitere date privind traseul parcurs de un autovehicul* ....177
*4.5.6 Funcționalități servicii web pentru achiziție roviniete , peaj si mod pre-paid distanta parcursa* 177
*4.5.7 Managementul utilizatorilor și accesul la sistem* ....177

*4.5.8 Integrarea cu alte sisteme externe* ....178
4.6 CERINȚE NON-FUNCȚIONALE ....179
**5 ETAPELE DE IMPLEMENTARE ....179**
5.1 ANALIZA ȘI PROIECTAREA ....179
5.2 DEZVOLTAREA ....181
5.3 IMPLEMENTAREA ....181
5.4 TESTAREA ȘI ASIGURAREA CALITĂȚII ....182
5.5 MIGRAREA DATELOR ISTORICE ....182
5.6 PUNEREA ÎN PRODUCȚIE ....183
5.7 GRAFICUL DE IMPLEMENTARE ....183
**6 INSTRUIRE ....185**
**7 DURATA DE EXECUTIE ....186**
**8 GARANȚIA ....186**
**9 METODOLOGIA ȘI PLANUL DE LUCRU ....191**
9.1 METODOLOGIA ....191
9.2 PLANUL DE LUCRU ....192
9.3 ORGANIZAREA ȘI PERSONALUL ....192
*9.3.1 Cerințe privind experții* ....193
*9.3.2 Experții cheie* ....194
*9.3.3 Experții non-cheie* ....196
**10 MANAGEMENTUL CONTRACTULUI ....200**
10.1 ASPECTE ORGANIZATORICE ....200
10.2 FACILITĂȚI OFERITE DE PRESTATOR ....201
10.3 METODOLOGIE DE LUCRU ȘI RAPORTARE ....202
*10.3.1 Metodologia de lucru* ....202
*10.3.2 Cerințe privind raportarea* ....203
*10.3.3 Transmiterea și aprobarea rapoartelor* ....204
*10.3.4 Indicatori de performanță* ....204
10.4 CONFLICTUL DE INTERESE ....206

10.5 DREPTURI DE PROPRIETATE INTELECTUALĂ ..... 206
**11 ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI ..... 206**
11.1 CONȚINUTUL PROPUNERII TEHNICE ..... 206
11.2 PROPUNEREA FINANCIARĂ ..... 210
**12 MODALITĂȚI ȘI CONDIŢII DE PLATĂ ..... 210**
**13 IPOTEZE ȘI RISCURI ..... 212**
13.1 RISCURILE ..... 212
13.2 IPOTEZELE ..... 216
**14 ALTE MENȚIUNI ..... 217**

# 1 INFORMAȚII GENERALE. OBIECTIVELE PROIECTULUI

## 1.1 INFORMAȚII GENERALE

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

Prezentele specificații tehnice conțin indicațiile tehnice minime și obligatorii care trebuie respectate astfel încât potențialii ofertanți să elaboreze propunerea tehnică corespunzător cu necesitățile proiectului.

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

Cerințele 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 cerințelor minime din prezentul Caiet de sarcini. Propunerea Tehnică ce conține 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 potențialii ofertanți să elaboreze propunerea tehnică corespunzător cu necesitățile autorității contractante.

**Specificațiile tehnice care indică o anumită origine, sursă, producție, un produs special, o marcă de fabricație sau de comerț, un brevet de invenție, o licență de fabricație sunt menționate doar pentru identificarea cu ușurință a tipului de produs şi nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau anumitor produse. Aceste specificații vor fi considerate ca având mențiunea "sau echivalent".**

Fără a aduce atingere altor prevederi legale sau dispozițiilor legale privind liberul acces la informațiile de interes public ori ale altor acte normative care reglementează activitatea autorității contractante, autoritatea contractantă are obligația de a nu dezvălui informațiile din propunerea tehnică, elementele din propunerea financiară și/sau fundamentări/justificări de preţ/cost transmise de operatorii economici indicate şi dovedite de aceștia ca fiind confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Caracterul confidențial se aplică doar asupra datelor/informațiilor indicate și 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 informații din propunerea tehnică, elemente din propunerea financiară şi/sau fundamentări/justificări de preț/cost sunt confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Informațiile indicate de operatorii economici din propunerea tehnică, elemente din propunerea financiară şi/sau fundamentări/justificări de preţ/cost ca fiind confidențiale 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 şi furniza documentele/lucrările specifice Contractului având în vedere toate prevederile legale naționale, europene și internaționale relevante existente la momentul semnării Contractului, precum şi cele emise ulterior, pe parcursul derulării Contractului, precum şi ansamblul reglementărilor subsecvente, al recomandărilor şi 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 şi Drumuri Naţionale 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 Naţională 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);<br>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);<br>Vehicular Communications; Geographical Area Definition; |
| 13 | ETSI TR 103 576-2 - Intelligent Transport Systems (ITS);<br>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 Unități 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

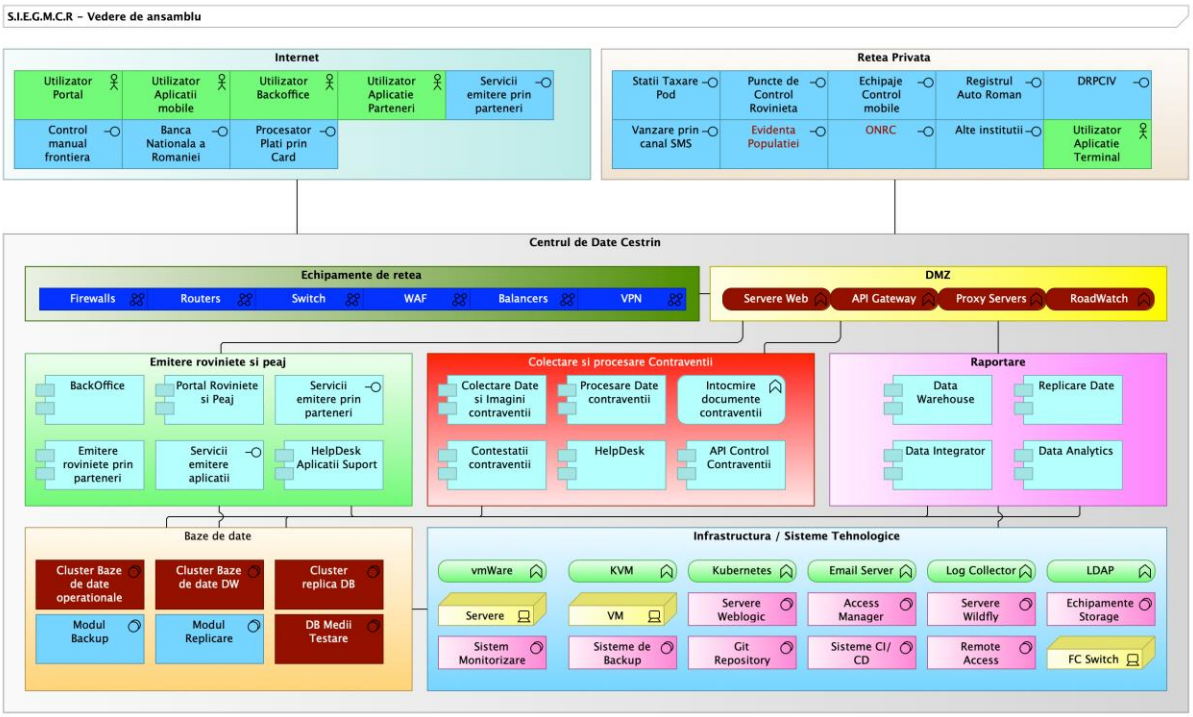



*Figura 1 Diagrama sistemului actual "SIEGMCR"*

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
  - Routere
  - IPS
  - F5 BigIP (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 |
| 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 funcționalități 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 şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice,
- Prelucrarea fotografiilor - fotografiile intră sub incidența definiţiei datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice,
- Pseudonimizare și criptare - prelucrarea datelor cu caracter personal în zona de testare într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizată, fără a se utiliza informații suplimentare,
- 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:

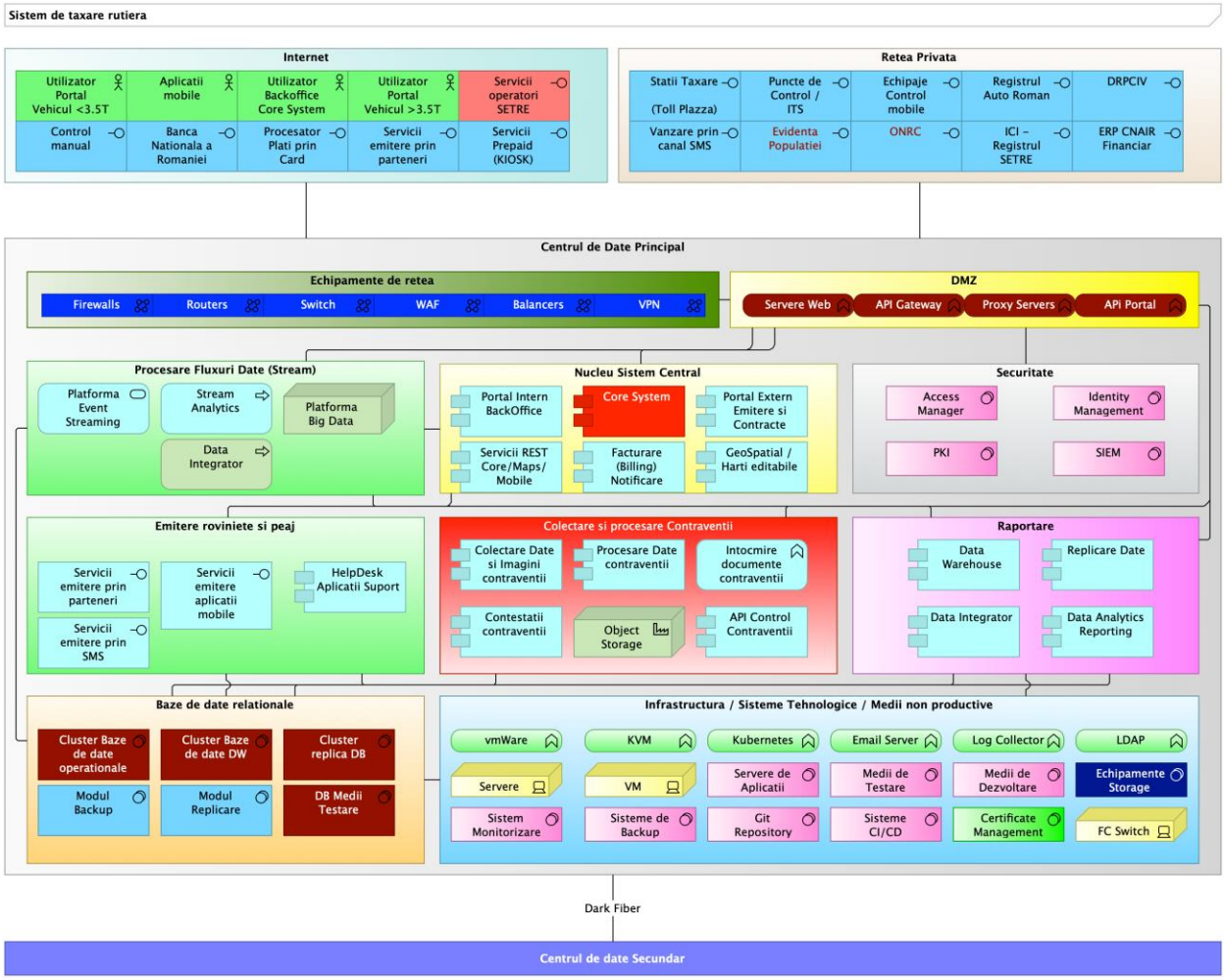



*Figura 2 Arhitectura Logica și Componentele Funcționale*

| 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<br>- Notifica inadvertente legate de mesajele recepționate (exemplu – același număr auto se afla in 2 locuri diferite)<br>- Determina daca datele recepționate pentru autovehicul sunt corecte din punct de vedere operațional (poziție geografica corecta, vehicul înrolat, etc.)<br>- 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.<br><br>Asigura prelucrarea datelor in zona Data-Warehouse |
| 6 | Componenta Nucleu central (core system) | - Gestiune nomenclatoare<br>- Gestiune clienți (persoane fizice si juridice)<br>- Gestiune tarife pentru roviniete , peaj sau tarif per km<br>- Gestiune porți virtuale (virtual gates) pentru segmente de drum<br>- Gestiune parteneri si punct de lucru parteneri<br>- Gestiune scutiri la plata rovinietei sau a tarifului de utilizare a infrastructurii rutiere<br>- Gestiune tarif pre-paid si post-paid tarif de utilizare infrastructura rutiera<br>- Gestiunea emiterilor de roviniete si peaj (inclusiv gestiunea trecerilor efectuate prin obiectivele cu tarif special)<br>- Funcționalități de backoffice |
| 7 | Componenta de colectare si procesare contravenții | Oferă servicii pentru colectarea datelor de la punctele de control sau sistemele ITS<br><br>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<br><br>Oferă servicii web pentru echipajele de control mobile<br><br>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:<br><br>- Înrolare autovehicul in sistemul de tarifare a utilizării infrastructurii rutiere<br>- 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<br>- 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 |
| 12 | Componenta GIS | - Permite definirea pozițiilor geografice ale tronsoanelor de drum care vor fi incluse in domeniile de taxare<br>- Produce harți geografice pentru afișarea vizuala a tronsoanelor de drum<br>- 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:<br>- Înrolarea unui client nou<br>- Înrolarea unui autovehicul pe oricare din cele 2 moduri de tarifare – per timp sau per kilometru<br>- Emitere roviniete si peaj |

| | | |
|---|---|---|
| | | - Expune informații clienților autentificați dupa caz despre rovinietele si peaj-ul achitat , traseul parcurs de un autovehicul si tariful aferent<br>- Notificări despre rute ocolitoare<br>- Informații despre tarifele practicate<br>- Funcționalități de tip service desk / call center digital pentru utilizatorii externi<br><br>Integrare:<br><br>- Integrare cu procesator de plăti electronice (card)<br>- Se integrează cu modulul central (core sistem)<br>- Se integrează cu modulul GIS |
| 16 | Portal Intern | - Reprezintă interfața utilizator a modulului central (core sistem) – User Interface<br>- 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.<br>- 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<br>- 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<br>- 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<br><br>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<br><br>Asigura evidenta contestațiilor<br><br>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<br><br>Persista in sisteme de tip object storage a imaginilor recepționate de la punctele de control<br><br>Asigura funcționalitatea unui punct de control fie in mod verificare locala autovehicul fie prin transmitere integrala a imaginilor autovehiculelor<br><br>Asigura suplimentar fără intervenție umana a recunoașterii numărului auto a autovehiculului din imagine (dubla verificare)<br><br>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.<br><br>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 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:<br><br>- Inventar infrastructura<br>- 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.<br><br>Certificatele si cheile publice vor fi utilizate pentru criptarea pachetelor cu mesaje de la punctele de control , sistemele ITS si echipajele mobile.<br><br>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<br><br>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.

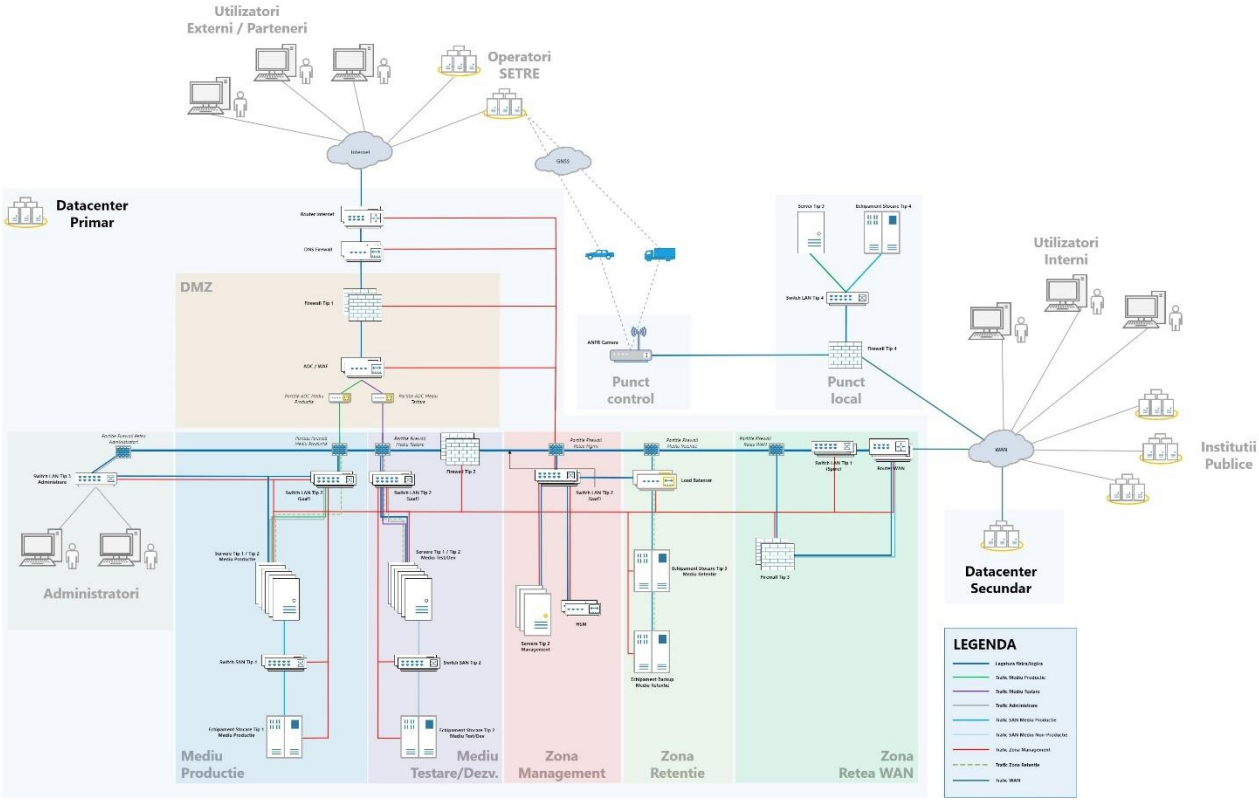



*Figura 3: Arhitectura Fizică*

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.

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

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

- versiuni noi ale produselor software licențiate, patch-uri de securitate, upgrade-uri cu îmbunătățiri ale produselor software licențiate și 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 și de integrare între componentele sistemului care să asigure implementarea cu succes a proiectului care este unul de interes național cu o arhitectura care permite integrarea cu alte sisteme informatice și servicii electronice naționale.

Dimensionarea componentelor aferente mediului de producție 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 relaționale 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 și 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 și 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 management centralizat echipamente firewall | 1 | Single Node | 8 |

| | | | | |
|---|---|---|---|---|
| 17 | Componenta de disaster recovery | 1 | Single Node | 8 |
| 18 | Componenta de analiză și detecție atacuri cibernetice | 1 | Single Node | 16 |
| 19 | Componenta PKI | 4 | Cluster Activ-Activ | 8 |
| 20 | Componenta SIEM | 4 | Single Node | 16 |
| 21 | Platforma CI/CD, Source repository, Code Quality | 6 | Cluster Distribuit | 16 |
| 22 | 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 relaționale 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 și 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 și 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 mgmt centralizat echipamente firewall | 1 | Single Node | 8 |
| 17 | Componenta de disaster recovery | 1 | Single Node | 8 |
| 18 | Componenta de analiză și detecție atacuri cibernetice | 1 | Single Node | 16 |
| 19 | Componenta PKI | 4 | Cluster Activ-Activ | 8 |
| 20 | Componenta SIEM | 4 | Single Node | 16 |
| 21 | Platforma CI/CD, Source repository, Code Quality | 6 | Cluster Distribuit | 16 |
| 22 | Alte resurse (Manager Virtualizare, Platforma Automatizare, DNS, Email) | 6 | Single Node | 8 |

Sistemul va fi compus din cel puțin următoarele componente hardware și de comunicații la nivelul site-ului principal care găzduiește mediul de producție și mediul de testare-dezvoltare:

| Nr. crt. | Componentă | Cantitate |
|---|---|---|

| | | |
|---|---|---|
| 2.4.1 | Echipament server tip 1 | 18 |
| 2.4.2 | Echipament server tip 2 | 15 |
| 2.4.3 | Echipament stocare tip 1 | 1 |
| 2.4.4 | Echipament stocare tip 2 | 1 |
| 2.4.5 | Echipament stocare tip 3 | 1 |
| 2.4.6 | Router internet | 2 |
| 2.4.7 | Router WAN | 2 |
| 2.4.8 | DNS Firewall | 2 |
| 2.4.9 | Firewall tip 1 | 2 |
| 2.4.10 | Firewall tip 2 | 2 |
| 2.4.11 | Firewall tip 3 | 2 |
| 2.4.12 | Switch LAN tip 1 | 2 |
| 2.4.13 | Switch LAN tip 2 | 6 |
| 2.4.14 | Switch LAN tip 3 | 2 |
| 2.4.15 | Switch SAN tip 1 | 2 |
| 2.4.16 | Switch SAN tip 2 | 2 |
| 2.4.17 | ADC / WAF | 2 |
| 2.4.18 | Load Balancer | 2 |
| 2.4.19 | Soluție de backup | 1 |
| 2.4.20 | HSM | 2 |
| 2.4.21 | Rack și accesorii tip 1 | 6 |

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

| Nr. crt. | Componentă | Cantitate |
|---|---|---|
| 2.4.1 | Echipament server tip 1 | 14 |
| 2.4.2 | Echipament server tip 2 | 13 |
| 2.4.3 | Echipament stocare tip 1 | 1 |
| 2.4.4 | Echipament stocare tip 2 | 1 |
| 2.4.5 | Echipament stocare tip 3 | 1 |
| 2.4.6 | Router internet | 2 |
| 2.4.7 | Router WAN | 2 |
| 2.4.8 | DNS Firewall | 2 |
| 2.4.9 | Firewall tip 1 | 2 |
| 2.4.10 | Firewall tip 2 | 2 |
| 2.4.11 | Firewall tip 3 | 2 |

| | | |
|---|---|---|
| 2.4.12 | Switch LAN tip 1 | 2 |
| 2.4.13 | Switch LAN tip 2 | 6 |
| 2.4.14 | Switch LAN tip 3 | 2 |
| 2.4.15 | Switch SAN tip 1 | 2 |
| 2.4.16 | Switch SAN tip 2 | 2 |
| 2.4.17 | ADC / WAF | 2 |
| 2.4.18 | Load Balancer | 2 |
| 2.4.19 | Soluție de backup | 1 |
| 2.4.20 | HSM | 2 |
| 2.4.21 | Rack și accesorii tip 1 | 5 |

#### 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. 2.4.12);
- **Nivelul Access**: Switch Access DC cu interfețe 10/25 Gbps (Switch LAN tip 2, cap. 2.4.13);
- **Nivelul Administrare/Operare**: Platforma hardware si software de administrare a rețelei programabile și Switch-uri de management (Switch LAN tip 3, cap. 2.4.14);

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

**Nivelul Agregare** trebuie sa îndeplinească următoarele cerințe:

- Sa conecteze toate subcomponentele nivelului Acces
- Sa asigure o comunicație redundanta si scalabila intre subcomponentele nivelului Acces

- Sa asigure comunicația intre locații prin interconectarea scalabila si reziliența cu rețeaua 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 rețea 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 rețelelor programabile din ambele locații (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 rețelei programabile ce va fi ofertată in cadrul acestui proiect. In acest scop, Platforma hardware si software de administrare a rețelei programabile ofertată va asigura următoarele funcționalități minimale:

- Să ofere o interfață grafică pentru administratorii rețelei;
- Să ofere o interfață programatică standardizată și deschisă de tip "Representational State Transfer" (REST) sau echivalent, care să faciliteze integrarea cu alte platforme și aplicații existente și viitoare;
- Să ofere un grad înalt de redundanță și reziliență care să asigure protecția (N+2) împotriva erorilor sistemelor pe care rulează Soluția de Administrare a Rețelelor din Centre de Date;
- Să ofere toate licențele necesare folosirii funcționalităților împreună cu echipamentele cerute la nivelul Agregare și nivelul Acces;
- Să asigure suportul fizic de calcul necesar pentru rularea în condiții optime de performanță, scalabilitate și redundanță, inclusiv modulele optice de conectare necesare pentru conectarea la rețea;
- Să ofere facilitați de monitorizare și administrare a anomaliilor și a erorilor de funcționare ale sistemului;
- Să ofere facilități de monitorizare a performanței atât pe termen scurt cât și pe termen lung;
- Să ofere facilități de configurare automată a echipamentelor cerute la nivelul Agregare și nivelul Acces conform unui set de reguli și politici definite prin interfața grafică sau prin intermediul interfeței programatice (API sau echivalent)
- Sa asigure segmentarea si micro-segmentarea rețelei Centrului de Date pe baza regulilor impuse de necesitățile operaționale.
- 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 informatii 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 informatii noi, precum si acces rapid la informatii 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 conținutului fără a necesita resurse de dezvoltare, distribuirea conținutului, 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 funcționalități generale:

- interfața web, facila pentru prezentare si navigare rapida si simpla;
- Posibilitatea de a personaliza conținutul;
- Caracteristici pentru securitate ridicata;
- Configurare in regim de înalta disponibilitate;
- Să ruleze pe sisteme de operare Windows, Linux si Unix.
- Sa poată fi configurat astfel încât sa permită crearea de zone securizate pe care utilizatorii sa le poată accesa din interiorul si exteriorul organizației, 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 aplicațiilor trebuie sa se facă ușor, respectând standardele in domeniu;
- Portalul trebuie sa ofere un punct centralizat de lucru pentru utilizatori si o interfața unica;
- Este necesar ca interfața portalului sa fie separata, din punct de vedere logic, de codul aplicatiilor integrate, astfel încât in cazul actualizării unei aplicații, sa se păstreze toate particularizările ce au fost efectuate asupra interfeței;
- Conținutul accesat prin portal trebuie sa poată fi automat afișat sau ascuns, pe baza rolurilor utilizatorilor, roluri care sunt predefinite;
- Administratorii trebuie sa poată controla drepturile utilizatorilor funcție de rolul acestora sau funcție de regulile definite;
- Posibilitatea de integrare și comunicare în timp real cu o soluție de Management al indentații externă portalului sau cu un director de utilizatori (AD/ LDAP) oferind inclusiv posibilitatea de sincronizare în timp real cu soluția respectivă; Posibilitatea de a folosi o bază de date externă cu utilizatori;
- Sistemul portal trebuie sa permită utilizarea de mecanisme pentru autentificare, autorizare SSO si SSL; de asemenea, trebuie sa permită si integrarea cu soluții de securitate;
- Pentru aplicațiile care nu pot fi modificare (aplicații găzduite de alt provider) soluția 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 aplicații;
- Sa permită impunerea unor filtre de acces (operațiuni de autorizare) - cel puțin interval orar si locație de rețea de unde s-a inițiat 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 informații dintr-o baza de date de conținut, fără a fi necesara restaurarea întregii soluții din care face parte acea baza de date;
- Trebuie sa permită un asistent de creare de site-uri ce permite setarea permisiunilor, crearea de șabloane de conținut si adăugarea de teme personalizate;
- Trebuie sa permită dezvoltarea de aplicatii bazate pe standarde web;
- Trebuie sa pună la dispoziție un mecanism robust de monitorizare a încărcării si performantei sistemului;
- Trebuie sa pună la dispoziție 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;
- Solutia trebuie sa ofere capabilitati de clustering si load balancing;
- Sa aibă o metodă de analiză anonimizată a traficului web, care să permită identificarea proveniență vizitatorilor, a resurselor vizitate, informatiilor demografice si dispozitivelor utilizate;
- Sa ofere suport pentru personalizare folosind un sistem de reguli care să susțină cel puțin afișarea de conținut relevant utilizatorilor pe baza informațiilor demografice ale utilizatorului, precum și activități și proprietăți asociate profilului acestuia;
- Sa includa un sistem de colectare feedback (customer satisfaction / rate your experience);
- Sa ofere funcționalități de editare instant a paginilor cu publicarea modificărilor într-un singur pas, fie la final fie programatic, specificând ce trebuie publicat, la ce ora și în ce locație;
- Să ofere posibilitatea de definire de câmpuri suplimentare cel puțin la nivel de pagini, foldere, documente, imagini, mesaje din forum, blog, calendar şi wiki. Astfel, administratorii vor putea adăuga, edita sau șterge 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 si offline, care să ofere capabilități 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 autenticității și integrității prin posibilitatea de aplicare de semnătură utilizând un certificat digital;
  - Descărcarea formularelor pe stația de lucru a solicitantului, completarea de informații și 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 informațiile completate în formular, aceste coduri fiind la rândul lor conținute 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 tipărește/scanează, dar și în cazul în care este transmis în format electronic;

- sa permită publicarea unui formular web pe orice site sau aplicatie 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 informatiilor 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 permita 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 definirea de politici de retenție pentru documente, site-uri si casute postale de echipa in funcție de diverse criterii;
- sa permita vizualizarea si editarea direct din interfata web a documentelor de tip doc, xls si ppt sau echivalent;
- sa permita filtrarea afisarii informatiilor 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 permita 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 permita 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 permitand 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 permita 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 si Unix). 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 ;
- interogarea direct din baza de date a fisierelor text externe, fara a necesita in prealabil o operatiune de incarcare intr-o tabela din baza de date inclusiv posibilitatea de a rula anumite scripturi la momentul interogarii acestor fisiere din interiorul bazei de date ;
- 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;
- definirea de tabele de tip index pentru acces rapid la anumite tabele in care datele sa fie ordonate dupa o anumita coloana;
- 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 permita interogarea istoricului modificarilor unei tabele, atat de tip DDL cat si DML, fara a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvarea periodica sau utilizarea functiei de audit

#### *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 permita 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 permita 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 permita 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.

### *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).

Pentru asigurarea securității si confidențialității datelor exportate in vederea previzionării mediilor de test, baza de date trebuie sa includă mecanisme de anonimizare si mascare a subseturilor de date astfel încât sa poată fi păstrate relațiile logice si caracteristicile acestora (tipuri de date, dimensiune, pondere, etc) dar ascunzand valoarea lor initiala. Operatiile de anonimizare trebuie realizate fie static (situatie in care datele sunt exportate sau mutate intr-un alt mediu) fie dinamic (situatie in care datele sunt anonimizare in timp real pentru utilizatorii ce acceseaza baza de date).

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

#### *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 informatii de tip text, analize statistice, calcule numerice avansate, precum si grafice interactive. 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 informatiilor
- Sa foloseasca protocolul TCP/IP pentru a trimite datele, pentru a elimina constrangerile legate de distantele geografice dintre sitemele sursa si destinatie.
- Sa permita replicarea selectiva, astfel incat in cazul in care intr-o tabela s-au modificat informatii ce nu sunt necesare in procesul de transformare, acestea sa nu fie extrase si replicate.
- Sa permita compresia datelor rutate.
- Sa permita definirea de puncte de control pentru consistenta procesului de furnizare de date.
- Sa permita extragerea datelor si colectarea acestora in fisiere independente de platforma pe care ruleaza. Fiserele astfel obtinute vor putea fi incarcate in mod continuu in baza de date destinatie
- Sa permita criptarea datelor.
- Sa permita gestionarea automata a memoriei.
- Capabilitatea de a publica datele modificate sub forma de mesaje XML.
- Asigurarea integritatii bazei de date prin aplicarea operatiilor in ordinea in care au fost comise.
- Sa permita integrarea cu instrumente de extragere, transformare si incarcare a datelor (ETL) astfel incat asupra datelor extrase sa poata fi aplicate transformari complexe.
- Sa permita rollback dinamic – funtionalitate pentru refacerea datelor in cazul in care baza de date master este corupta.

- Sa permita replicarea volumelor mari de date tranzactionale intre baze de date eterogene cu impact minim asupra sistemului de productie.
- Solutia trebuie sa fie disponibila in caz de dezastru
- Sa asigure integritatea tranzactionala asupra surselor si destinatiilor
- Sa includa functionalitati de arhivare si auditare
- Sa permita mentinerea noului sistem disponibil in permanenta, atat in timpul intreruperilor planificate, cat si a celor neplanificate.
- Sa permita timp de nefunctionare zero pentru intretinerea planificata (in timpul migrarilor si a actualizarilor).
- Sa permita replicarea datelor si sincronizarea pentru sisteme distribuite.
- Sa permita doar replicarea datelor comise
- Sa permita replicarea bidirectionala a datelor comise pe baza de jurnal
- Sa permita toleranta in caz de dezastru / recuperare in caz de dezastru
- Sa permita mecanisme de captare a datelor modificate (change data capture).
- Sa permita mecanisme rapide, paralele, masive de mutare a datelor intre bazele de date, diferite de cele standard de import/export.
- Sa permita 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 permita urmarirea imediata a tranzactiilor de la nivelul bazelor de date (sursa – destinatie).
- Sa permita replicarea instructiunilor 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 vizualizare extinsa a datelor, oferind o paleta larga de grafice cum ar fi: bar chart, pie chart sau harti
- 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 de a importa modele in format PMML pentru o varietate larga de algoritmi, cum ar fi mașini vectoriale, reguli de asociere, clasificator Naive Bayes, modele de grupare, modele text, arbori de decizie și diferite modele de regresie.
- 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 cu posibilități de vizualizare avansata
- Sa ofere posibilitatea de vizualizare in timp real a locațiilor pe harta in timp ce datele sunt procesate
- Posibilitatea de a marca vizual pe harta, funcție de anumite condiții, spre exemplu marcat cu roșu daca un parametru este mai mare decât un prag setat apriori.
- Posibilitatea de a trasa anumite poligoane pe harta in vederea definirii anumitor limite la nivelul acestora
- 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
- Sa ofere un limbaj avansat de interogare ce permite selectarea datelor din etape anterioare ale fluxului de date si definirea de reguli custom ce pot fi integrate in acesta.

#### *4.3.6.6 Deployment*

- Sa permita implementarea conceptului de Continous Integration ce va permite interpretarea in timp real a fluxurilor de date
- Cloud ready: sa permita 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 retenție a mesajelor pe o perioada de timp configurabila;
- Funcționare continuă și în cazul în care oricare din nodurile clusterului se defectează;
- Stabilirea de cote de utilizare a rețelei si a CPU;
- Sa ofere garanții 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 permita 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 functionare a clusterului, cozilor de mesaje, consumatorilor si producatorilor de mesaje;
- Sa permita streaming-ul datelor primite către alte sisteme;
- Sa permita 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 și gateway pentru servicii web*

Aceasta componenta va asigura interconectarea sistemului informatic integrat cu aplicațiile/sistemele informatice ale altor instituții, precum și 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 colecție de sarcini sau activități structurate, ce descriu un scenariu de utilizare și 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 și 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 permita 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 puțin 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 permita 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 aplicații complete prin gruparea API-urilor relevante aplicațiilor, 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 aplicație in cel puțin doua limbaje de programare majore: Java, JavaScript, .NET, Python, C;
  - Să includă capabilități de testare vizuala a API-urilor din cadrul unei aplicații, fara a avea cunoștințe de programare;
  - Să asigure modelarea și execuția fluxurilor de schimb de date in mod vizual;
  - Să permită combinarea de multiple servicii web sincrone și asincrone în cadrul fluxurilor de procese colaborative și tranzacționale;
  - Să asigure filtrarea și transformarea mesajelor XML utilizând cel puțin următoarele standarde deschise W3C Extensible Stylesheet Language Transformation (XSLT) și 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 specificațiilor standardelor WS-Security, WS-Policy și WS-Security Policy pentru a asigura criptarea / decriptarea mesajelor în vederea asigurării confidențialității mesajelor transportate si semnarea / verificarea digitală a mesajelor în vederea asigurării integrității 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 capabilități 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 direcționarea acestuia către un sistem destinație;
  - 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 permita 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 permita 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/exluderea 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:
  - permita vizualizarea si gestiunea clusterelor;
  - permita vizualizarea si gestiunea replicilor unui serviciu din cadrul clusterului, inclusive configurarea numarului de replici ;
  - permita configurarea variabilelor de environment, a retelelor atasate, a porturilor expuse, a limitelor de resurse (CPU, RAM) si a volumelor atasate;
  - permita administratorului vizualizarea log-urilor tuturor replicilor unui serviciu;
  - permita administratorului sa deschida o consola virtuala interactiva pentru accesarea containerului unui serviciu si executia de comenzi in cadrul containerului;
  - permita gestiunea retelelor virtuale;
  - permita 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 permita 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 permita ingestia datelor folosind mecasnisme de tip streaming;
  - sa permita crearea de indecsi pe unul sau mai multe coloane din cadrul unei tabele;
  - sa ofere drivere JDBC si ODBC;
  - sa permita partitionarea tabelelor;
  - sa ofere capabilitati de incarcare in memorie a datelor utilizate frecvent;
  - sa permita 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 permita crearea de interogari SQL de tip long-running, care sa genereze notificari cu privire la modificari asupra datelor;
  - sa permita 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 permita 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 permita 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;
  - permita 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 permita 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 permita executarea de job-uri multiple în mod concurent;

- Sa permita 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 permita 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 permita integrare cu sisteme de tip LDAP pentru autentificarea utilizatorilor;
- Sa permita definirea de fluxuri de tip mircoservicii
- Sa permita 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 permita 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 permita combinarea rezultatelor obținute din surse de date diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
  - Sa permita datelor în format tabelar al informațiilor afișate;
  - Sa permita crearea de rapoarte utilizand un editor vizual de interogari, dar si scrierea manuala a interogarilor SQL complexe;
  - Sa permita salvarea interogarilor SQL ca notite pentru utilizare ulterioara;
  - Sa permita definirea de tablouri de bord și includerea rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
  - Sa permita modificarea tablourilor de bord sau a rapoartelor, posibilitatea de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
  - Sa permita 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 permita crearea de coloane in cadrul tabelelor virtuale, bazate pe formule de calcul;
  - Sa permita crerea de modele virtuale de date pe baza unei interogari; sa permita utilizarea unui model virtual ca sursa de date pentru interogari noi;
  - Sa permita includerea dashboard-urilor in alte aplicatii;
  - Sa includa un mecanism de caching al datelor utilizate frecvent, pentru accelerarea timpului de livrare al rapoartelor;
  - Sa permita 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 permita 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 permita restrictionarea accesului la interogari, tablouri de bord si rapoarte, atat la nivel de utilizator, cat la nivel de grup de utilizatori;
- Sa permita auditarea actiunilor utilizatorilor, inclusiv auditarea accesului la date, precum si vizualizarea informatiilor de audit din cadrul zonei de administrare;
- Sa permita 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 informatii 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 permita 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 permita rularea de scenarii de tip “what-if”;
- Sa permita definite de sabloane de filtre ce pot fi aplicate de utilizator asupra rezultatelor unei interogari;
- Sa permita 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 permita:
  - 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 permita 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 permita creara de view-uri simple si view-uri materializate ;
- sa permita 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 permita:
  - 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 (internaţionale, naţionale şi/sau locale, fie că sunt predefinite în aplicaţie 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 permita 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. vizualizarea de straturi si obiecte 3D
f. adaugă straturi suplimentare in funcție de nevoi
g. tipări zona de harta afișata pe ecran, cu posibilitatea de configura rezolutia, formatul paginii si alte informații necesare: legenda, scara, font
h. măsura distanta, aria si orientarea (bearing)
i. distribui harta pentru includerea in aplicații externe
j. vizualiza metadatele asociate harții si ale straturilor spațiale incluse
k. vizualiza puncte de interes de pe harta impreuna cu metadatele asociate
l. exporta zona de harta afișata in formate recunoscute: GeoJSON, GML, KML, CSV, Shapefile
m. realiza interogări complexe in mod vizual dupa metadatele asociate obiectelor din cadrul hartii prin utilizarea de operatori logici (AND, OR, NOT)
n. interoga obiectele din cadrul hartii prin desenarea de catre utilizator a unei zone folosind forme geometrice de tip cerc, dreptunghi, poligon si impreuna cu un operator spatial (intersectie, bounding box, contains)

d) Portalul sa permită realizarea de prezentări interactive folosind un editor vizual in cadrul caruia se pot plasa elemente de tip pagina, harta interactiva, text, imagini si video-uri de prezentare
e) Portalul sa permită realizarea de tablouri de bord interactive prin includerea de widget-uri de tip grafic, tabel, harta si indicatori de performanta
f) Sa permită lucruri cu informații de temporale asociate straturilor spatiale, inclusiv vizualizare evolutiei stratului in timp folosind un player interactiva
g) Sa includa un motor de date spatiale care sa:
   a. organizarea modului de lucru in proiecte;
   b. permita crearea de straturi spatiale folosind baze de date si fisiere;
   c. pentru un strat spatial sa permita configurarea sistemului de coordonate, stilul de afisare si metadatele aferente;
   d. sa permita crearea de straturi spatiale ce grupeaza mai multe sub-straturi spatiale;
   e. sa permita crearea de straturi spatiale de tip raster;
   f. sa permita crearea de straturi spatiale de tip reverse-proxy catre alte servere ce contin informatii spatiale spatiale;
   g. sa includa mecanisme de caching pentru optimizarea performantei datelor spatiale si a straturilor raster;
   h. sa permita publicarea hartilor si a straturilor spatiale in formate recunoscute in industrie: WMS, WFS, WCS, WMTS;
   i. sa permita realizarea si publicarea de operatii spatiale in format WPS
   j. sa ofere un mecanism avansat securitate bazat pe utilizatori, grupuri de utilizatori si roluri care sa:
      i. permita restrictionarea accesului la straturile spatiale in functie de rolurile asociate;

ii. permita 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. permita integrarea cu servere LDAP;
v. permita integrarea cu mecanisme de tip Single Sign-On;
vi. permita aplicarea de filtre asupra seturilor de date spatiale pentru a restrictiona accesul catre anumite zone;

k. sa permita 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 permita rularea in mediu containerizat, precum si pe sisteme de operare Linux, Unix si Windows
m. sa oferea API-uri de dezvoltare de tip REST pentru dezvoltarea de aplicatii.

h) 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;
i) Definirea de hărţi tematice;
j) Sistemul trebuie sa permita 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 informatiile georeferentiate.
k) Componenta geospațială trebuie sa permita selectia straturilor din hartile afisate;
l) Sa permita 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. permita 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. permita 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 cerințe funcționale 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 experienței de utilizare dar și pentru a creste nivelul de securizare și a scădea costurile operațiunilor administrative legate de controlul accesului la aplicațiile și componentele sistemului, se dorește implementarea unei componente de securizare a accesului la interfețe web si servicii web in mod centralizat.

#### 4.3.13.1 Soluție gestiune acces utilizatori aplicații web si servicii web

Pentru optimizarea costurilor autoritatea contractanta dorește reutilizarea licențelor 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 dorește implementarea unei soluții care sa satisfacă cel puțin următoarele cerințe tehnice:

- Sa protejeze resursele împotriva acceselor neautorizate - atât din interiorul cat și 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 aplicații;
- Sa permită administratorului sistemului sa poată alege metode de autentificare și autorizare diferite in funcție de alocarea grupurilor;
- 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;
- 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 reușite, autentificări nereușite, autorizări reușite, autorizări nereușite 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;
  - WS-Trust, WS-Federation;
  - 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 prin intermediul standardului XACML;

- 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 management centralizat echipamente firewall*

Soluția oferă posibilitatea de configurare și monitorizare centralizată a tuturor funcțiilor oferite de echipamentele de tip firewall oferite. Soluția trebuie sa fie ofertata de la același producător cu producătorul soluțiilor de tip firewall.

Soluția trebuie ofertata sub forma de mașina virtuala să ofere următoarele funcționalități:

- Gestionarea centralizată a echipamentelor de tip firewall oferite;
- Permite automatizarea fluxurilor de lucru și distribuirea configurațiilor și politicilor de securitate pentru echipamentele de comunicații oferite;
- Oferă posibilitatea creării de șabloane de configurare pe echipamente pentru distribuție către alte echipamente similare din rețea;
- Configurarea colectivă a setărilor echipamentelor de tip firewall prin utilizarea șabloanelor avansate;
- Backup automat al configurațiilor echipamentelor gestionate;
- Oferă administratorilor o bază de date cu modele de configurare;
- Administrare bazată pe roluri;
- Instalare într-un mediu virtual cu multiple opțiuni pentru gestionarea dinamică a stocării
- Soluția oferită va fi dimensionata pentru toate echipamentele de tip firewall din proiect, conform cu centralizatorul de echipamente.

#### *4.3.15 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 și va oferi următoarele funcționalități:

- 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 suport pentru o gamă largă de sisteme de operare instalate la nivel de mașină virtuală - Windows (Server: 2019, 2016, 2012 R2, 2008 R2, 2003 R2; Desktop: 10, 8.1, 7), Red Hat (7, 8, 9), 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 cu până Ia 768 de CPU-uri logice și 16TB de memorie RAM;
- Să permită rularea de aplicații mari consumatoare de resurse, oferind suport de configurare a mașinilor virtuale cu până la 256 procesoare virtuale și 6TB 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 crearea de grupuri virtuale de resurse (memorie şi procesor) pentru controlul și asigurarea performanțelor maşinilor virtuale care folosesc în comun respectivele grupuri de resurse;
- Asigură suport pentru Trusted Platform Module (TPM) 2.0 la nivel de hipervizor si pentru virtual Trusted Platform Module (TPM) 2.0 pentru mașinile virtuale, asigurând astfel o protecție și integritate sporită atât pentru hipervizor cât și pentru sistemele de operare guest;
- Asigură suport pentru tehnologiile VBS (virtualization-based security) integrate în noile sisteme de operare Microsoft - Windows 2016 si Windows 2019;
- Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalități disponibile în noile versiuni de procesoare;
- Asigură posibilitatea de criptare a tuturor fișierelor asociate unei mașini virtuale, indiferent de sistemul de operare din mașina virtuală sau de tipul de stocare folosită;
- Asigură posibilitatea criptării traficului necesar migrării unei mașini virtuale în funcționare de pe un host pe altul, caracteristică ce poate fi setată la nivelul mașinii virtuale;
- Asigură identificarea automată a celei mai bune modalități de stocare a unei mașini virtuale, în funcție de nivelul de servicii asociat acesteia și să ofere informații în timp real privind conformitatea cu nivelul de servicii asociat;
- Permite gruparea mai multor volume de stocare cu performanțe similare în clustere pentru simplificarea managementului și plasarea inteligentă respectiv balansarea încărcării (în funție spațiul disponibil sau timpul de acces la sistemul de stocare) mașinilor virtuale în mod automat la nivel de cluster;
- Permite balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vedere asigurării resurselor optime pentru funcționare;
- Asigură funcționalitate de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster;
- Să ofere arhitecturi cu disponibilitate continuă, fără întreruperea funcționării mașinilor virtuale configurate cu pana la 8 CPU-uri virtuale și 128GB RAM și independent de sistemul de operare folosit, în cazul defectării fizice a host-urilor pe care acestea rulează;

- Să dispună de capacități de failover astfel încât, în cazul defectării parțiale a unui host, mașinile virtuale care rulau pe acel host să fie migrate automat pe celelalte host-uri din cluster iar host-ul degradat să fie trecut automant în mentenanță după evacuarea mașinilor virtuale;
- Să dispună de capacități de failover astfel încât, în cazul blocării sistemului de operare instalat într-o mașină virtuală, respectiva mașina virtuală să fie restartată automat pe același host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor;
- Să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster;
- Să ofere posibilitatea de boot-are rapidă în cazul aplicării actualizărilor, prin eliminarea timpilor mari necesari inițializării hardware în timpul procesului de boot;
- Asigură comutatoare de reţea virtuale (switch-uri) administrate centralizat, la care să se conecteze maşinile virtuale şi interfețele de rețea fizice de pe fiecare host;
- Permite creare de profile pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri să se facă foarte rapid, respectând o configuraţie prestabilită, configurabilă pentru eliminarea erorilor umane de configurare;
- Asigură o platformă unificată pentru rularea în paralel a mașinilor virtuale și a containerelor;
- Asigură dezvoltatorilor accesul de tip self-service la resursele mediului virtual folosind API-urile Kubernetes, menținând totodată politicile și controlul securității în conformitate cu nevoile IT-ului;
- 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.

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

#### *4.3.16 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, permitand 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, permitand 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.

### *4.3.17 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 interfață grafică interactivă prin care utilizatorul poate vizualiza activitatea de analiză și monitorizare.
Accesarea interfeței grafice se poate realiza dintr-un browser web, folosind o conexiune criptată bazată pe certificat digital.
Pentru conexiunea la interfața grafică este necesară autentificarea utilizatorului pe baza unui nume de utilizator și a unei parole.
Interfața grafică dispune de un meniu principal cu diverse opțiuni disponibile unui utilizator în funcție de permisiunile acestuia.
Descoperă/identifică subrețelele și dispozitivele din cadrul acestora din rețeaua analizată.
Echipamentul furnizează, în funcție de traficul analizat, informații despre dispozitivele identificate.
Soluția facilitează vizualizarea istoricului de alerte pentru un dispozitiv informatic.
Pentru fiecare dispozitiv se poate selecta un interval de timp pentru a vedea istoricul conexiunilor.

Soluția asigură gruparea dispozitivelor informatice în baza unor activități similare (ex: conexiuni către aceeași destinație).
Din interfața 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 și control accesate din interiorul rețelei se pot extrage/vizualiza dispozitivele interne care au efectuat conexiuni către acesta.
Utilizatorul poate modifica intervalul de timp pentru care se dorește vizualizarea alertelor.
Alertele identificate sunt afișate în interfața grafică în funcție de nivelul de severitate atribuit de către echipament. De asemenea se poate alege un interval de timp pentru vizualizare.
Pentru fiecare alertă soluția va furniza detalii suplimentare precum: data și ora, cine a generat alerta (adresă IP, hostname, etc.).
Utilizatorul are opțiunea 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 afișarea dispozitivelor în funcție de un tip de comportament / categorie de detecție.
Pentru fiecare dispozitiv soluția generează și stochează informații despre comportamentul dispozitivului sub forma unui istoric al conexiunilor realizate. Asupra acestui istoric de conexiuni utilizatorul poate aplica opțiuni de filtrare. De asemenea utilizatorul poate descărca conexiunile sub forma unui fișier .pcap.
Soluția trebuie să poată genera rapoarte automate despre întreaga rețea și incidentele detectate. Rapoartele pot fi descărcate pentru vizualizarea într-o aplicație externă.
Utilizatorul poate eticheta (poate adăuga tag-uri) anumite incidente, dispozitive sau utilizatori din rețea.
Soluția dispune de un modul ce asigură o căutare avansată în datele colectate din trafic. Căutarea poate fi realizată în funcție 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

### *4.3.18 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 permita 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 permita 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 permita 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 permita 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 permita 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 permita integrarea cu solutii de securitate de la vendori precum: Cisco, Fortinet, Juniper, PaloAlto, Microsoft.
Solutia trebuie sa permita stocarea unor informatii 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.

### *4.3.19 Componenta PKI*

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

- Autentificare
- Confidențialitate
- Integritate

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

- Autentificare: va fi asigurata prin certificate digitale emise la nivel local, pentru fiecare dispozitiv și server în parte. Sistemul va utiliza aceste certificate digitale pentru autentificare prin integrare și cu componenta de gestiune a identității utilizatorilor și a accesului.
- Confidențialitate: va fi asigurata prin criptarea informațiilor, utilizând tehnologiile PKI și algoritmi standard recunoscuți la nivel internațional. Sistemul va utiliza certificatele digitale pentru criptare.
- Integritate: Sistemul va utiliza certificatele digitale și se va integra cu echipamentele HSM pentru criptarea informațiilor și verificarea validității semnăturilor astfel încât să fie asigurată non-repudierea.

Platforma PKI trebuie să asigure următoarele funcționalități:

- Integrare cu echipamentele HSM ofertate pentru utilizarea capabilităților de criptare hardware;
- Scanarea întregii rețele pentru certificate și consolidarea acestora într-un depozit central;
- Descoperirea de certificate din surse diferite, indiferent de CA emitent. Suport pentru procese de descoperire la cerere, programate și recurente;
- Scanează certificate SSL într-o varietate de locații, inclusiv servere de e-mail SMTP, balansoare de încărcare, AWS, AD, MS-CA și 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 menținerea la zi a informațiilor din depozit, astfel încât acesta să țină evidența certificatelor și 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.

### *4.3.20 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*

| | |
|---|---|
| Procesor | Tehnologie:<br>- Tip: CISC 64 biţi tip Intel Xeon generația a treia sau echivalent;<br>- Nuclee: 28 fizice per procesor;<br>- Frecvența de bază: minim 2,6 GHz;<br>- Cache: minim 42 MB Smart Cache sau echivalent.<br>- Magistrală: 3 x UPI 11,2 GT/s sau echivalent<br>- Putere consumată: maxim 235 W<br>Număr de procesoare instalate: minim 2<br>Număr de procesoare instalabile: minim 2 |
| Memorie RAM | Cel puțin 512 GB DDR4 ECC 3200 MT/s, suport pentru tehnologii de protecție de tip patrol scrubbing, SDDC sau echivalent;<br>Min. 32 sloturi de memorie (din care 16 libere) disponibile în șasiu, posibilitate de instalare 4 TB de memorie RAM DDR4. |
| Capacitate de stocare interna | Șasiu cu 8 sloturi hot-swap de tip 2.5”;<br>Serverul va fi echipat cu cel puțin 2 module 200GB SSD configurate în RAID 1, dedicate pentru instalarea sistemului de operare; |
| Controller RAID intern | Controller RAID cu suport pentru RAID 0, 10, 1, 5, 50, 6, 60; Memorie cache instalată la nivelul controller-ului de min 8 GB de tip DDR4 non-volatile; Controller-ul trebuie să dispună de mecanisme interne de mărire a capacității online, configurare de disk hot-spare dedicat si global; |
| Interfață video | Interfață video integrată ce suportă o rezoluție minimă de 1920 x 1200 |
| Interfețe rețea | Minim 4 porturi 10 Gb SFP+, echipate cu tranceivere SR, formate din două placi distincte<br>Minim 4 porturi 32 Gbps Fibre Channel |
| Porturi | Minim: 1 x serial, 2 x VGA (din care 1 frontal), minim 2 x USB 2.0 și 2 x USB 3.0; |
| Management | Sistem încorporat de monitorizare a: procesoarelor, memoriilor, HDD-urilor, interfețelor IO, ventilatoarelor, surselor de alimentare, temperaturii; analize predictive de eroare pentru componentele sistemului cu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componente. |

| | |
|---|---|
| | LCD display sau panou cu LED-uri ce trebuie sa permită citirea mesajelor de eroare cu panoul frontal instalat, fără operațiuni suplimentare; |
| | Aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului, capabilă de instalare locală și *remote* în mod neasistat, inclusiv configurare RAID; |
| | Echipamentul trebuie să fie livrat cu capabilități hardware și software, instalate, activate și licențiate pentru următoarele funcționalități:<br>- management de la distanță;<br>- redirectare interfață grafică cu tastatură și mouse;<br>- suport pentru virtual clipboard: copiere, taiere, lipire text de pe consola virtuală pe serverul gazdă;<br>- posibilitate de pornire/oprire de la distanță;<br>- suport pentru remote media (virtual CD);<br>- suport pentru SSL (Secure Socket Layer);<br>- integrare cu Active Directory / LDAP (Lightweight Directory Access Protocol);<br>- autentificare two-factor;<br>- monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice;<br>- managementul evenimentelor și alarmelor;<br>- inventarul și monitorizarea componentelor (inclusiv GPU, module optice SFP);<br>- instalarea update-urilor și patch-urilor;<br>- analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat;<br>- realizarea de rapoarte de performanță pe baza datelor transmise de senzori (streaming telemetry) care indică utilizarea resurselor sistemului de calcul (procesor, memorie, I/O), consumului de energie electrică, temperatură, independent de sistemul de operare și fără a consuma resurse de procesor din server;<br>- repornirea și reconfigurarea automată a serverului;<br>- permite generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere similare din infrastructură;<br>- permite stocarea pe un NAS extern cu funcționalități de retenție a fișierelor pentru a asigura protecția la ștergere și modificare a fișierelor |

| | |
|---|---|
| | de update, șabloanelor de configurare și imaginilor de sistem de operare;<br>- permite ștergerea securizată a unităților de stocare de tip SSD și HDD;<br>- validare a configurației serverului față de o referință;<br>- RESTFul API cu suport Redfish;<br>- Interfețe acces utilizator: HTML5 Web GUI, SSH, telnet, redirecționare pe port serial;<br>- Funcționalitățile vor fi asigurate fără a fi necesară instalarea de agenți software. |
| | Port dedicat 1 Gigabit Ethernet ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului; |
| Format | Serverul rackabil trebuie să fie montabil în rack-uri standard de 19”.<br>Înălțimea maximă a Serverul rackabil trebuie să fie 2 RU.<br>Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive).<br>Serverul rackabil trebuie să aibă LED de localizare pentru controlul poziţiei.<br>Bezel frontal cu posibilitate de securizare echipament și LCD pentru indicarea stării sistemului. |
| Securitate | Trusted Platform Module 2.0;<br>Posibilitatea de a dezactiva butonul de pornire (*power*) din BIOS;<br>Capabilități incluse pentru *chassis intrusion detection*;<br>Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate;<br>Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS *boot loader* și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze;<br>Suport hardware inclus pentru verificarea și validarea autenticității *firmware*-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare);<br>Update-urile de *firmware* trebuie să fie semnate criptografic de către producătorul echipamentului ofertat pentru a fi autentificate la instalare;<br>Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare |

| | |
|---|---|
| | (conturi utilizator sau certificate). Log-urile acestor informații de audit vor fi securizate și vor putea fi accesate doar din componenta de management a soluției propuse;<br>Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului;<br>Suport inclus pentru utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare și posibilitatea de a utiliza un certificat personalizat pentru semna un Linux OS *boot loader*;<br>*Firmware rollback;* |
| Surse alimentare electrica | Serverul trebuie alimentat printr-un sistem de surse de alimentare electrică care trebuie să îndeplinească următoarele cerințe:<br>- număr surse interne instalate: minimum 2;<br>- funcționare în regim „N+1”;<br>- surse de tip „hot pluggable”;<br>- putere: minim 1100 W per sursă.<br>Ofertantul trebuie să livreze minim 2 cabluri de alimentare de tip bypass C13-C14 pentru conectarea la PDU. |
| Compatibilitate sisteme de operare | Citrix Xen Server 8.2 LTSR, Microsoft Windows Server 2016&2019, Hyper-V, Red Hat Enterprise Linux 7&8, SUSE Linux Enterprise Server 15, Ubuntu Server LTS 20.04, VMware ESXi 6.7&7 |
| Garantie si suport | Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare - *Next Business Day*) care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri.<br>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.<br>Suportul software va oferi 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).<br>Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate moral, ce nu se mai află in linia de fabricație a producătorului).<br>Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. |
| Cerințe Virtualizare | - 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;<br>- oferă suport pentru o gamă largă de sisteme de operare instalate la nivel de mașină virtuală - Windows (Server: 2019, 2016, 2012 R2, 2008 R2, 2003 R2; Desktop: 10, 8.1, 7), Red Hat (7, 8, 9), SuSE, Ubuntu, Debian, Oracle Linux;<br>- Să asigure o densitate mare de mașini virtuale, oferind suport pentru configurații fizice generoase la nivel de host, prin configurarea cu până la 768 de CPU-uri logice și 16TB de memorie RAM;<br>- Să permită rularea de aplicații mari consumatoare de resurse, oferind support de configurare a mașinilor virtuale cu până la 256 procesoare virtuale și 6TB RAM;<br>- Să asigure rate mari de consolidare a mașinior 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;<br>- Suport larg pentru aplicații terțe din partea ISV (Independent Software Vendors);<br>- Permite crearea de grupuri virtuale de resurse (memorie şi procesor) pentru controlul și asigurarea performanțelor mașinilor virtuale care folosesc în comun respectivele grupuri de resurse; |

| | |
|---|---|
| | - Asigură suport pentru Trusted Platform Module (TPM) 2.0 la nivel de hipervizor si pentru virtual Trusted Platform Module (TPM) 2.0 pentru mașinile virtuale, asigurând astfel o protecție și integritate sporită atât pentru hipervizor cât și pentru sistemele de operare guest;<br>- Asigură suport pentru tehnologiile VBS (virtualization-based security) integrate în noile sisteme de operare Microsoft - Windows 2016 si Windows 2019;<br>- Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalități disponibile în noile versiuni de procesoare;<br>- Asigură posibilitatea de criptare a tuturor fișierelor asociate unei mașini virtuale, indiferent de sistemul de operare din mașina virtuală sau de tipul de stocare folosită;<br>- Asigură posibilitatea criptării traficului necesar migrării unei mașini virtuale în funcționare de pe un host pe altul, caracteristică ce poate fi setată la nivelul mașinii virtuale;<br>- Asigură identificarea automată a celei mai bune modalități de stocare a unei mașini virtuale, în funcție de nivelul de servicii asociat acesteia și să ofere informații în timp real privind conformitatea cu nivelul de servicii asociat;<br>- Permite gruparea mai multor volume de stocare cu performanțe similare în clustere pentru simplificarea managementului și plasarea inteligentă respectiv balansarea încărcării (în funție spațiul disponibil sau timpul de acces la sistemul de stocare) mașinilor virtuale în mod automat la nivel de cluster;<br>- Permite balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vedere asigurării resurselor optime pentru funcționare;<br>- Asigură funcționalitate de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster;<br>- Să ofere arhitecturi cu disponibilitate continuă, fără întreruperea funcționării mașinilor virtuale configurate cu pana la 8 CPU-uri virtuale și 128GB RAM și independent de sistemul de operare folosit, în cazul defectării fizice a host-urilor pe care acestea rulează; |

| | |
|---|---|
| | - Să dispună de capacități de failover astfel încât, în cazul defectării parțiale a unui host, mașinile virtuale care rulau pe acel host să fie migrate automat pe celelalte host-uri din cluster iar host-ul degradat să fie trecut automant în mentenanță după evacuarea mașinilor virtuale;<br>- Să dispună de capacități de failover astfel încât, în cazul blocării sistemului de operare instalat într-o mașină virtuală, respectiva mașina virtuală să fie restartată automat pe același host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor;<br>- Să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster;<br>- Să ofere posibilitatea de boot-are rapidă în cazul aplicării actualizărilor, prin eliminarea timpilor mari necesari inițializării hardware în timpul procesului de boot;<br>- Asigură comutatoare de reţea virtuale (switch-uri) administrate centralizat, la care să se conecteze maşinile virtuale şi interfețele de rețea fizice de pe fiecare host;<br>- Permite creare de profile pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri să se facă foarte rapid, respectând o configuraţie prestabilită, configurabilă pentru eliminarea erorilor umane de configurare;<br>- Asigură o platformă unificată pentru rularea în paralel a mașinilor virtuale și a containerelor;<br>- Asigură dezvoltatorilor accesul de tip self-service la resursele mediului virtual folosind API-urile Kubernetes, menținând totodată politicile și controlul securității în conformitate cu nevoile IT-ului;<br>- 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;<br>- 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; |

### *4.4.2 Echipament server tip 2*

| | |
|---|---|
| Procesor | Tehnologie:<br>- Tip: CISC 64 biţi tip Intel Xeon generația a treia sau echivalent;<br>- Nuclee: 24 fizice per procesor;<br>- Frecvența de bază: minim 2,4 GHz;<br>- Cache: minim 36 MB Smart Cache sau echivalent.<br>- Magistrală: 3 x UPI 11,2 GT/s sau echivalent<br>- Putere consumată: maxim 235 W<br>Număr de procesoare instalate: minim 2<br>Număr de procesoare instalabile: minim 2 |
| Memorie RAM | Cel puțin 512 GB DDR4 ECC 3200 MT/s, suport pentru tehnologii de protecție de tip patrol scrubbing, SDDC sau echivalent;<br>Min. 32 sloturi de memorie (din care 16 libere) disponibile în șasiu, posibilitate de instalare 4 TB de memorie RAM DDR4. |
| Capacitate de stocare interna | Șasiu cu 8 sloturi hot-swap de tip 2.5”;<br>Serverul va fi echipat cu cel puțin 2 module 200GB SSD configurate în RAID 1, dedicate pentru instalarea sistemului de operare; |
| Controller RAID intern | Controller RAID cu suport pentru RAID 0, 10, 1, 5, 50, 6, 60; Memorie cache instalată la nivelul controller-ului de min 8 GB de tip DDR4 non-volatile; Controller-ul trebuie să dispună de mecanisme interne de mărire a capacității online, configurare de disk hot-spare dedicat si global; |
| Interfață video | Interfață video integrată ce suportă o rezoluție minimă de 1920 x 1200 |
| Interfețe rețea | Minim 4 porturi 10 Gb SFP+, echipate cu tranceivere SR, formate din două placi distincte<br>Minim 4 porturi 32 Gbps Fibre Channel |
| Porturi | Minim: 1 x serial, 2 x VGA (din care 1 frontal), minim 2 x USB 2.0 și 2 x USB 3.0; |
| Management | Sistem încorporat de monitorizare a: procesoarelor, memoriilor, HDD-urilor, interfețelor IO, ventilatoarelor, surselor de alimentare, temperaturii; analize predictive de eroare pentru componentele sistemului cu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componente. |
| | LCD display sau panou cu LED-uri ce trebuie sa permită citirea mesajelor de eroare cu panoul frontal instalat, fără operațiuni suplimentare; |

| | |
|---|---|
| | Aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului, capabilă de instalare locală și *remote* în mod neasistat, inclusiv configurare RAID; |
| | Echipamentul trebuie să fie livrat cu capabilități hardware și software, instalate, activate și licențiate pentru următoarele funcționalități:<br>- management de la distanță;<br>- redirectare interfață grafică cu tastatură și mouse;<br>- suport pentru virtual clipboard: copiere, taiere, lipire text de pe consola virtuală pe serverul gazdă;<br>- posibilitate de pornire/oprire de la distanță;<br>- suport pentru remote media (virtual CD);<br>- suport pentru SSL (Secure Socket Layer);<br>- integrare cu Active Directory / LDAP (Lightweight Directory Access Protocol);<br>- autentificare two-factor;<br>- monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice;<br>- managementul evenimentelor și alarmelor;<br>- inventarul și monitorizarea componentelor (inclusiv GPU, module optice SFP);<br>- instalarea update-urilor și patch-urilor;<br>- analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat;<br>- realizarea de rapoarte de performanță pe baza datelor transmise de senzori (streaming telemetry) care indică utilizarea resurselor sistemului de calcul (procesor, memorie, I/O), consumului de energie electrică, temperatură, independent de sistemul de operare și fără a consuma resurse de procesor din server;<br>- repornirea și reconfigurarea automată a serverului;<br>- permite generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere similare din infrastructură;<br>- permite stocarea pe un NAS extern cu funcționalități de retenție a fișierelor pentru a asigura protecția la ștergere și modificare a fișierelor de update, șabloanelor de configurare și imaginilor de sistem de operare; |

| | |
|---|---|
| | - permite ștergerea securizată a unităților de stocare de tip SSD și HDD;<br>- validare a configurației serverului față de o referință;<br>- RESTFul API cu suport Redfish;<br>- Interfețe acces utilizator: HTML5 Web GUI, SSH, telnet, redirecționare pe port serial;<br>- Funcționalitățile vor fi asigurate fără a fi necesară instalarea de agenți software. |
| | Port dedicat 1 Gigabit Ethernet ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului; |
| Format | Serverul rackabil trebuie să fie montabil în rack-uri standard de 19”.<br>Înălțimea maximă a Serverul rackabil trebuie să fie 2 RU.<br>Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive).<br>Serverul rackabil trebuie să aibă LED de localizare pentru controlul poziției.<br>Bezel frontal cu posibilitate de securizare echipament și LCD pentru indicarea stării sistemului. |
| Securitate | Trusted Platform Module 2.0;<br>Posibilitatea de a dezactiva butonul de pornire (*power*) din BIOS;<br>Capabilități incluse pentru *chassis intrusion detection*;<br>Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate;<br>Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS *boot loader* și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze;<br>Suport hardware inclus pentru verificarea și validarea autenticității *firmware*-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare);<br>Update-urile de *firmware* trebuie să fie semnate criptografic de către producătorul echipamentului ofertat pentru a fi autentificate la instalare;<br>Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Log-urile acestor informații de audit vor fi |

| | |
|---|---|
| | securizate și vor putea fi accesate doar din componenta de management a soluției propuse;<br>Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului;<br>Suport inclus pentru utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare și posibilitatea de a utiliza un certificat personalizat pentru semna un Linux OS *boot loader*;<br>*Firmware rollback;* |
| Surse alimentare electrica | Serverul trebuie alimentat printr-un sistem de surse de alimentare electrică care trebuie să îndeplinească următoarele cerințe:<br>- număr surse interne instalate: minimum 2;<br>- funcționare în regim „N+1”;<br>- surse de tip „hot pluggable”;<br>- putere: minim 1100 W per sursă.<br>Ofertantul trebuie să livreze minim 2 cabluri de alimentare de tip bypass C13-C14 pentru conectarea la PDU. |
| Compatibilitate sisteme de operare | Citrix Xen Server 8.2 LTSR, Microsoft Windows Server 2016&2019, Hyper-V, Red Hat Enterprise Linux 7&8, SUSE Linux Enterprise Server 15, Ubuntu Server LTS 20.04, VMware ESXi 6.7&7 |
| Garantie si suport | Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare - *Next Business Day*) care să garanteze diagnosticarea echipamentului sau modului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri.<br>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.<br>Suportul software va oferi 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.<br>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).<br>Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate moral, ce nu se mai află in linia de fabricație a producătorului).<br>Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. |
| Cerințe Virtualizare | - oferă o arhitectură independentă de un sistem de operare de uz general cu o amprentă pe disc cât mai mică (max 300 MB) și care 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;<br>- oferă suport pentru o gamă largă de sisteme de operare instalate la nivel de mașină virtuală - Windows (Server: 2019, 2016, 2012 R2, 2008 R2, 2003 R2; Desktop: 10, 8.1, 7), Red Hat (4,5,6,7), SuSE, Ubuntu, FreeBSD, Debian, CentOS, Solaris, Oracle Linux;<br>- Să asigure o densitate mare de mașini virtuale, oferind suport pentru configurații fizice generoase la nivel de host, prin configurarea cu până la 768 de CPU-uri logice și 16TB de memorie RAM;<br>- Să permită rularea de aplicații mari consumatoare de resurse, oferind support de configurare a mașinilor virtuale cu până la 128 procesoare virtuale și 6TB RAM;<br>- Să permită utilizarea disk-urilor rapide instalate pe server pentru configurarea ca read cache la nivel de mașină virtuală sau de disk, oferind astfel performațe deosebite pentru aplicațiile Tier 1 (simultan cu soluția de stocare hiper-convergentă);<br>- Să asigure rate mari de consolidare a mașinior 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;<br>- Suport larg pentru aplicații terțe din partea ISV (Independent Software Vendors); |

| | |
|---|---|
| | - Permite crearea de grupuri virtuale de resurse (memorie şi procesor) pentru controlul și asigurarea performanțelor maşinilor virtuale care folosesc în comun respectivele grupuri de resurse;<br>- Asigură suport pentru Trusted Platform Module (TPM) 2.0 la nivel de hipervizor si pentru virtual Trusted Platform Module (TPM) 2.0 pentru mașinile virtuale, asigurând astfel o protecție și integritate sporită atât pentru hipervizor cât și pentru sistemele de operare guest;<br>- Asigură suport pentru tehnologiile VBS (virtualization-based security) integrate în noile sisteme de operare Microsoft - Windows 10, Windows 2016 si Windows 2019;<br>- Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalități disponibile în noile versiuni de procesoare;<br>- Asigură posibilitatea de criptare a tuturor fișierelor asociate unei mașini virtuale, indiferent de sistemul de operare din mașina virtuală sau de tipul de stocare folosită;<br>- Asigură criptarea traficului necesar migrării unei mașini virtuale în funcționare de pe un host pe altul, caracteristică ce poate fi setată la nivelul mașinii virtuale;<br>- Asigură identificarea automată a celei mai bune modalități de stocare a unei mașini virtuale, în funcție de nivelul de servicii asociat acesteia și să ofere informații în timp real privind conformitatea cu nivelul de servicii asociat;<br>- Permite gruparea mai multor volume de stocare cu performanțe similare în clustere pentru simplificarea managementului și plasarea inteligentă respectiv balansarea încărcării (în funție spațiul disponibil sau timpul de acces la sistemul de stocare) mașinilor virtuale în mod automat la nivel de cluster;<br>- Permite balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vedere asigurării resurselor optime pentru funcționare;<br>- Asigură funcționalitate de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster;<br>- Să dispună de capacități de failover astfel încât, în cazul defectării parțiale a unui host, mașinile virtuale care rulau pe acel host să fie |

| | |
|---|---|
| | migrate automat pe celelalte host-uri din cluster iar host-ul degradat să fie trecut automant în mentenanță după evacuarea mașinilor virtuale;<br>- Să dispună de capacități de failover astfel încât, în cazul blocării sistemului de operare instalat într-o mașină virtuală, respectiva mașina virtuală să fie restartată automat pe același host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor;<br>- Să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster;<br>- Să ofere posibilitatea de boot-are rapidă în cazul aplicării actualizărilor, prin eliminarea timpilor mari necesari inițializării hardware în timpul procesului de boot;<br>- Asigură comutatoare de reţea virtuale (switch-uri) administrate centralizat, la care să se conecteze maşinile virtuale şi interfețele de rețea fizice de pe fiecare host;<br>- Permite creare de profile pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri să se facă foarte rapid, respectând o configuraţie prestabilită, configurabilă pentru eliminarea erorilor umane de configurare;<br>- Oferă interfața unică de management bazată pe interfața web HTML 5, accesibilă de pe majoritatea sistemelor de operare și browser-erelor existente precum Firefox (Windows, Mac OSX), Google Chrome (Windows, Mac OSX), IE sau Edge (Windows) pentru simplificarea managementului;<br>- Soluția de management centralizat să fie disponibilă ca appliance virtual pentru simplificarea instalării, actualizării și administrării precum și pentru reducerea costurilor asociate (ex. licență sistem de operare, licență bază de date);<br>- Soluția de management centralizat permite nativ configurarea în înaltă disponibilitate pentru evitarea situațiilor de downtime la nivelul de management; |

### *4.4.3 Echipament stocare tip 1*

Acest echipament este destinat pentru stocarea datelor aferente bazelor de date relaționale și mediilor virtuale de producție și alte date cu cerințe ridicate de performanță. Echipamentul trebuie sa respecte următoarele cerințe minimale:

- Echipament de ultimă generație, cu caracteristici de performanță extrem de ridicate, situat în categoria high-end enterprise în gama de produse a producătorului acestuia;
- Poate fi instalat în rack-urile standard 42U și poate fi ulterior, dacă va fi cazul, amplasat în alt rack al beneficiarului, după dorința acestuia;
- Asigură o disponibilitate de 99,9999%;
- Capacitate utilă instalată: minim **500 TB in RAID 6** pe discuri flash/SSD de același tip
- Echipamentul trebuie să aibă funcționalități avansate de deduplicare și compresie hardware; pentru eficiență optimă, echipamentul ofertat trebuie să conțină funcții integrate de deduplicare și compresie de tipul “in-line” (în timp real);
- Capacitatea de stocare livrată va fi exclusiv flash drive (maxim 2TB per disc/modul flash), atât cea solicitată inițial cât și cea prevăzută suplimentar de către Ofertant / Furnizor în momentul livrării sau pe durata proiectului
- Minim două discuri spare deja instalate, cu funcționare tip hot-spare
- Minim 4 controllere cu funcționare activ-activ simetrică (prezentarea în mod activ-activ a tuturor LUN-unilor, în mod nepreferențial către servere) pentru acces de tip bloc si minim doua controllere pentru acces de tip file;
- Minim 2TB memorie cache de tip RAM per sistem, cu protecție pentru cădere de tensiune pe termen lung
- Conectivitate front-end (porturi pentru conectarea host-urilor): minim 16 porturi FC 32Gbps (câte 4 pe fiecare controller); minim 8 porturi 10Gbps Ethernet SFP
- Conectivitate back-end (porturi pentru conectarea controllerelor la discuri): fiecare controller va dispune de porturi back-end care să asigure o lărgime de bandă totală de cel puțin 128Gbps
- În configuraţia ofertată echipamentul de stocare trebuie să asigure o performanţă de cel puţin 300000 IOPS cu timp de răspuns de maxim 1 ms în cazul rulării Vdbench cu workload cu block-size de 32 KB, random/secvenţial 70%/30%, rata de citire/scriere 50%/50%, cu deduplicarea si compresia datelor activate.
- Toate componentele și subansamblele echipamentului (inclusiv surse de alimentare și ventilație) vor fi în configurație redundantă și vor putea fi înlocuite fără a afecta buna funcționare a echipamentului (hot-swap)
- Suport oficial de la producător pentru sistemele de operare Windows Server și Linux Enterprise, precum și pentru soluții de virtualizare VMware, KVM ;
- Software-ul trebuie licențiat pentru întreg echipamentul de stocare și funcționalitățile minime obligatorii solicitate de entitate contractantă, indiferent de capacitatea inițială și viitoare a acestuia.
- În cazul unor defecțiuni a unităților de disk flash/SSD , constatarea defectului se face de către Furnizor la sediul Beneficiarului. Furnizorul are obligaţia de a înlocui (pe cheltuială proprie) unitatea de disk flash/SDD defectă (inclusiv in cazul in uzurii prin rescriere) cu una nouă, care să îndeplinească minim caracteristicile unității defecte.

- Echipamentul de stocare va fi livrat cu următoarele funcționalități de bază:
  - Thin Provisioning, mecanism de alocare virtuală a capacității de stocare;
  - Snapshot, pentru realizarea copiilor locale instantanee (minim 256 de sesiuni), manual si mod programatic cu opțiune de retenție si ștergere automată a acestuia atunci când expiră (Scheduled Snapshot);
  - Clonare, permite realizarea copiilor locale integrale, cu impact minimal asupra performanțelor echipamentului de stocare (nu se acceptă încărcări mai mari de 15% asupra sistemului pentru activitățile de clonare);
  - Echipamentul trebuie să includă funcționalități care permit resincronizarea 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 relația dintre volume a fost eliminată la un moment dat;
  - Crearea de volume virtuale (VVOLs), compatibile cu soluția/soluțiile de virtualizare utilizate în cadrul soluției integrate
- Administrare prin consola tip WEB/GUI și CLI
- Managementul tuturor funcționalităților se va realiza prin intermediul unei interfețe unice, centralizat, cu suport pentru integrare LDAP.
- Sistemul de administrare WEB/GUI, va permite cel puțin realizarea următoarelor activități:
  - Creare, ștergere, modificare grupuri diskuri fizice și/sau virtuale
  - Creare, ștergere, modificare volume, LUN-uri
  - Creare grupuri consistente de volume
  - Definire, modificare, ștergere servere (tip hosts sau targets) și grupuri de servere
  - Definire, modificare, ștergere porturi FC per sistem și per server (host)
  - Definire, modificare, ștergere politică copiere la distanță, adăugare volume, creare grupuri (tip storage replication)
  - Creare, modificare, ștergere utilizatori și roluri de tip: citire, audit, editare, administrator, service - sau similar.
  - Crearea de rapoarte istorice sau diagrame de performanță în timp real minim pentru:
    - Grad încărcare discuri fizice, statistici performanță (număr de IO, mărime date transferate - ex. KBs/sec, timpi de răspuns în ms)
    - Grad de utilizare porturi, viteza transfer, volum date transferate, statistici performanță (număr de IO, mărime date transferate - ex. KBs/sec, timpi de răspuns în ms)
    - Date statistice cu privire la volume și grupuri/seturi de volume
    - Grad de utilizare controllere, încărcare procesoare, performanță și încărcare memorie cache
    - Statistici LUN, performanță pe fiecare LUN (număr de IO, mărime date transferate - ex. KBs/sec, timpi de răspuns în ms)
    - Vizualizare alerte, probleme discuri fizice, grupuri, volume, porturi FC și Ethernet etc.

- Monitorizarea performanței sistemului și auditarea log-urilor în manieră istorică (generare și vizualizare rapoarte pentru 1 zi, 7 zile, 30 de zile etc)

- Echipamentul de stocare all flash ofertat include mecanisme de integrare directă cu echipamentul de realizare si stocare a backup-ului pe disc, cu deduplicare a datelor. Prin integrare directa, entitatea contractanta defineste mecanismul de copiere a datelor ce se va realiza direct intre echipamentul de stocare si echipamentul de backup pe disc deduplicat (mapare directa a echipamentului de backup la echipamentul de stocare si copiere datelor prin FC), fara necesitatea de trecere a datelor printr-un al treilea echipament de tip host (server).

### *4.4.4 Echipament stocare tip 2*

Acest echipament este destinat pentru stocarea datelor aferente bazelor de date relaționale și mediilor virtuale de testare-dezvoltare și alte date cu cerințe ridicate de performanță. Echipamentul trebuie sa respecte următoarele cerințele minimale:

- Tip: sistemul solicitat trebuie sa fie de tip All-NVMe (toate drive-urile si modulele de expansiune suportate sa aiba interfata NVMe), sa foloseasca protocolul NVMe pentru conectarea drive-urilor Flash propuse la controller-e si sa suporte atat medii de stocare NAND, cat si SCM (Storage-Class Memory), ca medii de stocare persistente pentru stocarea datelor; sistemul trebuie sa folosească tehnologii inline de reducere a datelor (compresie si deduplicare)
- Controller: sistemul solicitat va fi echipat cu minimum 2 controller-e hot-swap, prin care se pot scrie și citi datele simultan, ambele controller-e fiind active atat in front-end (accesul dinspre servere se va face prin ambele controller-e), cat si in back-end (accesul catre mediile de stocare All-Flash se va face prin ambele controller-e, care vor procesa in paralel operatii IO catre mediile de stocare)
- Sistemul va dispune de minimum urmatoarele porturi instalate (conectivitate), toate populate cu transceiver-e optice:
  - 8 porturi 25 Gbps SFP+ (4 porturi per controller) pentru acces de tip file (SMB, NFS), respectiv block (iSCSI); porturile trebuie sa suporte si protocolul NVMe over TCP
  - 8 porturi FC 32 Gbps (4 porturi per controller) echipate cu module optice SR multimode; porturile trebuie sa suporte atat protocolul FCP, cat si NVMe over FC;
  - Cel puțin un slot liber per controller pentru scalabilitate ulterioară, prin adăugarea de module I/O cu porturi FC 32 Gbps, porturi 100 Gbps Ethernet sau porturi 25 Gbps Ethernet;
- Memorie cache: minim 1,024 GB memorie cache de tip RAM pe sistem, in configuratia propusa (512 GB pe fiecare controller)
- Medii de stocare instalate: pentru stocarea datelor, echipamentul va avea instalata la livrare o capacitate brută de minimum **500 TB** folosind drive-uri NVMe SSD, iar sistemul va permite cresterea capacitatii brute pana la **1.25 PB** pe drive-uri NVMe SSD, prin upgrade ulterior, fara adaugarea de controller-e suplimentare; sistemul va include (în capacitatea brută) o capacitate de rezerva (spare) de dimensiunea unui drive, distribuita pe toate drive-urile propuse, pe care sa se reconstruiasca datele

pierdute in cazul defectării unui drive; datele stocate pe drive-urile propuse vor fi protejate prin RAID-5; toate drive-urile trebuie sa fie de tip SED (Self-Encrypting Drive), pentru criptarea tuturor datelor stocate cu un impact minim asupra performantei; nu se accepta drive-uri SSD ce folosesc integral sau partial tehnologie QLC (Quad-Level Cell)

- Capacitatea de stocare efectiva: sistemul va pune la dispozitie o capacitate efectivă alocabilă către host-uri de cel puțin 80 TiB, in configuratia propusa, in urma aplicarii metodelor de reducere a datelor (compresie si deduplicare); in situația în care sistemul nu oferă capacitatea efectivă solicitată, furnizorul va livra beneficiarului drive-uri Flash suplimentare, de acelasi tip cu cele ofertate, pana la atingerea capacitatii de stocare solicitate (80 TiB), pe toată perioada de garantie si suport a echipamentului.
- Suport extensie capacitate de stocare și scalabilitate: solutia propusa trebuie sa suporte configurarea mai multor sisteme intr-un cluster multi-controller (de cel putin 8 controller-e), in vederea cresterii performantei si capacitatii; sistemul va permite o scalabilitate la minimum 5 PiB capacitate totală brută, in configurație maxima; soluția trebuie sa permită adăugarea in cluster de noduri cu module de stocare tip SCM (Storage Class Memory), folosite ca medii de stocare persistente pentru stocarea datelor
- Număr host-uri suportate: minim 500 host-uri SAN
- Număr maxim LUN-uri: minim 1,000
- Dimensiune maximă file system: minim 200 TB
- Dimensiune maxima LUN/volum: minim 200 TB
- Protocoale suportate pentru accesul la date: echipamentul ofertat va avea suport inclus, unificat, pentru: FCP (Fibre Channel Protocol), NVMe over FC (inclusiv pentru VMware vVols), iSCSI, NVMe over TCP, VMware vVols 2.0, SMB (1, 2, 3, 3.1.1), NFS (v3, v4, v4.1), FTP si SFTP
- Mecanisme de reducere a datelor:
  - Sistemul propus trebuie sa dispuna de mecanisme de compresie si deduplicare inline, accelerate prin componente hardware. In cazul in care sistemul detecteaza o incarcare foarte mare a procesoarelor, trebuie sa poata decide sa amane procesul de deduplicare pentru un moment in care incarcarea procesoarelor scade, pentru a permite sistemului sa raspunda rapid operatiilor IO dinspre servere
  - Mecanismul de deduplicare trebuie sa fie global, pentru intreg sistemul de stocare cu doua controller-e, si nu la nivel de volum, storage pool sau controller
- Protecția si replicarea datelor:
  - Suport inclus pentru a realiza copii complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp (snapshot). Sistemul va permite realizarea de clone ale volumelor existente, bazate pe snapshot-uri, astfel încât acestea să poată fi montate imediat către sistemele host în mod read-write. La rândul lor volumele de tip clona vor putea avea definite snapshot-uri
  - Suport software inclus pentru replicarea nativa a datelor în mod asincron, la distanță, între sisteme similare. Replicarea va putea fi parametrizata la nivel de RPO (Recovery Point Objectiv) într-un

interval de 5 minute - 24 ore. Replicarea trebuie sa poata fi configurata individual, pentru date accesate la nivel de Block, File sau vVol

- Sistemul va permite definirea de politici de protecție aplicabile la nivel de volum (inclusiv volume de tip clona) și de grupuri de volume, în care să poate fi incluse politicile de realizare a snapshot-urilor și politicile de replicare
- Suport inclus pentru integrarea cu soluții de tip anti-virus pentru scanarea fișierelor vehiculate de serverele NAS, prin protocol CIFS/SMB, astfel încât să asigure identificarea și eliminarea amenințărilor înainte ca acestea să infecteze sistemul ce accesează fișierele stocate
- Suport inclus pentru protocol NDMP în configurație 3-way pentru asigurarea interconectării cu sisteme de tip librărie de benzi în vederea realizării operațiunilor de backup, cu suport atât pentru backup-uri full cât și incrementale

- Facilitați de management: echipamentul va include porturi de management de minimum 1Gbps Ethernet pe fiecare controller; sistemul intern de management și monitorizare al echipamentului de stocare va oferi minimum următoarele facilități:
  - Va fi accesibil de la distanță prin interfață grafică web-based HTML 5, CLI, REST API
  - Va dispune de acces securizat SSL
  - Va permite definirea de utilizatori locali având roluri cu permisiuni diferite, precum si suport LDAP pentru integrarea cu sisteme Active Directory sau echivalent
  - Va permite, pentru exporturile prin VMware vVols, vizualizarea minimum a numelui mașinii virtuale, a capacității provizionate și a capacității ocupate efectiv pe datastore
  - Pentru mediile virtuale VMware, va include suport pentru accelerarea hardware a operațiunilor ce au loc între hipervizor și sistemul de stocare, prin degrevarea unor procese de la nivelul hipervizorului și preluarea lor la nivelul echipamentului de stocare. Aceasta funcționalitate va permite accelerarea mutării unei mașini virtuale între două volume de date ale hipervizorului și accelerarea efectuării de copii ale mașinilor virtuale
  - Va asigura suport inclus pentru analiza și monitorizarea volumelor alocate către sistemele host. Sistemul de stocare va permite vizualizarea în mod grafic din interfața de management locală a parametrilor de tip lățime de banda (bandwith), numărul total de IOPS și timpul de răspuns la nivel de volum. Toate informațiile vor fi disponibile pe o perioada de minimum un an de zile (în urmă) de la momentul la care se face interogarea
  - Va permite update, upgrade software și hardware al echipamentului de stocare menținând accesul la date, fără întreruperea serviciilor
  - Volumele definite vor putea fi grupate în grupuri de volume asupra cărora se vor putea aplica politici de protecție colective
  - Sistemele host vor putea fi grupate astfel încât un volum să poata fi mapat la un grup de sisteme host (de exemplu, un cluster)

- Sistemul va dispune de mecanisme interne inteligente care să analizeze încărcarea din punct de vedere a capacității la nivelul controller-elor, a stării acestora și a limitărilor maximale de resurse ce pot rula pe ele. Astfel, în cazul în care sistemul detectează o anomalie în funcționare (defect hardware, controller offline, capacitate insuficienta), realizează o analiza predictiva a resurselor bazata pe date istorice, si prezinta un set de recomandări care va permite migrarea online a volumelor între oricare dintre controller-ele sistemului. Migrarea va putea fi făcută atât asistat cât și manual. La definirea de volume noi, sistemul va lua în calcul datele rezultate din mecanismele interne inteligente și va oferi o propunere de plasare automată a volumului care va lua în calcul toți parametrii menționați pentru o stare și o încărcare optima a întreg sistemului
- Soluția propusă va oferi o platformă unificată de management care va permite vizualizarea resurselor hardware, consumul acestora, erori și evenimente, cât și posibilitatea de a se conecta la portalul de support al producătorului pentru deschiderea și gestionarea tichetelor de service (evenimente hardware, evenimente software). Producătorul echipamentului de stocare va pune la dispoziție atât un număr de contact telefonic cât și un portal web în care sa apară istoricul evenimentelor de service, starea evenimentelor în desfășurare cât și posibilitatea de a deschide unele noi. Tot în cadrul portalului vor fi disponibile actualizări ale software-ului ce rulează pe platforma, ghiduri de configurare și administrare, cât și informații despre garanția soluției și suportul software. Portalul va facilita interacțiunea cu inginerii de service ai producătorului prin chat
- Pe toată durata de garanție și suport a soluției propuse, producătorul / furnizorul va pune la dispoziție o soluție centralizată cu punct unic de acces (de tip portal in Cloud) care va permite vizualizarea informațiilor legate de performanța, capacitatea, configurație și starea sistemului:
  - Din punct de vedere al informațiilor ce privesc performanța soluției, va permite:
    - vizualizarea grafică a informațiilor pentru sistemul monitorizat legate de lățimea de banda, numărul de IOPs, încărcarea pe procesor, dimensiunea blocurilor de date vehiculate, latenta, numărul de cozi (queue lenght), ponderea operațiilor de scriere / citire, încărcarea la nivel de controller din interiorul sistemului
    - vizualizarea datelor va fi disponibilă de la instalarea echipamentului, pe o perioada egală cu suportul echipamentului (atât timp cât echipamentul este în suport, toate datele statistice de performanță vor fi disponibile pe toată perioada)
  - Din punct de vedere al informațiilor ce privesc capacitatea soluția va permite:
    - vizualizarea grafică a informațiilor pentru sistemul monitorizat legate de capacitatea utilă configurată, capacitatea folosită, capacitatea libera, capacitatea provizionată
    - vizualizarea grafică a informațiilor pentru sistemul monitorizat legate de eficiența sistemului de stocare luând în calcul numărul de copii în timp (snapshots), coeficientul de reducere ce rezultă în urma compresiei și deduplicării și supra-alocarea capacității utile către servere (thin provisioning)

- vizualizarea grafică a informațiilor pentru sistemul monitorizat legate de distribuția capacității folosite între tipurile de resurse (volume, datastore-uri alocate către VMware, snapshot-uri, sisteme de fișiere)
- vizualizarea grafică a informațiilor pentru sistemul monitorizat legate de durata de viață a discurilor de tip flash

o Din punct de vedere al informațiilor ce privesc configurația și starea sistemului soluția va permite:

- vizualizarea nivelului de cod de sistem de operare ce rulează pe sistemul de stocare
- vizualizarea de informații legate de alertele critice ale sistemului de stocare (disk-uri, porturi, controllere, căi de comunicație cu serverele)
- vizualizarea de informații ce privesc suportul echipamentului și perioada de expirare a acestuia
- vizualizarea de informații ce privesc numărul de sisteme de tip host conectate, sistemul de operare ce rulează pe acesta, protocolul pe care se conectează și numărul de inițiatori

- Licențiere software: toate funcționalitățile software solicitate vor fi activate, licențiate pe echipamentul ofertat, indiferent de capacitatea de stocare prezenta sau viitoare, indiferent de numărul de host-uri ce se vor conecta la echipamentul de stocare
- Sisteme de operare și virtualizare suportate (echipamentul va include licențele necesare accesului sistemelor de operare suportate): Microsoft Windows Server 2016, 2019 si 2022; Microsoft Hyper-V; VMware ESXi 6.5, 6.7 si 7.0; Red Hat Enterprise Linux 8 si 9; SUSE Linux Enterprise Server 12 (SP3-SP5) și 15 (SP1-SP3); Oracle Linux 8 si 9, sisteme de virtualizare Linux
- Se va asigura acces 24x7 in centrul online de suport al producatorului echipamentului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de nivelul de severitate. De asemenea, pe perioada suportului se va asigura dreptul de a face update-uri si upgrade-uri ale tuturor componentelor software (sistem de operare, firmware etc).

### *4.4.5 Echipament stocare tip 3*

Acest echipament este destinat pentru stocarea imaginilor si a altor documente gestionate de către sistem la nivel central. Echipamentul trebuie sa respecte următoarele cerințe minimale:

- Sistemul de stocare trebuie sa fie de tip object storage.
- Sistemul de stocare trebuie sa includă o capacitate completa de minim 1536TB fara pierderi de capacitate datorita mecanismelor de tip RAID sau similare.
- Memorie RAM: minim 64GB per nod.
- Sistemul trebuie sa nu aiba limitari din punct de vedere scalabilitate iar performanta sa crească direct proporțional cu orice creștere de capacitate.
- Sistemul trebuie sa fie complet redundant fara vreo componenta de tip “single point of failure”.

- Sistemul trebuie sa includa mecanisme de protectie la scriere cat si discuri tip SSD pentru access rapid la metadate fara a fi necesar accesarea discurilor rotationale.
- Datele stocate trebuie sa fie segmentate si protejate printr-o dispersie a acestora peste noduri multiple aparținând sistemului de stocare de obiecte.
- In cazul unor obiecte de mici dimensiuni sistemul trebuie sa includă un mecanism de eficientizarea a alocării resurselor sistemului.
- Creșterea de capacitate sa fie posibila prin adaugarea unui nod ce va continue resurse de calcul, de memorie si stocare in mod integrat.
- Sistemul trebuie sa fie de tip “multitenant” si sa poată fi monitorizat si integrat in infrastructura prin “SNMP traps” si “SYSLOG”.
- Sistemul trebuie sa sustina in mod nativ protocoale multiple de scriere si citire, interoperabile dpdv al accesului la date, ca AWS S3, OpenStack Swift, NFS, HDFS, inclusiv integrare cu sisteme de operare MS Windows/SMB.
- Sistemul trebuie sa sustina procese de criptare a datelor tip “at rest” si “in-flight”.
- Sistemul trebuie sa permita criptarea datelor la nivel de obiect, bucket sau sistemul in intregime prin cel putin doua metode de criptare.
- Sistemul nu trebuie sa limiteze ca numar sau marime obiectele, grupurile de obiecte sau zonele alocate.
- Sistemul trebuie fie eficient limitand cresterea metadatelor prin stocarea obiectelor mici si mari.
- Sistemul trebuie sa protejeze in aceiasi masura metadatele si obiectele salvate si sa utilizeze mecansime de compresie.
- Protectia metadatelor trebuie sa utilizeze un mecanism de protectie avansata “triple mirroring” sau similar.
- Sistemul trebuie sa permita cautarea unui sub set de date parte a unui singur obiect fara a fi necesar citirea intregului obiect astfel incat aplicatia sa utilizez exact datele de care are nevoie.
- Sistemul trebuie sa includa un portal de cautare dupa caracteristicile metadatelor salvate atat pentru “user-defined”, cele personalizate, cat si cele aferente sistemului, “system defined”.
- Sistemul trebuie sa includa capabilitati de monitorizare, de protectie si control a datelor conform SEC Rule 17a-4(f) si cu mecanisme de securizare compliant regulilor STIG.
- Sistemul trebuie sa includa capabilitati de a bloca accesul utilizatorilor sau a aplicatiilor la obiectele scrise si protejate in baza politicilor de retentie fara ca acestea sa poata fi modificate sau sterse.
- Sistemul trebuie sa permita cel putin doua nivele de securizare a datelor la scriere impotriva oricarei incercari de accessare neautorizata.
- Sistemul trebuie sa includa cel putin urmatoarele capabilitati de securitate a datelor:
  - Retention policy on bucket and object level;
  - Litigation Hold;
  - Event-Based Retention;
- Sistemul trebuie sa permita aplicarea politicilor de retentie la nivel de obiect sau bucket.

- Sistemul trebuie sa permita autentificarea, autorizare si controlul accesului prin integrare cu Active Diectory, LDAP, Keystone si IAM.
- Sistemul trebuie sa permita integrarea cu sisteme externe de administrare a cheilor de securitate.
- Sistemul trebuie sa permita alocarea de cote, la nivel de bucket cat si al intregului sistem. Acestea trebuie sa fie de cel putin doua tipuri, pentru alerte si pentru a bloca scrierea unor date suplimentare.
- Sistemul trebuie sa permita categorisirea obiectelor prin asignare de etichete specifice cu informatii despre acel obiect.
- Sistemul trebuie se se integreze direct cu Data Domain astfel incat backup set-ruile cu retentie lunga, deduplicate, sa poata fi mutate in mod automat din Data Domain direct in sistemul de stocare de tip obiect, pentru optimizarea costurile salvarii si protectiei datelor pe termen lung.
- Sistemul trebuie sa includa un serviciu nativ de replicare la distanta cat si un serviciu de replicare geografica bazat pe o distributie globala a datelor pentru eficientizarea consumului de capacitate alocat fiecarui obiect indiferent din ce locatie este accesat acesta.
- Sistemul trebuie sa includa mecanisme de consistenta continua si consistenta a obiectelor distribuite.
- Sistemul trebuie sa ofere posibilitatea de a se integra prin capabilitati avansate tip REST API.
- Sistemul trebuie sa permita replicare asincrona a obiectelor catre un sistem similar asigurand consistenta datelor printro replicare la nivelul segmentelor.
- Procesul de replicare trebuie sa permita utilizarea criptarii datelor pe parcursul replicarii acestora.

#### *4.4.6 Router internet*

| | |
|---|---|
| **Descriere hardware** | - Echipament cu functii de rutare echipat cu minimum:<br>  ○ 2 interfete 10Gbps (SFP+)<br>  ○ 4 interfete 1Gbps BASE-T<br>- Memorie:<br>  ○ DRAM: 8 GB (sa permita up-grade pana la minim 32GB)<br>  ○ Flash: 16 GB<br>- Echipamentul trebuie sa fie montabil in rack-uri standard de 19” si sa includa accesoriile necesare montarii; maxim 1RU |
| **Performanta** | - Minimum:<br>  ○ 15 Gbps throughput IPSec<br>  ○ 19 Gbps trafic IPv4<br>  ○ 3900 tunele IPSec<br>  ○ 1.5 Milioane route IPv4<br>  ○ 1.5 Milioane route IPv6<br>  ○ 1.2 Milioane sesiuni NAT<br>  ○ 4000 instante virtuale de rutaj (VRF-uri) |

| | |
|---|---|
| | - Echipamentul va asigura trafic criptat de minim 2 Gbps, duplex |
| **Functionalitati retelistica** | - Sistemul de operare al echipamentului oferit va asigura urmatoarele standarde:<br>o RIP, OSPF, EIGRP, BGP, IS-IS, DHCP, IGMPv3, PIM SM, PIM SSM, RSVP, L2TPv3, BFD, MPLS<br>o GRE, PPP, PPPoE, MLPPP, HDLC<br>o QoS, PBR, PfR, NBAR<br>o VRF<br>o IP SLA |
| **Functionalitati securitate** | - Sistemul de operare al echipamentului oferit va asigura urmatoarele functionalitati:<br>o DMVPN<br>o DES, 3DES, AES (128, 256)<br>o RSA, ECDSA<br>o MD5, SHA (256, 384, 512)<br>o 802.1X, RADIUS, AAA<br>o Firewall bazat pe zone de Securitate (ZBFW), PKI<br>- Echipamentul va avea capabilitatea sa exporte detalii despre toate fluxurile de date. In vederea atingerii acuratetei necesare in detectia posibilelor amenintari de securitate, este necesar si obligatoriu sa se asigure exportarea statisticilor cu includerea informatiilor despre fiecare pachet de date, fara restrictii cu privire la sursa sau destinatie, fara a se efectua esantionare. Trebuie sa se asigure capabilitati de exportare a statisticilor despre traficul tranzitat (cel putin: adresa IP sursa, adresa IP destinatie, port sursa, port destinatie, protocol TCP/UDP, TOS, interfața logica de intrare), aplicatii.<br>- Mecanisme pentru auditarea traficului criptat pentru identificarea versiunii de protocol TLS folosita.<br>- Mecanisme pentru detectia de malware in traficul criptat. |
| **Functionalitati monitorizare, troubleshooting si management** | - Echipamentul va fi configurabil folosind API-uri deschise, NETCONF, RESTCONF, YANG.<br>- Echipamentul trebuie sa permita intergrarea in solutii de tip SD-WAN (Software Defined WAN) fara sa fie necesare module hardware suplimentare. |
| **Conditii de mediu** | - Surse de alimentare la 230V AC. |

| | |
|---|---|
| | - Temperatura de lucru: 0 la 40°C<br>- Umiditate: 10 la 85%<br>- MTBF: minim 530.000 ore |
| **Licente si servicii suport** | - Se vor oferta toate licentele necesare pentru acoperirea functionalitatilor cerute si servicii de suport din partea vendorului pentru 3 ani |

### *4.4.7 Router WAN*

| | |
|---|---|
| **Descriere hardware** | - Echipament cu functii de rutare echipat cu minimum:<br>  o 12 interfete 10Gbps (SFP+)<br>- Memorie:<br>  o DRAM: 16 GB (sa permita up-grade pana la minim 32GB)<br>  o Flash: 32 GB<br>- Echipamentul trebuie sa fie montabil in rack-uri standard de 19” si sa includa accesoriile necesare montarii; maxim 1RU |
| **Performanta** | - Minimum:<br>  o 80 Gbps troughput IPSec<br>  o 115 Gbps trafic IPv4<br>  o 3800 tunele IPSec<br>  o 3.8 Milioane route IPv4<br>  o 3.8 Milioane route IPv6<br>  o 11,5 Milioane sesiuni NAT<br>  o 8000 instante virtuale de rutaj (VRF-uri)<br>- Echipamentul va oferi redundanta la nivel de sistem de operare<br>- Echipamentul trebuie sa suporte MACSEC pe toate porturile, la viteaza nominala a porturilor<br>- Echipamentul va asigura trafic criptat de minim 20Gbps, duplex |
| **Functionalitati retelistica** | - Sistemul de operare al echipamentului oferit va asigura urmatoarele standarde:<br>  o RIP, OSPF, EIGRP, BGP, IS-IS, DHCP, IGMPv3, PIM SM, PIM SSM, RSVP, L2TPv3, BFD, MPLS<br>  o GRE, PPP, PPPoE, MLPPP, HDLC<br>  o QoS, PBR, PfR, NBAR<br>  o VRF |

| | |
|---|---|
| | ○ IP SLA |
| **Functionalitati securitate** | - Sistemul de operare al echipamentului oferit va asigura urmatoarele functionalitati:<br>○ VPN Site-to-Site, DMVPN<br>○ DES, 3DES, AES (128, 256)<br>○ RSA, ECDSA<br>○ MD5, SHA (256, 384, 512)<br>○ 802.1X, RADIUS, AAA<br>○ Firewall bazat pe zone de Securitate (ZBFW), PKI<br>- Echipamentul va avea capabilitatea sa exporte detalii despre toate fluxurile de date. In vederea atingerii acuratetei necesare in detectia posibilelor amenintari de securitate, este necesar si obligatoriu sa se asigure exportarea statisticilor cu includerea informatiilor despre fiecare pachet de date, fara restrictii cu privire la sursa sau destinatie, fara a se efectua esantionare. Trebuie sa se asigure capabilitati de exportare a statisticilor despre traficul tranzitat (cel putin: adresa IP sursa, adresa IP destinatie, port sursa, port destinatie, protocol TCP/UDP, TOS, interfața logica de intrare), aplicatii.<br>- Mecanisme pentru auditarea traficului criptat pentru identificarea versiunii de protocol TLS folosita.<br>- Mecanisme pentru detectia de malware in traficul criptat. |
| **Functionalitati monitorizare, troubleshooting si management** | - Echipamentul va fi configurabil folosind API-uri deschise, NETCONF, RESTCONF, YANG.<br>- Echipamentul trebuie sa permita intergrarea in solutii de tip SD-WAN (Software Defined WAN) fara sa fie necesare module hardware suplimentare. |
| **Conditii de mediu** | - Surse de alimentare la 230V AC.<br>- Temperatura de lucru: 0 la 40°C<br>- Umiditate: 10 la 85%<br>- MTBF: minim 156.000 ore |
| **Licente si servicii suport** | - Se vor oferta toate licentele necesare pentru acoperirea functionalitatilor cerute si servicii de suport din partea vendorului pentru 3 ani |

### *4.4.8 DNS Firewall*

| | |
|---|---|
| Specificatii hardware | - 4 interfete GE SFP+<br>- 5 interfete GE RJ45<br>- 1 interfata Ethernet de management<br>- 1 port consola<br>- Tip stocare interna: SSD<br>- Memorie RAM: 8 GB ECC<br>- Rackabil: maxim 1U<br>- Capacitate sursa: 750W<br>- Sursa certificata 80 Plus Platinum pentru eficienta<br>- Echipamentul trebuie sa fie echipat cu surse de putere redundante<br>- Ventilatoare detasabile |
| Performante | - Trafic procesat la Layer 4: 20 Gbps<br>- Trafic procesat la Layer 7: 20 Gbps<br>- Capacitate SSL bruta: 8.5 Gbps<br>- Numar conexiuni pe secunda Layer 4: 500.000<br>- Numar conexiuni pe secunda Layer 7: 180.000<br>- Numar cereri pe secunda la Layer 4 (HTTP): 2.000.000<br>- Numarul de sesiuni concurente la Layer 4: 32.000.000<br>- Numar tranzactii SSL RSA pe secunda: 15.000<br>- Numar tranzactii SSL ECDSA pe secunda: 15.000<br>- Protectie DDoS impotriva “SYN Flood”, numar mesaje TCP SYN pe secunda: 4.000.000<br>- Numarul de instante virtuale pentru aplicatii, licentiate: 32<br>- Certificari: FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM, RoHS |
| Functionalitati disponibilitate aplicatii | - Solutia include suport pentru IPv4 si IPv6<br>- Solutia permite balansarea traficului la Layer 4 si Layer 7(Fast HTTP si Full HTTP Proxy)<br>- Solutia permite manipularea header/URL/domain la Layer 7 pe baza de sabloane<br>- Solutia ofera persistenta sesiunilor la Layer 7<br>- Solutia include suport pentru HTTP/2, FTP, DNS, FIX<br>- Solutia ofera balansare de tip: Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response |

| | |
|---|---|
| | - Solutia ofera posibilitatea de inspectia profunda a pachetelor<br>- Suport pentru monitorizarea starii de sanatate a aplicatiilor: ICMP, TCP, UDP, HTTP, HTTPS, FTP, RTSP, SMTP, POP3, SNMP, DNS, RADIUS, LDAP<br>- Suport pentru adaugarea de script-uri (TCL, Python, Perl, Bash) care sa verifice starea de sanatate a aplicatiilor<br>- Suport pentru disponibilitate ridicata(activ-activ si activ-pasiv)<br>- Suport pentru balansarea aplicatiilor de voce: SIP<br>- Suport pentru STARTTLS (pentru aplicatii de email si LDAP)<br>- Suport pentru filtrarea traficului de retea<br>- Solutia trebuie sa includa functionalitati de:<br>o Firewall Load Balancing;<br>o Global Server Load Balancing (GSLB);<br>o Suport pentru protocolul ICAP;<br>o Balansare a bazelor de date;<br>o Balansare a protocolului Diameter AAA ;<br>o Balansare de link-uri multiple (NHLD);<br>o Transparent Cache Switching (TCS);<br>o DNS Proxy;<br>o Balansarea protocolului RTSP;<br>- Solutia permite raspunsuri DNS bazate pe proximitatea utilizatorului care acceseaza aplicatia<br>- Suport pentru instante virtuale dedicate care sa aiba un set unic de politici si sa fie izolate complet de restul instantelor virtuale de pe echipament |
| Functionalitati generale | - Posibilitatea de a gestiona echipamentul dintr-o consola de management oferita de acelasi producator<br>- Posibilitatea de a comunica prin REST API cu alte platforme multi-vendor: Cisco ACI, OpenStack si VMware<br>- Posibilitatea de a adauga servicii suplimentare de Threat Intelligence, cum ar fi: DShield si Shadowserver<br>- Posibilitatea de a bloca atacurile cunoscute ca OWASP Top 10<br>- Posibilitatea de a schimba timpul TCP Half-Open<br>- Posibilitatea de a ajusta TCP Fast Open<br>- Posibilitatea de a marca DSCP traficul<br>- Posibilitatea de a face NAT 1 la 1(NAT 1:1) |

| | |
|---|---|
| | - Posibilitatea de a aplica urmatoarele optiuni HTTP SLB: HTTP/2, URL Hash Switching, URL / Host Switching, URL Failover, 5xx Retry and Reassignment, Non-HTTP Bypass, HTTP Packet Flow Modes, High-speed HTTP Content Replacement, Content Compression, Client IP Insertion / Replacement, Header Insertion / Erasure, URL Redirect Rewrite, Strict Transaction Switching, HTTP Status Code Statistics, Client-IP Insertion Extensive |
| Securizarea aplicatiei | - Solutia trebuie sa includa functionalitati de Web Application Firewall (WAF)<br>- Solutia trebuie sa includa functionalitati de DNS Application Firewall (DAF)<br>- Solutia trebuie sa includa in mod integrat functionalitati pentru protectia impotriva atacurilor DoS distribuite(DDoS)<br>- Solutia permite gestionarea accesului in aplicatii: — SAML, WIA,Kerberos,NTLM,TDS SQL Logon, LDAP,RADIUS, Basic,OCSP stapling, HTML Form-based<br>- Solutia include suport pentru audit bazat pe Radius<br>- Solutia trebuie sa se integreze cu Ansible, Terraform si Prometheus<br>- Solutia include suport SSL/TLS: TLS 1.2 si 1.3, Perfect Forward Secrecy (PFS), ECDHE si ECC<br>- Solutia include suport pentru AES-NI/GCM<br>- Solutia include suport pentru detectia unor anomali<br>- Solutia include suport pentru limitarea numarului de conexiuni<br>- Solutia include suport pentru limitarea ratei(Rate Limiting) pe adresa IP sursa<br>- Solutia include suport pentru liste dinamice (lista alba/lista negra)<br>- Solutia include suport pentru Simple Certificate Enrollment Protocol (SCEP)<br>- Posibilitatea de a descarca periodic liste dinamice pentru filtrare/analiza/blocare de la un threat intelligence oferit de acelasi producator<br>- Solutia include suport pentru prevenirea atacurilor de tip DNS cache-poisoning prin DNSSEC<br>- Solutia include suport pentru single sign-on(SAML, Kerberos) |

| | |
|---|---|
| | - Solutia include suport pentru validarea certificatelor de client intr-un server OCSP<br>- Solutia include suport pentru algoritmi bazati pe curba eliptica |
| Metode de accelerare a aplicatiei | - Solutia include suport pentru accelerarea si optimizarea aplicatiilor HTTP: Multiplexare TCP, stocarea temporara intr-o zona tampon a memoriei RAM(RAM Caching) si compresie HTTP<br>- Solutia include suport pentru descarcarea SSL: terminatie SSL, reutilizarea ID-ului de sesiune SSL si SSL Bridging<br>- Suport pentru optimizari TCP(Selective Acknowledgment, Client KeepAlive si Window Scaling)<br>- Suport pentru HTTP Pipelining<br>- Suport pentru HTTP/2, SPDY |
| Functionalitati retea | - Se poate integra la Layer 2 sau la Layer 3<br>- Solutia include suport pentru integrare in mod transparent sau rutat(mod gateway)<br>- Solutia include suport pentru rutare: Statica, IS-IS (v4/v6), RIPv2/ng, OSPF v2/v3, BGP4+<br>- Solutia include suport pentru VLAN-uri (802.1Q)<br>- Solutia include suport pentru agregarea de link-uri(802.1AX), LACP<br>- Solutia include suport pentru liste de control acces(ACL)<br>- Solutia include suport pentru NAT (IPv4 NAT/NAPT)<br>- Solutia include suport pentru NAT (IPv6 NAPT)<br>- Solutia include suport pentru Jumbo Frame<br>- Solutia include suport pentru VXLAN<br>- Solutia include suport pentru NVGRE |
| Functionalitati de administrare si monitorizare a sistemului | - Echipamentul trebuie sa poata fi administrat prin interfata grafica web si CLI<br>- Acces la interfata de management prin SSH si TELNET<br>- Acces securizat la interfata de management web<br>- Suport SNMP, syslog, alerte prin email, NetFlow v9 and v10 (IPFIX), sFlow<br>- REST API<br>- Suport LDAP, TACACS+, RADIUS<br>- Control configurabil al procesorului |

| | |
|---|---|
| | - Interoperabilitatea cu o solutie de management, configurare si analiza oferita de acelasi producator |
| Conditii de alimentare si mediu | - Putere necesara: 100 - 240 VAC, 50 - 60 Hz<br>- Temperatura de operare: 0 - 40 grade Celsius<br>- Umiditate: 5% - 95% fara condens |
| Licentiere, Support si Garantie | - Support producator de tip 24x7x365 ce va include:<br>o Update-uri pentru pentru indeplinirea functionalitatilor de Securitate: WAF, DAF, DDoS<br>o Support telefonic si web (ticketing)<br>o Update software<br>o Acces documentatie tehnica<br>o Garantie hardware cu schimb echipament defect in maxim 3 zile lucratoare |

### *4.4.9 Firewall tip 1*

| | |
|---|---|
| Descriere generala | Echipamentul integrat de protectie in retea trebuie sa detina capabilitati de rutare Layer3, precum si capabilitati avansate de securitate precum scanare antivirus, scanare antispam, control la nivel de aplicatie, prevenirea intruziunilor, filtrare WEB, destinate folosirii ca o solutie de securitate unificata ce dispune de redundanta si disponibilitate inalta.<br>Functionalitatile de baza trebuiesc accelerate folosind ASIC-uri specializate, iar echipamentul trebuie sa suporte configurarea atat in modul Transparent, cat si in modul NAT.<br>Datorita necesitatii protectiei investitiei si a suportului, este impedios necesar ca toate modulele de filtrare si tehnologiile aplicate (incluzand sistemul de operare) sa provina de la acelasi producator. Sistemul nu trebuie licentiat per numar de utilizatori (nu exista numar limitat de utilizatori). |
| Specificații hardware | Pentru a asigura acuratete si performanta, toate modulele de protectie ce alcatuiesc modulele de securitate trebuie sa functioneze avand la baza un sistem de operare dedicat, dezvoltat de catre producatorul echipamentului. Nu este permisa folosirea unui sistem de operare comercial, pentru uz general.<br>Caracteristici:<br>- Montabil in rack, maximum 3U rack unit<br>- 2 x interfete dedicate pentru management GE RJ-45 |

| | |
|---|---|
| | - 2 interfete 25 GE SFP28 /10 GE SFP+ pentru redundanta<br>- 16 interfete 25 GE SFP28 /10 GE SFP+<br>- 8 interfete 100 GE QSFP 28 / 40 GE QSFP+<br>- 1 x USB<br>- 1 x port consola RJ-45<br>- Sursa redundata de alimentare echipata<br>- 2 module de stocare interne instalate, fiecare cu o capacitate de minim 2 TB, de tipul Solid State Drive (SSD) |
| Performanta sistemului | - Firewall Throughput IPv4/IPv6 (packete UDP de 1518 bytes): 750 Gbps<br>- Firewall Throughput IPv4/IPv6 (packete UDP de 512 bytes): 735 Gbps<br>- Firewall Throughput IPv4/IPv6 (packete UDP de 64 bytes): 380 Gbps<br>- Firewall Throughput (pachete pe secunda) : 580 Mpps<br>- IPSec VPN Throughput (512 bytes): 200 Gbps<br>- IPS Throughput (Enterprise Mix): 50 Gbps<br>- NGFW Throughput: 45 Gbps<br>- Tunele IPSec VPN Gateway-Gateway concurente: 40.000<br>- Concurrent sessions (TCP): 200.000.000<br>- New Session/Sec: 950.000<br>- Firewall and security policies: 175.000<br>- Suport definire pana la 10 firewall-uri virtuale (tabele separate de rutare) fara licenta aditionala cu posibilitatea de a licentia ulterior pana la 500 firewall-uri virtuale<br>- Configuratii redundante posibile: Activ/Activ, Activ/Pasiv<br>- Unlimited Users Licences |
| Parametrii echipament | - Alimentare alternativa 100-240V, 50-60Hz |
| Protocoale si standarde | *Servicii de Retea*<br>Rutare/Retea:<br>- Suport WAN multiplu<br>- Suport PPPoE<br>- Client/Server DHCP<br>- Policy-based routing<br>- Rutare dinamica IPv4/IPv6- RIP, OSPF ,BGP, IS-IS, Multicast(IPv4)<br>- Suport multi-zone<br>- Rutare intre zone |

| | |
|---|---|
| | - VLAN Tagging(802.1q)<br>- Link aggregation (802.3ad)<br>- Rutare intre VLAN-uri<br>- Multi-link aggregation(802.3ad)<br>- Suport IPv6 (Firewall, AntiVirus, Web-Filtering, IPS, DNS, Transparent Mode, SIP, rutare dinamica, Admin access, Management)<br>Traffic shaping :<br>- Policy-based<br>- Suport DiffServ<br>- Banda Garantata/Maxima/Prioritara<br>- Shaping per- IP, per-Policy, per application<br>Domenii virtuale:<br>- Domenii Firewall/Rutare separate<br>- Posibilitatea de folosire mixta a domeniilor virtuale in modul Transparent/NAT<br>- Interfete VLAN separate<br>High Availability:<br>- Activ/Activ, Activ/Pasiv<br>- Statefull Failover<br>- Link status monitor<br>- Link failover<br>- Server Load balancing<br><br>*Servicii de securitate*<br>Firewall :<br>- NAT, PAT, Transparent<br>- Rutare dinamica-RIP, OSPF, BGP, Multicast, Policy-based NAT<br>- Domenii Virtuale (NAT/Transparent)<br>- VLAN Tagging (802.1q)<br>- SIP/H.323/SCCP NAT Traversal<br>- Suport session helpers (DCE-RPC, DNS, FTP, H.245, H.323, MGCP, ONC-RPC, PPTP, RSH, RTSP, SIP, TFTP, TNS)<br>- Profile granulare de protectie per-policy<br>- Suport proxy explicit |

| | |
|---|---|
| | - Suport pentru management centralizat a pana la 8192 access point-uri fizice<br>- Suport pentru autentificarea userilor la nivel de politici firewall :<br>o baza locala<br>o Windows AD<br>o External RADIUS/LDAP/TACACS+<br>o XAUTH over RADIUS (IPSEC)<br>o RSA Secure ID<br>o 2-factor authentication cu tokenuri hardware/software dedicate<br>VPN:<br>- PPTP, IPSec, SSL<br>- Suport criptare DES, 3DES, AES<br>- Autentificare SHA-l / MD5<br>- PPTP, L2TP, VPN Client pass through<br>- Suport VPN "Hub and Spoke"<br>- Autentificare IKE cu Certificate (x.509 v1 si v2)<br>- IPSec NAT Traversal<br>- Producatorul trebuie sa aiba in portofoliu client de VPN propriu, atat pentru PC-uri cat si pentru device-uri mobile<br>Prevenirea intruziunilor :<br>- Suport Anomalii de protocoale<br>- Suport Semnaturi definite de utilizator<br>- Suport Ipv6<br>Antivirus :<br>- Suport Antispyware<br>- Worm Prevention<br>- HTTP/HTTPS;POP/POP3S;SMTP/SMTPS;IMAP/IMAPS;FTP/FTPS;IM<br>- Blocarea fisierelor in functie de tip sau dimensiune<br>- Suport Ipv6<br>Antispam :<br>- Inspectie SMTP/SMTPS;IMAP/IMAPS;POP/POPS<br>Application control :<br>- Identificarea si controlul la nivel de aplicatie a peste 3000 de aplicatii (control Layer 7 indiferent de port/protocol)<br>- Traffic shaping (per aplicatie) |

| | |
|---|---|
| | - Diff Serv per aplicatie<br>- Suport inspectie trafic SSL<br>Suport Data Loss Prevention<br>- Identificarea si controlul datelor sensitive<br>- Suport actiuni configurabile (block/log/archive)<br>- Suport document fingerprinting<br>Filtrare WEB<br>- Blocarea accesului utilizatorilor la site-uri de tip malitios sau cu continut nepotrivit folosind o baza de date globala cu certificare recunoscuta.<br>- Posibilitatea definirii de liste statice cu URL-uri permise/blocate<br>- Posibilitatea de customizare a categoriilor globale prin suprascriere<br>Identificarea device-urilor:<br>- Colectarea informatiilor device-urilor conectate la retea precum adresa MAC, adresa IP, sistem de operare, hostname, username. |
| Management | Administrare:<br>- Consola, Telnet, SSH, HTTP/HTTPS, CLI<br>- Utilizatori/ Administratori cu drepturi configurabile<br>- Syslog, SNMP, log-uri interne, grafice, notificari email<br>- System software rollback<br>- Posibilitatea de management centralizat prin intermediul unui echipament dedicat<br>Autentificare :<br>- Baza de date locala<br>- Integrare Active Directory<br>- Integrare LDAP/RADIUS/Tacacs+<br>- IP/MAC address binding<br>- Suport 2-factor authentication |
| Software | - Licente pentru activarea actualizarilor serviciilor Antivirus, AntiBot, Antispam, Prevenirea Intruziunilor, Web Filtering, Content Disarm and Reconstruct, Cloud Sandbox |
| Certificate | - Acuratețea filtrării componentelor trebuie sa fie demonstrata de următoarele certificate:<br>- ICSA: Firewall, VPN - SSL/TLS, IPS, Antivirus, IPsec<br>- FCC Class A Part 15 |

| | |
|---|---|
| | - VCCI<br>- CB<br>- ISO 9001-2000 pentru producator |
| Service si garanție | Solutia va beneficia de suport ce va include:<br>- Inlocuirea echipamentului in caz de defectiune hardware<br>- Suport tehnic din partea vendorului 7 zile pe saptamana, 24 ore pe zi<br>- Update firmware versiuni minore si majore<br>Solutia va beneficia de update-uri automate de semnaturi de securitate pentru indeplinirea tuturor functionalitatilor cerute mai sus pe perioada de garantie si suport tehnic.<br>Dupa expirarea serviciilor achizitionate, echipamentul trebuie sa functioneze, sa permita atat administrarea cat si fluxurile de date, chiar daca semnaturile nu mai sunt actualizate la zi.<br>În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare. |

#### *4.4.10 Firewall tip 2*

| | |
|---|---|
| Descriere generala | Echipamentul integrat de protectie in retea trebuie sa detina capabilitati de rutare Layer3, precum si capabilitati avansate de securitate precum scanare antivirus, scanare antispam, control la nivel de aplicatie, prevenirea intruziunilor, filtrare WEB, destinate folosirii ca o solutie de securitate unificata ce dispune de redundanta si disponibilitate inalta.<br>Functionalitatile de baza trebuiesc accelerate folosind ASIC-uri specializate, iar echipamentul trebuie sa suporte configurarea atat in modul Transparent, cat si in modul NAT.<br>Datorita necesitatii protectiei investitiei si a suportului, este impedios necesar ca toate modulele de filtrare si tehnologiile aplicate (incluzand sistemul de operare) sa provina de la acelasi producator. Sistemul nu trebuie licentiat per numar de utilizatori (nu exista numar limitat de utilizatori). |
| Specificatii hardware | Pentru a asigura acuratete si performanta, toate modulele de protectie ce alcatuiesc modulele de securitate trebuie sa functioneze avand la baza un sistem de operare dedicat, dezvoltat de catre producatorul echipamentului. Nu este permisa folosirea unui sistem de operare comercial, pentru uz general. |

| | |
|---|---|
| | Caracteristici:<br>- Montabil in rack, maximum 3U rack unit<br>- 2 x interfete dedicate pentru management GE RJ-45<br>- 2 interfete 25 GE SFP28 /10 GE SFP+ pentru redundanta<br>- 16 interfete 25 GE SFP28 /10 GE SFP+<br>- 8 interfete 100 GE QSFP 28 / 40 GE QSFP+<br>- 1 x USB<br>- 1 x port consola RJ-45<br>- Sursa redundata de alimentare echipata<br>2 module de stocare interne instalate, fiecare cu o capacitate de minim 2 TB, de tipul Solid State Drive (SSD) |
| Performanta sistemului | - Firewall Throughput IPv4/IPv6 (packete UDP de 1518 bytes): 750 Gbps<br>- Firewall Throughput IPv4/IPv6 (packete UDP de 512 bytes): 735 Gbps<br>- Firewall Throughput IPv4/IPv6 (packete UDP de 64 bytes): 380 Gbps<br>- Firewall Throughput (pachete pe secunda) : 580 Mpps<br>- IPSec VPN Throughput (512 bytes): 200 Gbps<br>- IPS Throughput (Enterprise Mix): 50 Gbps<br>- NGFW Throughput: 45 Gbps<br>- Tunele IPSec VPN Gateway-Gateway concurente: 40.000<br>- Concurrent sessions (TCP): 200.000.000<br>- New Session/Sec: 950.000<br>- Firewall and security policies: 175.000<br>- Suport definire pana la 10 firewall-uri virtuale (tabele separate de rutare) fara licenta aditionala cu posibilitatea de a licentia ulterior pana la 500 firewall-uri virtuale<br>- Configuratii redundante posibile: Activ/Activ, Activ/Pasiv<br>- Unlimited Users Licences |
| Parametrii echipament | - Alimentare alternativa 100-240V, 50-60Hz |
| Protocoale si standarde | *Servicii de Retea*<br>Rutare/Retea:<br>- Suport WAN multiplu<br>- Suport PPPoE<br>- Client/Server DHCP<br>- Policy-based routing |

| | |
|---|---|
| | - Rutare dinamica IPv4/IPv6- RIP, OSPF ,BGP, IS-IS, Multicast(IPv4)<br>- Suport multi-zone<br>- Rutare intre zone<br>- VLAN Tagging(802.1q)<br>- Link aggregation (802.3ad)<br>- Rutare intre VLAN-uri<br>- Multi-link aggregation(802.3ad)<br>- Suport IPv6 (Firewall, AntiVirus, Web-Filtering, IPS, DNS, Transparent Mode, SIP, rutare dinamica, Admin access, Management)<br>Traffic shaping :<br>- Policy-based<br>- Suport DiffServ<br>- Banda Garantata/Maxima/Prioritara<br>- Shaping per- IP, per-Policy, per application<br>Domenii virtuale:<br>- Domenii Firewall/Rutare separate<br>- Posibilitatea de folosire mixta a domeniilor virtuale in modul Transparent/NAT<br>- Interfete VLAN separate<br>High Availability:<br>- Activ/Activ, Activ/Pasiv<br>- Statefull Failover<br>- Link status monitor<br>- Link failover<br>- Server Load balancing<br><br>*Servicii de securitate*<br>Firewall :<br>- NAT, PAT, Transparent<br>- Rutare dinamica-RIP, OSPF, BGP, Multicast, Policy-based NAT<br>- Domenii Virtuale (NAT/Transparent)<br>- VLAN Tagging (802.1q)<br>- SIP/H.323/SCCP NAT Traversal |

| | |
|---|---|
| | - Suport session helpers (DCE-RPC, DNS, FTP, H.245, H.323, MGCP, ONC-RPC, PPTP, RSH, RTSP, SIP, TFTP, TNS)<br>- Profile granulare de protectie per-policy<br>- Suport proxy explicit<br>- Suport pentru management centralizat a pana la 8192 access point-uri fizice<br>- Suport pentru autentificarea userilor la nivel de politici firewall :<br>o baza locala<br>o Windows AD<br>o External RADIUS/LDAP/TACACS+<br>o XAUTH over RADIUS (IPSEC)<br>o RSA Secure ID<br>o 2-factor authentication cu tokenuri hardware/software dedicate<br>VPN:<br>- PPTP, IPSec, SSL<br>- Suport criptare DES, 3DES, AES<br>- Autentificare SHA-l / MD5<br>- PPTP, L2TP, VPN Client pass through<br>- Suport VPN "Hub and Spoke"<br>- Autentificare IKE cu Certificate (x.509 v1 si v2)<br>- IPSec NAT Traversal<br>- Producatorul trebuie sa aiba in portofoliu client de VPN propriu, atat pentru PC-uri cat si pentru device-uri mobile<br>Prevenirea intruziunilor :<br>- Suport Anomalii de protocoale<br>- Suport Semnaturi definite de utilizator<br>- Suport Ipv6<br>Antivirus :<br>- Suport Antispyware<br>- Worm Prevention<br>- HTTP/HTTPS;POP/POP3S;SMTP/SMTPS;IMAP/IMAPS;FTP/FTPS;IM<br>- Blocarea fisierelor in functie de tip sau dimensiune<br>- Suport Ipv6<br>Antispam :<br>- Inspectie SMTP/SMTPS;IMAP/IMAPS;POP/POPS |

| | |
|---|---|
| | Application control :<br>- Identificarea si controlul la nivel de aplicatie a peste 3000 de aplicatii (control Layer 7 indiferent de port/protocol)<br>- Traffic shaping (per aplicatie)<br>- Diff Serv per aplicatie<br>- Suport inspectie trafic SSL<br>Suport Data Loss Prevention<br>- Identificarea si controlul datelor sensitive<br>- Suport actiuni configurabile (block/log/archive)<br>- Suport document fingerprinting<br>Filtrare WEB<br>- Blocarea accesului utilizatorilor la site-uri de tip malitios sau cu continut nepotrivit folosind o baza de date globala cu certificare recunoscuta.<br>- Posibilitatea definirii de liste statice cu URL-uri permise/blocate<br>- Posibilitatea de customizare a categoriilor globale prin suprascriere<br>Identificarea device-urilor:<br>- Colectarea informatiilor device-urilor conectate la retea precum adresa MAC, adresa IP, sistem de operare, hostname, username. |
| Management | Administrare:<br>- Consola, Telnet, SSH, HTTP/HTTPS, CLI<br>- Utilizatori/ Administratori cu drepturi configurabile<br>- Syslog, SNMP, log-uri interne, grafice, notificari email<br>- System software rollback<br>- Posibilitatea de management centralizat prin intermediul unui echipament dedicat<br>Autentificare :<br>- Baza de date locala<br>- Integrare Active Directory<br>- Integrare LDAP/RADIUS/Tacacs+<br>- IP/MAC address binding<br>- Suport 2-factor authentication |
| Software | - Licente pentru activarea actualizarilor serviciilor Antivirus, AntiBot, Antispam, Prevenirea Intruziunilor, Web Filtering, Content Disarm and Reconstruct, Cloud Sandbox |

| | |
|---|---|
| Certificate | - Acuratetea filtrarii componentelor trebuie sa fie demonstrata de urmatoarele certificate:<br>- ICSA: Firewall, VPN - SSL/TLS, IPS, Antivirus, IPsec<br>- FCC Class A Part 15<br>- VCCI<br>- CB<br>- ISO 9001-2000 pentru producator |
| Service si garantie | Solutia va beneficia de suport ce va include:<br>- Inlocuirea echipamentului in caz de defectiune hardware<br>- Suport tehnic din partea vendorului 7 zile pe saptamana, 24 ore pe zi<br>- Update firmware versiuni minore si majore<br>Solutia va beneficia de update-uri automate de semnaturi de securitate pentru indeplinirea tuturor functionalitatilor cerute mai sus pe perioada de garantie si suport tehnic.<br>Dupa expirarea serviciilor achizitionate, echipamentul trebuie sa functioneze, sa permita atat administrarea cat si fluxurile de date, chiar daca semnaturile nu mai sunt actualizate la zi.<br>În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare. |

### *4.4.11 Firewall tip 3*

| | |
|---|---|
| Descriere generala | Echipamentul integrat de protectie in retea trebuie sa detina capabilitati de rutare Layer3, precum si capabilitati avansate de securitate precum scanare antivirus, scanare antispam, control la nivel de aplicatie, prevenirea intruziunilor, filtrare WEB, destinate folosirii ca o solutie de securitate unificata ce dispune de redundanta si disponibilitate inalta.<br>Functionalitatile de baza trebuiesc accelerate folosind ASIC-uri specializate, iar echipamentul trebuie sa suporte configurarea atat in modul Transparent, cat si in modul NAT.<br>Datorita necesitatii protectiei investitiei si a suportului, este impedios necesar ca toate modulele de filtrare si tehnologiile aplicate (incluzand sistemul de operare) sa provina de la acelasi producator. Sistemul nu trebuie licentiat per numar de utilizatori (nu exista numar limitat de utilizatori). |

| | |
|---|---|
| Specificatii hardware | Pentru a asigura acuratete si performanta, toate modulele de protectie ce alcatuiesc modulele de securitate trebuie sa functioneze avand la baza un sistem de operare dedicat, dezvoltat de catre producatorul echipamentului. Nu este permisa folosirea unui sistem de operare comercial, pentru uz general.<br>Caracteristici:<br>- 2 x interfete dedicate pentru management GE RJ-45<br>- 2 interfete 10 GE SFP+ / GE SFP pentru redundanta<br>- 16 interfete 10 GE / GE RJ45<br>- 16 interfete 25 GE SFP 28 / 10 GE SFP+ / GE SFP<br>- 4 interfete 100 GE QSFP 28 / 40 GE QSFP+<br>- 1 x USB<br>- 1 x port consola RJ-45<br>- Sursa redundata de alimentare echipata de tipul hot swappable<br>- 2 module de stocare interne instalate, fiecare cu o capacitate de minim 1 TB, de tipul Solid State Drive (SSD) |
| Performanta sistemului | - Firewall Throughput IPv4/IPv6 (packete UDP de 1518 bytes): 195 Gbps<br>- Firewall Throughput IPv4/IPv6 (packete UDP de 512 bytes): 190 Gbps<br>- Firewall Throughput IPv4/IPv6 (packete UDP de 64 bytes): 115 Gbps<br>- Firewall Throughput (pachete pe secunda) : 175 Mpps<br>- IPSec VPN Throughput (512 bytes): 52 Gbps<br>- IPS Throughput (Enterprise Mix): 22 Gbps<br>- NGFW Throughput: 18 Gbps<br>- Tunele IPSec VPN Gateway-Gateway concurente: 20.000<br>- Concurrent sessions (TCP): 23.000.000<br>- New Session/Sec: 950.000<br>- Firewall and security policies: 95.000<br>- Suport definire pana la 10 firewall-uri virtuale (tabele separate de rutare) fara licenta aditionala cu posibilitatea de a licentia ulterior pana la 500 firewall-uri virtuale<br>- Configuratii redundante posibile: Activ/Activ, Activ/Pasiv<br>- Unlimited Users Licences |
| Parametrii echipament | - Alimentare alternativa 100-240V |
| Protocoale si standarde | *Servicii de Retea* |

| | |
|---|---|
| | Rutare/Retea:<br>- Suport WAN multiplu<br>- Suport PPPoE<br>- Client/Server DHCP<br>- Policy-based routing<br>- Rutare dinamica IPv4/IPv6- RIP, OSPF ,BGP, IS-IS, Multicast(IPv4)<br>- Suport multi-zone<br>- Rutare intre zone<br>- VLAN Tagging(802.1q)<br>- Link aggregation (802.3ad)<br>- Rutare intre VLAN-uri<br>- Multi-link aggregation(802.3ad)<br>- Suport IPv6 (Firewall, AntiVirus, Web-Filtering, IPS, DNS, Transparent Mode, SIP, rutare dinamica, Admin access, Management)<br>Traffic shaping :<br>- Policy-based<br>- Suport DiffServ<br>- Banda Garantata/Maxima/Prioritara<br>- Shaping per- IP, per-Policy, per application<br>Domenii virtuale:<br>- Domenii Firewall/Rutare separate<br>- Posibilitatea de folosire mixta a domeniilor virtuale in modul Transparent/NAT<br>- Interfete VLAN separate<br>High Availability:<br>- Activ/Activ, Activ/Pasiv<br>- Statefull Failover<br>- Link status monitor<br>- Link failover<br>- Server Load balancing<br><br>*Servicii de securitate*<br>Firewall:<br>- NAT, PAT, Transparent |

| | |
|---|---|
| | - Rutare dinamica-RIP, OSPF, BGP, Multicast, Policy-based NAT<br>- Domenii Virtuale (NAT/Transparent)<br>- VLAN Tagging (802.1q)<br>- SIP/H.323/SCCP NAT Traversal<br>- Suport session helpers (DCE-RPC, DNS, FTP, H.245, H.323, MGCP, ONC-RPC, PPTP, RSH, RTSP, SIP, TFTP, TNS)<br>- Profile granulare de protectie per-policy<br>- Suport proxy explicit<br>- Suport pentru management centralizat a pana la 4096 access point-uri fizice<br>- Suport pentru autentificarea userilor la nivel de politici firewall :<br>o baza locala<br>o Windows AD<br>o External RADIUS/LDAP/TACACS+<br>o XAUTH over RADIUS (IPSEC)<br>o RSA Secure ID<br>o 2-factor authentication cu tokenuri hardware/software dedicate<br>VPN:<br>- PPTP, IPSec, SSL<br>- Suport criptare DES, 3DES, AES<br>- Autentificare SHA-l I MD5<br>- PPTP, L2TP, VPN Client pass through<br>- Suport VPN "Hub and Spoke"<br>- Autentificare IKE cu Certificate (x.509 v1 si v2)<br>- IPSec NAT Traversal<br>- Producatorul trebuie sa aiba in portofoliu client de VPN propriu, atat pentru PC-uri cat si pentru device-uri mobile<br>Prevenirea intruziunilor :<br>- Suport Anomalii de protocoale<br>- Suport Semnaturi definite de utilizator<br>- Suport Ipv6<br>Antivirus :<br>- Suport Antispyware<br>- Worm Prevention |

| | |
|---|---|
| | - HTTP/HTTPS;POP/POP3S;SMTP/SMTPS;IMAP/IMAPS;FTP/FTPS;IM<br>- Blocarea fisierelor in functie de tip sau dimensiune<br>- Suport Ipv6<br>Antispam :<br>- Inspectie SMTP/SMTPS;IMAP/IMAPS;POP/POPS<br>Application control :<br>- Identificarea si controlul la nivel de aplicatie a peste 3000 de aplicatii (control Layer 7 indiferent de port/protocol)<br>- Traffic shaping (per aplicatie)<br>- Diff Serv per aplicatie<br>- Suport inspectie trafic SSL<br>Suport Data Loss Prevention<br>- Identificarea si controlul datelor sensitive<br>- Suport actiuni configurabile (block/log/archive)<br>- Suport document fingerprinting<br>Filtrare WEB<br>- Blocarea accesului utilizatorilor la site-uri de tip malitios sau cu continut nepotrivit folosind o baza de date globala cu certificare recunoscuta.<br>- Posibilitatea definirii de liste statice cu URL-uri permise/blocate<br>- Posibilitatea de customizare a categoriilor globale prin suprascriere<br>Identificarea device-urilor:<br>- Colectarea informatiilor device-urilor conectate la retea precum adresa MAC, adresa IP, sistem de operare, hostname, username. |
| Management | Administrare:<br>- Consola, Telnet, SSH, HTTP/HTTPS, CLI<br>- Utilizatori/ Administratori cu drepturi configurabile<br>- Syslog, SNMP, log-uri interne, grafice, notificari email<br>- System software rollback<br>- Posibilitatea de management centralizat prin intermediul unui echipament dedicat<br>Autentificare :<br>- Baza de date locala<br>- Integrare Active Directory<br>- Integrare LDAP/RADIUS/Tacacs+ |

| | |
|---|---|
| | - IP/MAC address binding<br>- Suport 2-factor authentication |
| Software | - Licente pentru activarea actualizarilor serviciilor Antivirus, AntiBot, Antispam, Prevenirea Intruziunilor, Web Filtering, Content Disarm and Reconstruct, Cloud Sandbox |
| Certificate | - Acuratetea filtrarii componentelor trebuie sa fie demonstrata de urmatoarele certificate:<br>- ICSA: Firewall, VPN - SSL, IPS, Antivirus, IPsec<br>- FCC Class A Part 15<br>- VCCI<br>- CB<br>- ISO 9001-2000 pentru producator |
| Service si garantie | Solutia va beneficia de suport ce va include:<br>- Inlocuirea echipamentului in caz de defectiune hardware<br>- Suport tehnic din partea vendorului 7 zile pe saptamana, 24 ore pe zi<br>- Update firmware versiuni minore si majore<br>Solutia va beneficia de update-uri automate de semnaturi de securitate pentru indeplinirea tuturor functionalitatilor cerute mai sus pe perioada de garantie si suport tehnic.<br>Dupa expirarea serviciilor achizitionate, echipamentul trebuie sa functioneze, sa permita atat administrarea cat si fluxurile de date, chiar daca semnaturile nu mai sunt actualizate la zi.<br>În cazul defectării mediilor de stocare ale echipamentului garanția va implica înlocuirea acestora fără trimiterea lor la producător. În cazul în care este necesară depanarea de către producător, sistemul va fi trimis fără mediile de stocare. |

### *4.4.12 Switch LAN tip 1*

| | |
|---|---|
| Cerinte tehnice generale | - Echipamentul va avea caracteristicile unui switch destinat mediului de centru de date, care sa asigure simultan urmatoarele functionalitati:<br>  ○ Switch Ethernet Layer 2;<br>  ○ Switch Ethernet Layer 3;<br>- Interfete fizice disponibile:<br>  ○ Minim 28 40G/100G Ethernet (cu conector QSFP28) care sa suporte urmatoarele tipuri de transceivere: |

| | |
|---|---|
| | ▪ 40GBASE-SR4<br>▪ 40GBASE-LR4<br>▪ 10GBASE-SR<br>▪ 10GBASE-LR<br>▪ 100GBASE-SR4<br>▪ 100GBASE-LR4<br>○ Minim 8 100/400G Ethernet (cu conector SFP+) care sa suporte urmatoarele tipuri de transceivere:<br>▪ 100GBASE-SR4<br>▪ 100GBASE-LR4<br>▪ 400GBASE-DR4<br>▪ 400GBASE-FR4<br>▪ 400GBASE-LR8<br>- Arhitectura de tip „non-blocking”, capabila sa asigure comunicatii fara pierderi de frame-uri intre oricare doua porturi, la viteza maxima de 100Gbps si 400Gbps, cu o intarziere minima, atat la Layer 2 cat si la Layer 3;<br>- Sasiu instalabil in rack de 19”;<br>- Inaltime maxima 2RU, per switch;<br>- Kit de rack-are inclus. |
| Porturi instalate (per switch) | - 2 cabluri optice de tip 100G QSFP-QSFP cu lungime minima de 10 metri<br>- Minim 1 interfata 100Base-TX/1000Base-T pentru management „out of band”;<br>- Minim 1 port consola seriala;<br>- Minim 1 port USB; |
| Performante (per switch) | - Comutarea la nivel 2: minim 12 Tbps si minim 4000 Mpps;<br>- Tabela de adrese MAC de minim 250000 de inregistrari;<br>- Minim 3900 de ID-uri pentru VLAN-uri per switch;<br>- Procesor de control multi-core. |
| Functionalitati minimale de nivel 2 instalate | - Incapsulare IEEE 802.1Q;<br>- Rapid Per-VLAN Spanning Tree Plus sau echivalent;<br>- Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instante;<br>- Spanning Tree PortFast, Root Guard si Bridge Assurance; |

| | |
|---|---|
| | - Virtual Port Channel sau o tehnologie echivalenta care sa permita crearea unui “link-aggregation group” intre doua switch-uri pe de o parte si un alt echipament de tip client (server, switch, router, etc) de partea cealalta<br>- Link Aggregation Control Protocol (LACP): IEEE 802.3ad;<br>- Posibilitatea balansarii legaturilor din Port Chanel utilizand informatii de nivel 2, 3 si 4;<br>- Suport pentru “Jumbo frames” cu dimensiuni de 9216 bytes pe toate porturile;<br>- Mecanisme de control al inundarii retelei cu trafic unicast, multicast si broadcast;<br>- Private VLAN, inclusiv pe porturile de tip trunk 802.1Q;<br>- Suport pentru protocolul LLDP (IEEE 802.3ab)<br>- protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1Q-in-Q; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames;<br>- Support pentru protocolul VXLAN si cel putin 500 Virtual Tunnel End-Points (VTEP). |
| Functionalitati minimale de nivel 3 instalate | - Suport pentru urmatoarele protocoale Layer 3:<br>o Open Shortest Path First (OSPF) versiunile 2 si 3;<br>o Border Gateway Protocol (BGP);<br>o RIP v2<br>o Multicast PIM SM, SSM si MSDP<br>- Cel putin 800000 intrari in tabela de routare<br>- Posibilitatea de a filtra accesul pe interfete dupa informatii despre adresa IP sursa sau destinatie si in acelasi timp si portul TCP/UDP sursa sau destinatie<br>- DHCP snooping cu posibilitatea de a adauga Optiunea 82<br>- Facilitatea de a filtra pe un port/VLAN a raspunsurilor la cererile protocolului ARP<br>- VXLAN Routing line-rate pe toate porturile<br>- Suport pentru extinderea BGP-EVPN VXLAN in mai multe site-uri, sau o alta tehnologie de tip Fabric bazata pe VXLAN cu capabilitate multi-site echivalenta<br>- cel putin 1000 instante VRF |

| | |
|---|---|
| Functionalitati minimale de QoS | - Layer 2 IEEE 802.1p (CoS);<br>- Configurare QoS per port;<br>- Minim 4 cozi hardware de servire per port;<br>- Posibilitatea de clasificare a traficului bazata pe liste de control al accesului;<br>- Coada cu prioritate stricta. |
| Functionalitati de inalta disponibilitate | - Surse de alimentare, ventilatoare si module de expansiune de tip “hot-swappable”;<br>- Surse de alimentare redundante tip “1:1”;<br>- Ventilatoare redundante tip “N:1”. |
| Functionalitati de management | - Suport pentru SPAN si Encapsulated Routed SPAN<br>- Suport pentru netflow/sflow sau echivalent<br>- Suport pentru revenirea la o configuratie anterioara<br>- Suport pentru standardul AAA, Tacacs+ si Radius<br>- Suport pentru interfata XML (Netconf)<br>- Suport pentru monitorizarea utilizarii bufferelor interne<br>- Suport pentru protocolul SSHv2 si SCP |
| Parametri de alimentare (per switch) | - 2 (doua) surse AC integrate, configurabile in mod redundant ce pot fi inlocuite in timpul functionarii echipamentului, cu certificare 80 Plus Platinum;<br>- Tensiunea de functionare: 100-240 VAC;<br>- Frecventa de functionare: 50-60 Hz. |
| Mediu de functionare | - Temperatura de functionare: de la 0° la 40° C;<br>- Umiditate: de la 5 la 95%; |

### *4.4.13 Switch LAN tip 2*

| | |
|---|---|
| Cerințe tehnice generale | - Echipamentul va avea caracteristicile unui switch destinat mediului de centru de date, care sa asigure simultan urmatoarele functionalitati:<br>  ○ Switch Ethernet Layer 2;<br>  ○ Switch Ethernet Layer 3;<br>- Interfete fizice disponibile:<br>  ○ Minim 6 40G/100G Ethernet (cu conector QSFP28) care sa suporte urmatoarele tipuri de transceivere: |

| | |
|---|---|
| | ▪ 40GBASE-SR4<br>▪ 40GBASE-LR4<br>▪ 10GBASE-SR<br>▪ 10GBASE-LR<br>▪ 10GBASE-ER<br>▪ 100GBASE-SR4<br>▪ 100GBASE-LR4<br>o Minim 48 1G/10G/25G Ethernet (cu conector SFP+) care sa suporte urmatoarele tipuri de transceivere:<br>▪ 10GBASE-SR<br>▪ 10GBASE-LR<br>▪ 10GBASE-ER<br>▪ 25GBASE-SR<br>▪ 1000Base-T<br>- Suport pentru 25G FC-FEC (CL74) si RS-FEC (CL91)<br>- Arhitectura de tip „non-blocking”, capabila sa asigure comunicatii fara pierderi de frame-uri intre oricare doua porturi, la viteza maxima de 10/25Gbps, 40Gbps si 100Gbps, cu o intarziere minima, atat la Layer 2 cat si la Layer 3;<br>- Șasiu instalabil in rack de 19”;<br>- Înălțime maxima 1RU, per switch;<br>- Kit de rack-are inclus. |
| Conectica instalata (per switch) | - Patru (4) porturi de tip 100G Ethernet echipate cu cabluri optice active de tip QSFP-QSFP si lungime de cel putin 10 metri;<br>- Patruzeci (40) porturi de tip 10/25G Ethernet echipate cu transceivere optice de tip SFP28 pentru fibra optica multi-mode cu conector LC;<br>- Minim 1 interfata 100Base-TX/1000Base-T pentru management „out of band”;<br>- Minim 1 port consola seriala;<br>- Minim 1 port USB; |
| Performante (per switch) | - Comutarea la nivel 2: minim 3.5 Tbps si minim 1.2 Bpps;<br>- Tabela de adrese MAC de minim 288000 de inregistrari;<br>- Minim 3900 de ID-uri pentru VLAN-uri per switch;<br>- Procesor de control multi-core. |
| Functionalitati minimale de | - Incapsulare IEEE 802.1Q; |

| | |
|---|---|
| nivel 2 instalate | - Rapid Per-VLAN Spanning Tree Plus sau echivalent;<br>- Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instante;<br>- Spanning Tree PortFast, Root Guard si Bridge Assurance sau echivalent;<br>- MC-LAG/Virtual Port Channel sau o tehnologie echivalenta care sa permita crearea unui “link-aggregation group” intre doua switch-uri pe de o parte si un alt echipament de tip client (server, switch, router, etc) de partea cealalta;<br>- Link Aggregation Control Protocol (LACP): IEEE 802.3ad;<br>- Posibilitatea balansarii legaturilor din Port Chanel utilizand informatii de nivel 2, 3 si 4;<br>- Suport pentru “Jumbo frames” cu dimensiuni de 9216 bytes pe toate porturile;<br>- Mecanisme de control al inundarii retelei cu trafic unicast, multicast si broadcast;<br>- Private VLAN, inclusiv pe porturile de tip trunk 802.1Q;<br>- LLDP (IEEE 802.3ab)<br>- protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1Q-in-Q, IEEE 802.3an; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames;<br>- support pentru protocolul VXLAN si cel putin 500 Virtual Tunnel End-Points (VTEP).<br>- VXLAN Routing line-rate pe toate porturile<br>- Suport pentru extinderea BGP-EVPN VXLAN in mai multe site-uri, sau o alta tehnologie de tip Fabric bazata pe VXLAN cu capabilitate multi-site echivalenta<br>- Sa se poata activa prin instalarea unei licente suplimentare criptarea in hardware a interfetelor de viteza 10/24/40/100Gbps folosind tehnologia MacSec AES-256 |
| Functionalitati minimale de nivel 3 instalate | - Suport pentru urmatoarele protocoale Layer 3:<br>- Open Shortest Path First (OSPF) versiunile 2 si 3;<br>- Border Gateway Protocol (BGP);<br>- RIP v2<br>- Multicast PIM SM, SSM si MSDP<br>- Cel putin 350000 intrari in tabela de routare |

| | |
|---|---|
| | - Posibilitatea de a filtra accesul pe interfete dupa informatii despre adresa IP sursa sau destinatie si in acelasi timp si portul TCP/UDP sursa sau destinatie<br>- DHCP snooping cu posibilitatea de a adauga Optiunea 82<br>- Facilitatea de a filtra pe un port/VLAN a raspunsurilor la cererile protocolului ARP<br>- VXLAN Routing line-rate pe toate porturile<br>- cel putin 1000 instante VRF |
| Functionalitati minimale de QoS | - Layer 2 IEEE 802.1p (CoS);<br>- Configurare QoS per port;<br>- Minim 8 cozi hardware de servire per port;<br>- Clasificarea traficului bazata pe liste de control al accesului;<br>- Weighted Round-Robin (WRR) sau echivalent. |
| Functionalitati de inalta disponibilitate | - Surse de alimentare, ventilatoare si module de expansiune de tip “hot-swappable”;<br>- Surse de alimentare redundante tip “1:1”;<br>- Ventilatoare redundante tip “N:1”. |
| Functionalitati de management | - Suport pentru SPAN si Encapsulated Routed SPAN<br>- Suport pentru netflow/sflow sau echivalent<br>- Suport pentru revenirea la o configuratie anterioara<br>- Suport pentru standardul AAA, Tacacs+ si Radius<br>- Suport pentru interfata XML (Netconf)<br>- Suport pentru monitorizarea utilizarii bufferelor interne<br>- Suport pentru protocolul SSHv2 si SCP |
| Parametri de alimentare (per switch) | - 2 (doua) surse AC integrate, configurabile in mod redundant ce pot fi inlocuite in timpul functionarii echipamentului, cu certificare 80 Plus Platinum;<br>- Tensiunea de functionare: 100-240 VAC;<br>- Frecventa de functionare: 50-60 Hz. |
| Mediu de functionare | - Temperatura de functionare: de la 0° la 40° C;<br>- Umiditate: de la 5 la 90%;<br>- Fluxul de aer: dinspre surse/ventilatoare catre porturi. |
| Garantie si suport tehnic | - Suport hardware cu SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, 24 ore timp de remediere), pe o perioadă |

| | |
|---|---|
| | de 3 (trei) ani, care să garanteze diagnosticarea echipamentului/modulului defect şi înlocuirea acestuia, fără costuri suplimentare pentru beneficiar;<br>- Suport software pe o perioadă de 3 (trei) ani, acoperind dreptul de a face update-uri software la sistemul de operare al switch-ului ori de câte ori este necesar;<br>- Se vor preciza part-number-ul (-ele) care asigura conditiile de garantie hardware si suport software mai sus mentionate. |

#### *4.4.14 Switch LAN tip 3*

| | |
|---|---|
| Cerinte tehnice generale | - Echipamentul va avea caracteristicile unui switch destinat mediului de centru de date, care sa asigure simultan urmatoarele functionalitati:<br>  ○ Switch Ethernet Layer 2;<br>  ○ Switch Ethernet Layer 3;<br>- Interfete fizice disponibile:<br>  ○ Electrice: minim 48 100Mbps/1 Gigabit Ethernet (cu conector RJ45)<br>  ○ Optice: minim 4 1/10/25G Ethernet si 2 40G/100G Ethernet (cu conector QSFP28) care sa suporte urmatoarele tipuri de transceivere:<br>  ▪ 40GBASE-SR4<br>  ▪ 40GBASE-LR4<br>  ▪ 10GBASE-SR<br>  ▪ 10GBASE-LR<br>  ▪ 10GBASE-ER<br>  ▪ 25GBASE-SR<br>  ▪ 100GBASE-SR4<br>  ▪ 100GBASE-LR4<br>- Arhitectura de tip „non-blocking”, capabila sa asigure comunicatii fara pierderi de frame-uri intre oricare doua porturi, la viteza maxima de 1 Gbps, 10Gbps, 40Gbps si 100Gbps, cu o intarziere minima, atat la Layer 2 cat si la Layer 3;<br>- Sasiu instalabil in rack de 19”;<br>- Inaltime maxima 1RU, per switch;<br>- Kit de rack-are inclus. |
| Conectica instalata (per switch) | - Doua (2) porturi de tip 25G ethernet echipate cu cabluri pasive de tip SFP-SFP si lungime de cel putin 5 metri; |

| | |
|---|---|
| | - Un (1) porturi de tip 40G Ethernet echipate cu cablu pasiv de tip QSFP-QSFP si lungime de cel putin 3 metri;<br>- Minim 1 interfata 100Base-TX/1000Base-T pentru management „out of band";<br>- Minim 1 port consola seriala;<br>- Minim 1 port USB; |
| Performante (per switch) | - Comutarea la nivel 2: minim 0.6 Tbps si minim 0.5 Mpps;<br>- Tabela de adrese MAC de minim 92000 de inregistrari;<br>- Minim 3900 de ID-uri pentru VLAN-uri per switch;<br>- Procesor de control multi-core. |
| Functionalitati minimale de nivel 2 instalate | - Incapsulare IEEE 802.1Q;<br>- Rapid Per-VLAN Spanning Tree Plus sau echivalent;<br>- Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instante;<br>- Spanning Tree PortFast, Root Guard si Bridge Assurance sau echivalent;<br>- MC-LAG/Virtual Port Channel sau o tehnologie echivalenta care sa permita crearea unui "link-aggregation group" intre doua switch-uri pe de o parte si un alt echipament de tip client (server, switch, router, etc) de partea cealalta;<br>- Link Aggregation Control Protocol (LACP): IEEE 802.3ad;<br>- Posibilitatea balansarii legaturilor din Port Chanel utilizand informatii de nivel 2, 3 si 4;<br>- Suport pentru "Jumbo frames" cu dimensiuni de 9216 bytes pe toate porturile;<br>- Mecanisme de control al inundarii retelei cu trafic unicast, multicast si broadcast;<br>- Private VLAN, inclusiv pe porturile de tip trunk 802.1Q;<br>- LLDP (IEEE 802.3ab)<br>- protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1ad, IEEE 802.1ba, IEEE 802.3an; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames; |
| Functionalitati minimale de nivel 3 instalate | - Suport pentru urmatoarele protocoale in configuratia ofertata:<br>  ○ Rute statice;<br>  ○ VRRP sau echivalent;<br>  ○ RIP v2 |

| | |
|---|---|
| | - Suport pentru urmatoarele protocoale (prin adaugarea unei licente suplimentare):<br>  ○ Open Shortest Path First (OSPF) versiunile 2 si 3;<br>  ○ Border Gateway Protocol (BGP);<br>  ○ Multicast PIM SM, SSM si MSDP;<br>  ○ cel putin 1000 instante VRF;<br>- Cel putin 16000 intrari in tabela de routare;<br>- Posibilitatea de a filtra accesul pe interfete dupa informatii despre adresa IP sursa sau destinatie si in acelasi timp si portul TCP/UDP sursa sau destinatie;<br>- DHCP snooping cu posibilitatea de a adauga Optiunea 82;<br>- Facilitatea de a filtra pe un port/VLAN a raspunsurilor la cererile protocolului ARP; |
| Functionalitati minimale de QoS | - Layer 2 IEEE 802.1p (CoS);<br>- Configurare QoS per port;<br>- Minim 4 cozi hardware de servire per port;<br>- Clasificarea traficului bazata pe liste de control al accesului;<br>- Weighted Round-Robin (WRR) sau echivalent. |
| Functionalitati de inalta disponibilitate | - Surse de alimentare, ventilatoare si module de expansiune de tip “hot-swappable”;<br>- Surse de alimentare redundante tip “1:1”;<br>- Ventilatoare redundante tip “N:1”. |
| Functionalitati de management | - SPAN/Traffic mirroring si Encapsulated Routed SPAN<br>- Posibilitatea de a reveni la o configuratie anterioara<br>- AAA, Tacacs+ si Radius<br>- interfata de configurare de tip XML (Netconf)<br>- SSHv2 si SCP |
| Parametri de alimentare (per switch) | - 2 (doua) surse AC integrate, configurabile in mod redundant ce pot fi inlocuite in timpul functionarii echipamentului, cu certificare 80 Plus Platinum;<br>- Tensiunea de functionare: 100-240 VAC;<br>- Frecventa de functionare: 50-60 Hz. |
| Mediu de functionare | - Temperatura de functionare: de la 0° la 40° C;<br>- Umiditate: de la 5 la 90%; |

| | |
|---|---|
| | - Fluxul de aer: dinspre surse/ventilatoare catre porturi (porturile inspre spatele rack-ului). |
| Garantie si suport tehnic | - Suport hardware cu SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, 24 ore timp de remediere), pe o perioadă de 3 (trei) ani, care să garanteze diagnosticarea echipamentului/modulului defect şi înlocuirea acestuia, fără costuri suplimentare pentru beneficiar;<br>- Suport software pe o perioadă de 3 (trei) ani, acoperind dreptul de a face update –uri software la sistemul de operare al switch-ului ori de câte ori este necesar;<br>- Se vor preciza part-number-ul (–ele) care asigura conditiile de garantie hardware si suport software mai sus mentionate. |

### *4.4.15 Switch SAN tip 1*

| | |
|---|---|
| Numar porturi | - Switch Fibre Channel cu minim 48 porturi active, cu posibilitate de activare pana la minim 96 prin instalarea unei licente suplimentare |
| Tip interfete | - Fiber channel, minim 96 porturi de 8/16/32 Gbps, banda dedicata pentru fiecare port: minim 32 Gbps |
| Performanta | - capacitate de comutare: minim 3 Tbps<br>- pana la 16 porturi in configuratie PortChannel cu balansare automata<br>- buffer-credits de cel putin 8300 per grup de 16 porturi<br>- posibilitatea de a avea minim 8270 buffer-credits pentru un singur port dintr-un grup de 6 porturi prin instalarea unei licente suplimentare |
| Securitate | - Inspectie inteligenta a pachetelor la nivel de port<br>- Impartire in zone la nivel hardware prin intermediul listelor de acces<br>- Suport pentru Secure FTP, SSHv2, SNMPv3 cu implementare de AES<br>- Logical-unit-number (LUN) zoning si read-only zones<br>- Extended broadcast zoning<br>- Autentificare FC-SP switch-to-switch<br>- Autentificare FC-SP host-to-switch<br>- Mecanisme de verificare a autenticității sistemului propriu de operare instalat |

| | |
|---|---|
| Capabilitati functionale instalate pe switch | - Suport pentru N_Port ID Virtualization<br>- Support pentru fabric-port (F-port) trunking si channeling<br>- Posibilitatea agregarii a minim 16 legaturi, cu balansarea traficului peste aceste legaturi<br>- Facilitate de integrare cu aplicatii de management prin intermediul API-urilor<br>- Sursa de putere redundanta, hot-swappable si fan tray hot-swappable<br>- module SFP+ hot-swappable<br>- diagnosticare online<br>- interfata programática de tip REST |
| Utilitare pentru diagnosticare si troubleshooting | - POST diagnostics<br>- Online diagnostics<br>- Internal loopbacks<br>- SPAN (remote SPAN<br>- Fibre Channel traceroute<br>- Fibre Channel ping<br>- Fibre Channel debug<br>- Syslog<br>- Port-level statistics<br>- Fabric-Analyzer |
| Management | - Porturi Out-of-band 10/100/1000 Ethernet, EIA/TIA-232 serial console<br>- In-band management folosind IP over Fibre Channel<br>- Acces comand line interface<br>- Acces pe baza de autentificare cu server RADIUS, TACACS+ sau echivalent<br>- Roluri pe baza de VSAN<br>- Suport pentru upgrade software in service |
| Standarde suportate | - Protocoale Fibre Channel:<br>○ FC-PH, Revision 4.3 (ANSI INCITS 230-1994)<br>○ FC-PH, Amendment 1 (ANSI INCITS 230-1994/AM1-1996)<br>○ FC-PH, Amendment 2 (ANSI INCITS 230-1994/AM2-1999)<br>○ FC-PH-2, Revision 7.4 (ANSI INCITS 297-1997) |

| | |
|---|---|
| | ○ FC-PH-3, Revision 9.4 (ANSI INCITS 303-1998)<br>○ FC-PI, Revision 13 (ANSI INCITS 352-2002)<br>○ FC-PI-2, Revision 10 (ANSI INCITS 404-2006)<br>○ FC-PI-3, Revision 4 (ANSI INCITS 460-2011)<br>○ FC-PI-4, Revision 8 (ANSI INCITS 450-2008)<br>○ FC-PI-5, Revision 6 (ANSI INCITS 479-2011)<br>○ FC-PI-6 (ANSI INCITS 512-2015)<br>○ FC-FS, Revision 1.9 (ANSI INCITS 373-2003)<br>○ FC-FS-2, Revision 1.01 (ANSI INCITS 424-2007)<br>○ FC-FS-2, Amendment 1 (ANSI INCITS 424-2007/AM1-2007)<br>○ FC-FS-3, Revision 1.11 (ANSI INCITS 470-2011)<br>○ FC-FS-4<br>○ FC-LS, Revision 1.62 (ANSI INCITS 433-2007)<br>○ FC-LS-2, Revision 2.21 (ANSI INCITS 477-2011)<br>○ FC-LS-3, Includes revision 3.53<br>○ FC-SW-2, Revision 5.3 (ANSI INCITS 355-2001)<br>○ FC-SW-3, Revision 6.6 (ANSI INCITS 384-2004)<br>○ FC-SW-4, Revision 7.5 (ANSI INCITS 418-2006)<br>○ FC-SW-5, Revision 8.5 (ANSI INCITS 461-2010)<br>○ FC-SW-6<br>○ FC-GS-3, Revision 7.01 (ANSI INCITS 348-2001)<br>○ FC-GS-4, Revision 7.91 (ANSI INCITS 387-2004)<br>○ FC-GS-5, Revision 8.51 (ANSI INCITS 427-2007)<br>○ FC-GS-6, Revision 9.4 (ANSI INCITS 463-2010)<br>○ FC-GS-7, Includes revision 10.8<br>○ FCP, Revision 12 (ANSI INCITS 269-1996)<br>○ FCP-2, Revision 8 (ANSI INCITS 350-2003)<br>○ FCP-3, Revision 4 (ANSI INCITS 416-2006)<br>○ FCP-4, Revision 2b (ANSI INCITS 481-2011)<br>○ FC-SB-2, Revision 2.1 (ANSI INCITS 349-2001)<br>○ FC-SB-3, Revision 1.6 (ANSI INCITS 374-2003)<br>○ FC-SB-3, Amendment 1 (ANSI INCITS 374-2003/AM1-2007)<br>○ FC-SB-4, Revision 3.0 (ANSI INCITS 466-2011)<br>○ FC-SB-5, Revision 2.00 (ANSI INCITS 485-2014)<br>○ FC-BB-6, Revision 2.00 (ANSI INCITS 509-2014)<br>○ FC-BB-2, Revision 6.0 (ANSI INCITS 372-2003)<br>○ FC-BB-3, Revision 6.8 (ANSI INCITS 414-2006) |

| | |
|---|---|
| | ○ FC-BB-4, Revision 2.7 (ANSI INCITS 419-2008)<br>○ FC-BB-5, Revision 2.0 (ANSI INCITS 462-2010)<br>○ FC-VI, Revision 1.84 (ANSI INCITS 357-2002)<br>○ FC-SP, Revision 1.8 (ANSI INCITS 426-2007)<br>○ FC-SP-2, Revision 2.71 (ANSI INCITS 496-2012)<br>○ FAIS, Revision 1.03 (ANSI INCITS 432-2007)<br>○ FAIS-2, Revision 2.23 (ANSI INCITS 449-2008)<br>○ FC-IFR, Revision 1.06 (ANSI INCITS 475-2011)<br>○ FC-FLA, Revision 2.7 (INCITS TR-20-1998)<br>○ FC-PLDA, Revision 2.1 (INCITS TR-19-1998)<br>○ FC-Tape, Revision 1.17 (INCITS TR-24-1999)<br>○ FC-MI, Revision 1.92 (INCITS TR-30-2002)<br>○ FC-MI-2, Revision 2.6 (INCITS TR-39-2005)<br>○ FC-MI-3, Revision 1.03 (INCITS TR-48-2012)<br>○ FC-DA, Revision 3.1 (INCITS TR-36-2004)<br>○ FC-DA-2, Revision 1.06 (INCITS TR-49-2012)<br>○ FC-MSQS, Revision 3.2 (INCITS TR-46-2011)<br>○ Clase de servicii Fibre Channel: Class 2, Class 3 si Class F<br>○ Tipuri de porturi Fibre Channel standard: E, F si B<br>○ Tipuri de porturi Fibre Channel extins: SD, ST si TE<br>○ FC-NVMe<br>○ Management In-band folosind protocolul IP over Fibre Channel (RFC 2625) |
| Dotari si functionalitati incluse | - Se vor include transceivere FC 32 Gbps short-reach pentru porturile active<br>- Se vor include licentele necesare pentru functionalitatile:<br>○ Inter-VSAN Routing<br>○ QoS<br>○ QoS zone-based<br>○ Traffic encryption |
| Mediu de functionare | - Temperatura de functionare: de la 0° la 40° C;<br>- Umiditate: de la 10 la 95%; |
| Parametri de alimentare (per switch) | - 2 (doua) surse AC integrate, ce pot fi inlocuite in timpul functionarii echipamentului;<br>- Tensiunea de functionare: 100-240 VAC;<br>- Frecventa de functionare: 50-60 Hz. |

| | |
|---|---|
| Garantie si suport tehnic | - Suport hardware cu SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, 24 ore timp de remediere), pe o perioadă de 3 (trei) ani, care să garanteze diagnosticarea echipamentului/modulului defect şi înlocuirea acestuia, fără costuri suplimentare pentru beneficiar;<br>- Suport software pe o perioadă de 3 (trei) ani, acoperind dreptul de a face update –uri software la sistemul de operare al switch-ului ori de câte ori este necesar;<br>- Se vor preciza part-number-ul (–ele) care asigura conditiile de garantie hardware si suport software mai sus mentionate. |

#### *4.4.16 Switch SAN tip 2*

| | |
|---|---|
| Numar porturi | - Switch Fibre Channel cu minim 24 porturi active, cu posibilitate de activare pana la minim 48 prin instalarea unei licente suplimentare |
| Tip interfete | - Fiber channel, minim 48 porturi de 8/16/32 Gbps, banda dedicata pentru fiecare port: minim 32 Gbps |
| Performanta | - capacitate de comutare: minim 1.5 Tbps<br>- pana la 16 porturi in configuratie PortChannel cu balansare automata<br>- buffer-credits de cel putin 8000 per grup de 16 porturi<br>- posibilitatea de a avea minim 8000 buffer-credits pentru un singur port dintr-un grup de 16 porturi prin instalarea unei licente suplimentare |
| Securitate | - Inspectie inteligenta a pachetelor la nivel de port<br>- Impartire in zone la nivel hardware prin intermediul listelor de acces<br>- Suport pentru Secure FTP, SSHv2, SNMPv3 cu implementare de AES<br>- Logical-unit-number (LUN) zoning si read-only zones<br>- Extended broadcast zoning<br>- Autentificare FC-SP switch-to-switch<br>- Autentificare FC-SP host-to-switch<br>- Mecanisme de verificare a autenticității sistemului propriu de operare instalat |
| Capabilitati functionale instalate pe switch | - Suport pentru N_Port ID Virtualization<br>- Support pentru fabric-port (F-port) trunking si channeling<br>- Posibilitatea agregarii a minim 16 legaturi, cu balansarea traficului peste aceste legaturi |

| | |
|---|---|
| | - Facilitate de integrare cu aplicatii de management prin intermediul API-urilor<br>- Sursa de putere redundanta, hot-swappable si fan tray hot-swappable<br>- module SFP+ hot-swappable<br>- diagnosticare online<br>- interfata programática de tip REST |
| Utilitare pentru diagnosticare si troubleshooting | - POST diagnostics<br>- Online diagnostics<br>- Internal loopbacks<br>- SPAN (remote SPAN<br>- Fibre Channel traceroute<br>- Fibre Channel ping<br>- Fibre Channel debug<br>- Syslog<br>- Port-level statistics<br>- Fabric-Analyzer |
| Management | - Porturi Out-of-band 10/100/1000 Ethernet, EIA/TIA-232 serial console<br>- In-band management folosind IP over Fibre Channel<br>- Acces comand line interface<br>- Acces pe baza de autentificare cu server RADIUS, TACACS+ sau echivalent<br>- Roluri pe baza de VSAN<br>- Suport pentru upgrade software in service |
| Standarde suportate | - Protocoale Fibre Channel:<br>o FC-PH, Revision 4.3 (ANSI INCITS 230-1994)<br>o FC-PH, Amendment 1 (ANSI INCITS 230-1994/AM1-1996)<br>o FC-PH, Amendment 2 (ANSI INCITS 230-1994/AM2-1999)<br>o FC-PH-2, Revision 7.4 (ANSI INCITS 297-1997)<br>o FC-PH-3, Revision 9.4 (ANSI INCITS 303-1998)<br>o FC-PI, Revision 13 (ANSI INCITS 352-2002)<br>o FC-PI-2, Revision 10 (ANSI INCITS 404-2006)<br>o FC-PI-3, Revision 4 (ANSI INCITS 460-2011)<br>o FC-PI-4, Revision 8 (ANSI INCITS 450-2008)<br>o FC-PI-5, Revision 6 (ANSI INCITS 479-2011) |

| | |
|---|---|
| | ○ FC-PI-6 (ANSI INCITS 512-2015)<br>○ FC-FS, Revision 1.9 (ANSI INCITS 373-2003)<br>○ FC-FS-2, Revision 1.01 (ANSI INCITS 424-2007)<br>○ FC-FS-2, Amendment 1 (ANSI INCITS 424-2007/AM1-2007)<br>○ FC-FS-3, Revision 1.11 (ANSI INCITS 470-2011)<br>○ FC-FS-4<br>○ FC-LS, Revision 1.62 (ANSI INCITS 433-2007)<br>○ FC-LS-2, Revision 2.21 (ANSI INCITS 477-2011)<br>○ FC-LS-3, Includes revision 3.53<br>○ FC-SW-2, Revision 5.3 (ANSI INCITS 355-2001)<br>○ FC-SW-3, Revision 6.6 (ANSI INCITS 384-2004)<br>○ FC-SW-4, Revision 7.5 (ANSI INCITS 418-2006)<br>○ FC-SW-5, Revision 8.5 (ANSI INCITS 461-2010)<br>○ FC-SW-6<br>○ FC-GS-3, Revision 7.01 (ANSI INCITS 348-2001)<br>○ FC-GS-4, Revision 7.91 (ANSI INCITS 387-2004)<br>○ FC-GS-5, Revision 8.51 (ANSI INCITS 427-2007)<br>○ FC-GS-6, Revision 9.4 (ANSI INCITS 463-2010)<br>○ FC-GS-7, Includes revision 10.8<br>○ FCP, Revision 12 (ANSI INCITS 269-1996)<br>○ FCP-2, Revision 8 (ANSI INCITS 350-2003)<br>○ FCP-3, Revision 4 (ANSI INCITS 416-2006)<br>○ FCP-4, Revision 2b (ANSI INCITS 481-2011)<br>○ FC-SB-2, Revision 2.1 (ANSI INCITS 349-2001)<br>○ FC-SB-3, Revision 1.6 (ANSI INCITS 374-2003)<br>○ FC-SB-3, Amendment 1 (ANSI INCITS 374-2003/AM1-2007)<br>○ FC-SB-4, Revision 3.0 (ANSI INCITS 466-2011)<br>○ FC-SB-5, Revision 2.00 (ANSI INCITS 485-2014)<br>○ FC-BB-6, Revision 2.00 (ANSI INCITS 509-2014)<br>○ FC-BB-2, Revision 6.0 (ANSI INCITS 372-2003)<br>○ FC-BB-3, Revision 6.8 (ANSI INCITS 414-2006)<br>○ FC-BB-4, Revision 2.7 (ANSI INCITS 419-2008)<br>○ FC-BB-5, Revision 2.0 (ANSI INCITS 462-2010)<br>○ FC-VI, Revision 1.84 (ANSI INCITS 357-2002)<br>○ FC-SP, Revision 1.8 (ANSI INCITS 426-2007)<br>○ FC-SP-2, Revision 2.71 (ANSI INCITS 496-2012)<br>○ FAIS, Revision 1.03 (ANSI INCITS 432-2007) |

| | |
|---|---|
| | ○ FAIS-2, Revision 2.23 (ANSI INCITS 449-2008)<br>○ FC-IFR, Revision 1.06 (ANSI INCITS 475-2011)<br>○ FC-FLA, Revision 2.7 (INCITS TR-20-1998)<br>○ FC-PLDA, Revision 2.1 (INCITS TR-19-1998)<br>○ FC-Tape, Revision 1.17 (INCITS TR-24-1999)<br>○ FC-MI, Revision 1.92 (INCITS TR-30-2002)<br>○ FC-MI-2, Revision 2.6 (INCITS TR-39-2005)<br>○ FC-MI-3, Revision 1.03 (INCITS TR-48-2012)<br>○ FC-DA, Revision 3.1 (INCITS TR-36-2004)<br>○ FC-DA-2, Revision 1.06 (INCITS TR-49-2012)<br>○ FC-MSQS, Revision 3.2 (INCITS TR-46-2011)<br>○ Clase de servicii Fibre Channel: Class 2, Class 3 si Class F<br>○ Tipuri de porturi Fibre Channel standard: E, F si B<br>○ Tipuri de porturi Fibre Channel extins: SD, ST si TE<br>○ FC-NVMe<br>○ Management In-band folosind protocolul IP over Fibre Channel (RFC 2625) |
| Dotari si functionalitati incluse | - Se vor include transceivere FC 32 Gbps short-reach pentru porturile active<br>- Se vor include licentele necesare pentru functionalitatile:<br>○ Inter-VSAN Routing<br>○ QoS<br>○ QoS zone-based<br>○ Traffic encryption |
| Mediu de functionare | - Temperatura de functionare: de la 0° la 40° C;<br>- Umiditate: de la 10 la 95%; |
| Parametri de alimentare (per switch) | - 2 (doua) surse AC integrate, ce pot fi inlocuite in timpul functionarii echipamentului;<br>- Tensiunea de functionare: 100-240 VAC;<br>- Frecventa de functionare: 50-60 Hz. |
| Garantie si suport tehnic | - Suport hardware cu SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, 24 ore timp de remediere), pe o perioadă de 3 (trei) ani, care să garanteze diagnosticarea echipamentului/modulului defect şi înlocuirea acestuia, fără costuri suplimentare pentru beneficiar; |

| | |
|---|---|
| | - Suport software pe o perioadă de 3 (trei) ani, acoperind dreptul de a face update –uri software la sistemul de operare al switch-ului ori de câte ori este necesar;<br>- Se vor preciza part-number-ul (–ele) care asigura condițiile de garanție hardware si suport software mai sus menționate. |

### *4.4.17 ADC / WAF*

| | |
|---|---|
| Specificatii hardware | - 48 interfete 1/10 GE SFP+<br>- 4 interfete 40 GE QSFP+<br>- 1 interfata Ethernet de management<br>- 1 port consola RJ-45<br>- Tip stocare interna: SSD<br>- Memorie RAM: 128 GB<br>- Rackabil: maxim 1U<br>- Sursa certificata 80 Plus Platinum pentru eficienta<br>- Echipamentul trebuie sa fie echipat cu surse de putere redundante<br>- Ventilatoare swappable |
| Performante | - Trafic procesat la Layer 4: 220 Gbps<br>- Trafic procesat la Layer 7: 200 Gbps<br>- Capacitate SSL bruta: 70 Gbps<br>- Numar conexiuni pe secunda Layer 4: 8.000.000<br>- Numar conexiuni pe secunda Layer 7: 2.500.000<br>- Numarul de sesiuni concurente la Layer 4: 256.000.000<br>- Numar tranzactii SSL RSA pe secunda: 195.000<br>- Numar tranzactii SSL ECDSA pe secunda: 70.000<br>- Protectie DDoS impotriva “SYN Flood”, numar mesaje TCP SYN pe secunda: 330.000.000<br>- Numarul de instante virtuale pentru aplicatii, licentiate: 1000<br>- Certificari: FCC Class A, UL, CE, CB, VCCI, CCC, KCC, BSMI, RoHS |
| Functionalitati disponibilitate aplicatii | - Solutia include suport pentru IPv4 si IPv6<br>- Solutia permite balansarea traficului la Layer 4 si Layer 7(Fast HTTP si Full HTTP Proxy)<br>- Solutia permite manipularea header/URL/domain la Layer 7 pe baza de sabloane |

| | |
|---|---|
| | - Solutia ofera persistenta sesiunilor la Layer 7<br>- Solutia include suport pentru HTTP/2, FTP, DNS, FIX<br>- Solutia ofera balansare de tip: Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response<br>- Solutia ofera posibilitatea de inspectia profunda a pachetelor<br>- Suport pentru monitorizarea starii de sanatate a aplicatiilor: ICMP, TCP, UDP, HTTP, HTTPS, FTP, RTSP, SMTP, POP3, SNMP, DNS, RADIUS, LDAP<br>- Suport pentru adaugarea de script-uri (TCL, Python, Perl, Bash) care sa verifice starea de sanatate a aplicatiilor<br>- Suport pentru disponibilitate ridicata(activ-activ si activ-pasiv)<br>- Suport pentru balansarea aplicatiilor de voce: SIP<br>- Suport pentru STARTTLS (pentru aplicatii de email si LDAP)<br>- Suport pentru filtrarea traficului de retea<br>- Solutia trebuie sa includa functionalitati de:<br>  ○ Firewall Load Balancing;<br>  ○ Global Server Load Balancing (GSLB);<br>  ○ Suport pentru protocolul ICAP;<br>  ○ Balansare a bazelor de date;<br>  ○ Balansare a protocolului Diameter AAA ;<br>  ○ Balansare de link-uri multiple (NHLD);<br>  ○ Transparent Cache Switching (TCS);<br>  ○ DNS Proxy;<br>  ○ Balansarea protocolului RTSP;<br>- Solutia permite raspunsuri DNS bazate pe proximitatea utilizatorului care acceseaza aplicatia<br>- Suport pentru instante virtuale dedicate care sa aiba un set unic de politici si sa fie izolate complet de restul instantelor virtuale de pe echipament |
| Functionalitati generale | - Posibilitatea de a gestiona echipamentul dintr-o consola de management oferita de acelasi producator<br>- Posibilitatea de a comunica prin REST API cu alte platforme multi-vendor: Cisco ACI, OpenStack si VMware<br>- Posibilitatea de a adauga servicii suplimentare de Threat Intelligence, cum ar fi: DShield si Shadowserver<br>- Posibilitatea de a bloca atacurile cunoscute ca OWASP Top 10 |

| | |
|---|---|
| | - Posibilitatea de a schimba timpul TCP Half-Open<br>- Posibilitatea de a ajusta TCP Fast Open<br>- Posibilitatea de a marca DSCP traficul<br>- Posibilitatea de a face NAT 1 la 1(NAT 1:1)<br>- Posibilitatea de a aplica urmatoarele optiuni HTTP SLB: HTTP/2, URL Hash Switching, URL / Host Switching, URL Failover, 5xx Retry and Reassignment, Non-HTTP Bypass, HTTP Packet Flow Modes, High-speed HTTP Content Replacement, Content Compression, Client IP Insertion / Replacement, Header Insertion / Erasure, URL Redirect Rewrite, Strict Transaction Switching, HTTP Status Code Statistics, Client-IP Insertion Extensive |
| Securizarea aplicatiei | - Solutia trebuie sa includa functionalitati de Web Application Firewall (WAF)<br>- Solutia trebuie sa includa functionalitati de DNS Application Firewall (DAF)<br>- Solutia trebuie sa includa in mod integrat functionalitati pentru protectia impotriva atacurilor DoS distribuite(DDoS)<br>- Solutia permite gestionarea accesului in aplicatii: — SAML, WIA,Kerberos,NTLM,TDS SQL Logon, LDAP,RADIUS, Basic,OCSP stapling, HTML Form-based<br>- Solutia include suport pentru audit bazat pe Radius<br>- Solutia trebuie sa se integreze cu Ansible, Terraform si Prometheus<br>- Solutia include suport SSL/TLS: TLS 1.2 si 1.3, Perfect Forward Secrecy (PFS), ECDHE si ECC<br>- Solutia include suport pentru AES-NI/GCM<br>- Solutia include suport pentru detectia unor anomali<br>- Solutia include suport pentru limitarea numarului de conexiuni<br>- Solutia include suport pentru limitarea ratei(Rate Limiting) pe adresa IP sursa<br>- Solutia include suport pentru liste dinamice (lista alba/lista negra)<br>- Solutia include suport pentru Simple Certificate Enrollment Protocol (SCEP)<br>- Posibilitatea de a descarca periodic liste dinamice pentru filtrare/analiza/blocare de la un threat intelligence oferit de acelasi producator |

| | |
|---|---|
| | - Solutia include suport pentru prevenirea atacurilor de tip DNS cache-poisoning prin DNSSEC<br>- Solutia include suport pentru single sign-on(SAML, Kerberos)<br>- Solutia include suport pentru validarea certificatelor de client intr-un server OCSP<br>- Solutia include suport pentru algoritmi bazati pe curba eliptica |
| Metode de accelerare a aplicatiei | - Solutia include suport pentru accelerarea si optimizarea aplicatiilor HTTP: Multiplexare TCP, stocarea temporara intr-o zona tampon a memoriei RAM(RAM Caching) si compresie HTTP<br>- Solutia include suport pentru descarcarea SSL: terminatie SSL, reutilizarea ID-ului de sesiune SSL si SSL Bridging<br>- Suport pentru optimizari TCP(Selective Acknowledgment, Client KeepAlive si Window Scaling)<br>- Suport pentru HTTP Pipelining<br>- Suport pentru HTTP/2, SPDY |
| Functionalitati retea | - Se poate integra la Layer 2 sau la Layer 3<br>- Solutia include suport pentru integrare in mod transparent sau rutat(mod gateway)<br>- Solutia include suport pentru rutare: Statica, IS-IS (v4/v6), RIPv2/ng, OSPF v2/v3, BGP4+<br>- Solutia include suport pentru VLAN-uri (802.1Q)<br>- Solutia include suport pentru agregarea de link-uri(802.1AX), LACP<br>- Solutia include suport pentru liste de control acces(ACL)<br>- Solutia include suport pentru NAT (IPv4 NAT/NAPT)<br>- Solutia include suport pentru NAT (IPv6 NAPT)<br>- Solutia include suport pentru Jumbo Frame<br>- Solutia include suport pentru VXLAN<br>- Solutia include suport pentru NVGRE |
| Functionalitati de administrare si monitorizare a sistemului | - Echipamentul trebuie sa poata fi administrat prin interfata grafica web si CLI<br>- Acces la interfata de management prin SSH si TELNET<br>- Acces securizat la interfata de management web<br>- Suport SNMP, syslog, alerte prin email, NetFlow v9 and v10 (IPFIX), sFlow |

| | |
|---|---|
| | - REST API<br>- Suport LDAP, TACACS+, RADIUS<br>- Control configurabil al procesorului<br>- Interoperabilitatea cu o solutie de management, configurare si analiza oferita de acelasi producator |
| Conditii de alimentare si mediu | - Putere necesara: 100 - 240 VAC, 50 - 60 Hz<br>- Temperatura de operare: 0 - 40 grade Celsius<br>- Umiditate: 5% - 95% fara condens |
| Licentiere, Support si Garantie | - Support producator de tip 24x7x365 ce va include:<br>o Update-uri pentru pentru indeplinirea functionalitatilor de Securitate: WAF, DAF, DDoS<br>o Support telefonic si web (ticketing)<br>o Update software<br>o Acces documentatie tehnica<br>o Garantie hardware cu schimb echipament defect in maxim 3 zile lucratoare |

#### *4.4.18 Load Balancer*

| | |
|---|---|
| Specificatii hardware | - 4 interfete GE SFP+<br>- 5 interfete GE RJ45<br>- 1 interfata Ethernet de management<br>- 1 port consola<br>- Tip stocare interna: SSD<br>- Memorie RAM: 8 GB ECC<br>- Rackabil: maxim 1U<br>- Capacitate sursa: 750W<br>- Sursa certificata 80 Plus Platinum pentru eficienta<br>- Echipamentul trebuie sa fie echipat cu surse de putere redundante<br>- Ventilatoare detasabile |
| Performante | - Trafic procesat la Layer 4: 20 Gbps<br>- Trafic procesat la Layer 7: 20 Gbps<br>- Capacitate SSL bruta: 8.5 Gbps<br>- Numar conexiuni pe secunda Layer 4: 500.000<br>- Numar conexiuni pe secunda Layer 7: 180.000 |

| | |
|---|---|
| | - Numar cereri pe secunda la Layer 4 (HTTP): 2.000.000<br>- Numarul de sesiuni concurente la Layer 4: 32.000.000<br>- Numar tranzactii SSL RSA pe secunda: 15.000<br>- Numar tranzactii SSL ECDSA pe secunda: 15.000<br>- Protectie DDoS impotriva “SYN Flood”, numar mesaje TCP SYN pe secunda: 4.000.000<br>- Numarul de instante virtuale pentru aplicatii, licentiate: 32<br>- Certificari: FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM, RoHS |
| Functionalitati disponibilitate aplicatii | - Solutia include suport pentru IPv4 si IPv6<br>- Solutia permite balansarea traficului la Layer 4 si Layer 7(Fast HTTP si Full HTTP Proxy)<br>- Solutia permite manipularea header/URL/domain la Layer 7 pe baza de sabloane<br>- Solutia ofera persistenta sesiunilor la Layer 7<br>- Solutia include suport pentru HTTP/2, FTP, DNS, FIX<br>- Solutia ofera balansare de tip: Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response<br>- Solutia ofera posibilitatea de inspectia profunda a pachetelor<br>- Suport pentru monitorizarea starii de sanatate a aplicatiilor: ICMP, TCP, UDP, HTTP, HTTPS, FTP, RTSP, SMTP, POP3, SNMP, DNS, RADIUS, LDAP<br>- Suport pentru adaugarea de script-uri (TCL, Python, Perl, Bash) care sa verifice starea de sanatate a aplicatiilor<br>- Suport pentru disponibilitate ridicata(activ-activ si activ-pasiv)<br>- Suport pentru balansarea aplicatiilor de voce: SIP<br>- Suport pentru STARTTLS (pentru aplicatii de email si LDAP)<br>- Suport pentru filtrarea traficului de retea<br>- Solutia trebuie sa includa functionalitati de:<br>  ○ Firewall Load Balancing;<br>  ○ Global Server Load Balancing (GSLB);<br>  ○ Suport pentru protocolul ICAP;<br>  ○ Balansare a bazelor de date;<br>  ○ Balansare a protocolului Diameter AAA ;<br>  ○ Balansare de link-uri multiple (NHLD);<br>  ○ Transparent Cache Switching (TCS);<br>  ○ DNS Proxy; |

| | |
|---|---|
| | ○ Balansarea protocolului RTSP;<br>- Solutia permite raspunsuri DNS bazate pe proximitatea utilizatorului care acceseaza aplicatia<br>- Suport pentru instante virtuale dedicate care sa aiba un set unic de politici si sa fie izolate complet de restul instantelor virtuale de pe echipament |
| Functionalitati generale | - Posibilitatea de a gestiona echipamentul dintr-o consola de management oferita de acelasi producator<br>- Posibilitatea de a comunica prin REST API cu alte platforme multi-vendor: Cisco ACI, OpenStack si VMware<br>- Posibilitatea de a adauga servicii suplimentare de Threat Intelligence, cum ar fi: DShield si Shadowserver<br>- Posibilitatea de a bloca atacurile cunoscute ca OWASP Top 10<br>- Posibilitatea de a schimba timpul TCP Half-Open<br>- Posibilitatea de a ajusta TCP Fast Open<br>- Posibilitatea de a marca DSCP traficul<br>- Posibilitatea de a face NAT 1 la 1(NAT 1:1)<br>- Posibilitatea de a aplica urmatoarele optiuni HTTP SLB: HTTP/2, URL Hash Switching, URL / Host Switching, URL Failover, 5xx Retry and Reassignment, Non-HTTP Bypass, HTTP Packet Flow Modes, High-speed HTTP Content Replacement, Content Compression, Client IP Insertion / Replacement, Header Insertion / Erasure, URL Redirect Rewrite, Strict Transaction Switching, HTTP Status Code Statistics, Client-IP Insertion Extensive |
| Securizarea aplicatiei | - Solutia trebuie sa includa functionalitati de Web Application Firewall (WAF)<br>- Solutia trebuie sa includa functionalitati de DNS Application Firewall (DAF)<br>- Solutia trebuie sa includa in mod integrat functionalitati pentru protectia impotriva atacurilor DoS distribuite(DDoS)<br>- Solutia permite gestionarea accesului in aplicatii: — SAML, WIA,Kerberos,NTLM,TDS SQL Logon, LDAP,RADIUS, Basic,OCSP stapling, HTML Form-based<br>- Solutia include suport pentru audit bazat pe Radius<br>- Solutia trebuie sa se integreze cu Ansible, Terraform si Prometheus<br>- Solutia include suport SSL/TLS: TLS 1.2 si 1.3, Perfect Forward Secrecy (PFS), ECDHE si ECC<br>- Solutia include suport pentru AES-NI/GCM<br>- Solutia include suport pentru detectia unor anomali |

| | |
|---|---|
| | - Solutia include suport pentru limitarea numarului de conexiuni<br>- Solutia include suport pentru limitarea ratei(Rate Limiting) pe adresa IP sursa<br>- Soluția include suport pentru liste dinamice (lista alba/lista negra)<br>- Soluția include suport pentru Simple Certificate Enrollment Protocol (SCEP)<br>- Posibilitatea de a descarca periodic liste dinamice pentru filtrare/analiza/blocare de la un threat intelligence oferit de acelasi producator<br>- Soluția include suport pentru prevenirea atacurilor de tip DNS cache-poisoning prin DNSSEC<br>- Soluția include suport pentru single sign-on(SAML, Kerberos)<br>- Soluția include suport pentru validarea certificatelor de client intr-un server OCSP<br>- Soluția include suport pentru algoritmi bazati pe curba eliptica |
| Metode de accelerare a aplicației | - Soluția include suport pentru accelerarea si optimizarea aplicatiilor HTTP: Multiplexare TCP, stocarea temporara intr-o zona tampon a memoriei RAM(RAM Caching) si compresie HTTP<br>- Soluția include suport pentru descarcarea SSL: terminatie SSL, reutilizarea ID-ului de sesiune SSL si SSL Bridging<br>- Suport pentru optimizari TCP(Selective Acknowledgment, Client KeepAlive si Window Scaling)<br>- Suport pentru HTTP Pipelining<br>- Suport pentru HTTP/2, SPDY |
| Funcționalități rețea | - Se poate integra la Layer 2 sau la Layer 3<br>- Soluția include suport pentru integrare in mod transparent sau rutat(mod gateway)<br>- Soluția include suport pentru rutare: Statica, IS-IS (v4/v6), RIPv2/ng, OSPF v2/v3, BGP4+<br>- Soluția include suport pentru VLAN-uri (802.1Q)<br>- Soluția include suport pentru agregarea de link-uri(802.1AX), LACP<br>- Soluția include suport pentru liste de control acces(ACL)<br>- Soluția include suport pentru NAT (IPv4 NAT/NAPT)<br>- Soluția include suport pentru NAT (IPv6 NAPT)<br>- Soluția include suport pentru Jumbo Frame<br>- Soluția include suport pentru VXLAN |

| | |
|---|---|
| | - Soluția include suport pentru NVGRE |
| Functionalitati de administrare si monitorizare a sistemului | - Echipamentul trebuie sa poata fi administrat prin interfata grafica web si CLI<br>- Acces la interfata de management prin SSH si TELNET<br>- Acces securizat la interfata de management web<br>- Suport SNMP, syslog, alerte prin email, NetFlow v9 and v10 (IPFIX), sFlow<br>- REST API<br>- Suport LDAP, TACACS+, RADIUS<br>- Control configurabil al procesorului<br>- Interoperabilitatea cu o solutie de management, configurare si analiza oferita de acelasi producator |
| Conditii de alimentare si mediu | - Putere necesara: 100 - 240 VAC, 50 - 60 Hz<br>- Temperatura de operare: 0 - 40 grade Celsius<br>- Umiditate: 5% - 95% fara condens |
| Licentiere, Support si Garantie | - Support producator de tip 24x7x365 ce va include:<br>o Update-uri pentru pentru indeplinirea functionalitatilor de Securitate: WAF, DAF, DDoS<br>o Support telefonic si web (ticketing)<br>o Update software<br>o Acces documentatie tehnica<br>o Garantie hardware cu schimb echipament defect in maxim 3 zile lucratoare |

#### *4.4.19 Soluție de backup*

- Soluția trebuie sa asigure protecția sistemelor de producție, a datelor si aplicațiilor ce vor rula pe aceste sisteme, sa monitorizeze aplicarea politicilor de protecție si recuperare a datelor, sa utilizeze mecanisme de deduplicare si compresie și să permită replicarea continua a mașinilor virtuale.
- Licențierea soluției trebuie sa fie calculata după numărul de procesoare fizice in utilizare pe sistemele de calcul ale infrastructurii de producție.
- Licențierea trebuie sa fie de tip perpetuul, nu se accepta cea pe baza de abonament, tip subscripție.
- Soluția trebuie sa asigure protecția sistemelor virtualizate si fizice, a sistemului de operare, a fișierelor si aplicațiilor ce rulează pe aceste sisteme prin politici de protecție unitare sau distincte.
- Administratorul trebuie sa utilizeze o singura interfața de administrare a politicilor de protecție si restaurare a datelor pentru toate politicile de protecție indiferent de sistemele de protejat.
- Soluția trebuie sa permită configurarea politicilor de protecție in mod independent pentru protecția unui fisier, a sistemului de operare, a imaginii întregului sistem sau pentru o aplicație specifica.

- Sursa datelor, sistemul sau aplicația de protejat, trebuie sa comunice in mod direct si securizat cu sistemul dedicat pentru protecția datelor folosind mecanisme de autentificare.
- Soluția va permite protecția unui număr nelimitat de mașini virtuale si de aplicații ce rulează pe sistemele licențiate conform matricei de compliança 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.
- 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, SAP, DB2, Informix, MySQL, PostgreSQL si MongoDB.
- Soluția va permite protecția oricărui tip de baze 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.

- Soluția va include servicii de replicare a mașinilor virtuale tip VMware, in mod sincron sau asincron, local sau la distanta, cu jurnalizarea informațiilor modificate pe o perioada de timp determinata.
- 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 vederea stocării datelor salvate se dorește achiziționarea a unui sistem hardware dedicat protecției datelor, tip appliance, certificat de producător.
- Sistemul propus trebuie sa susțină deduplicarea datelor cu posibilitatea de a rula procese paralele de salvare si restaurare, utilizând interfețe multiple de rețea fără a afecta integritatea datelor.
- Echipamentul va susține un minim de 400 de sesiuni de transfer de date in paralel.
- Transferul datelor de la sursa la echipament hardware va putea utiliza toate resursele de retea disponibile peste conexiuni multiple prin mecanisme de tip load balancing si fail-over.
- Procesul de deduplicare trebuie sa se desfășoare continuu, “inline”, fara stocare temporara a datelor, iar factorul de deduplicare sa fie global indiferent de sursa acestor date.
- Echipamentul trebuie sa includă o capacitate utila de minim 1,5 PB si sa permită posibilitatea de creștere a capacității de cel puțin trei ori utilizând aceleași resurse de procesare si memorie.
- Echipamentul trebuie sa includă minim 4 x 10Gbps Ethernet si 4 x 32G Fiber Channel, capacitate de stocare de tip SSD aferent sistemului de operare, memorie tip NVRAM pentru protecția datelor in timpul procesului de scriere, doua surse electrice, protecția discurilor SAS prin RAID 6 si cate un disk hot-spare inclus pentru fiecare grup de discuri.
- Echipamentul trebuie să includă o capacitate de stocare de tip SSD destinata exclusiv memorării si accesări rapide a indecșilor specifici procesului de deduplicare indiferent de capacitatea utilizata.
- Echipamentul trebuie sa utilizeze un factor global de deduplicare pentru toate datele salvate sau arhivate, indiferent de sursa, protocol, sau interfața de rețea prin care au fost transferate.
- Echipamentul trebuie sa permită integrare cu protocoale multiple minim CIFS, NFS, NDMP si VTL.
- Segmentele de date deduplicate trebuie sa poată fi securizate prin mecanisme de tip WORM, protejate fata de eventuale acțiuni de ștergere ale unor intervenții neautorizate.
- Politicile de securizare a datelor in echipament trebuie sa permită mai multe nivele de protecție inclusiv pentru perioade nedefinite indiferent de politica de retenție aplicata la momentul salvării.
- Echipamentul trebuie sa susțină mecanisme de evaluare si corecție a datelor salvate, a sistemului de fișiere, prin care asigura verificarea continua a segmentelor de date deduplicate si disponibilitatea de restaurarea granulara sau completa a fiecărui proces de salvare finalizat cu succes.
- Procesul de expirare si ștergere a segmentelor de date deduplicate trebuie să se facă in mod automat permițând proceselor de salvare si restaurare sa se desfășoare fără oprire.
- Echipamentul trebuie sa includă mecanisme interne de protecție de tip snapshot.

- Echipamentul trebuie sa permită criptarea segmentelor unice de date in mod complianța FIPS 140-2.
- Echipamentul trebuie sa permită replicarea datele într-un sistem similar iar procesul de replicare va transfera doar segmentele de date noi, unice, deduplicate, către sistemul de la distanta.
- Componentele software si hardware ale soluției trebuie sa permită integrarea cu aplicații externe utilizând interfețe software standard tip REST API.

### *4.4.20 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.

#### *4.4.21 Rack și accesorii tip 1*

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:

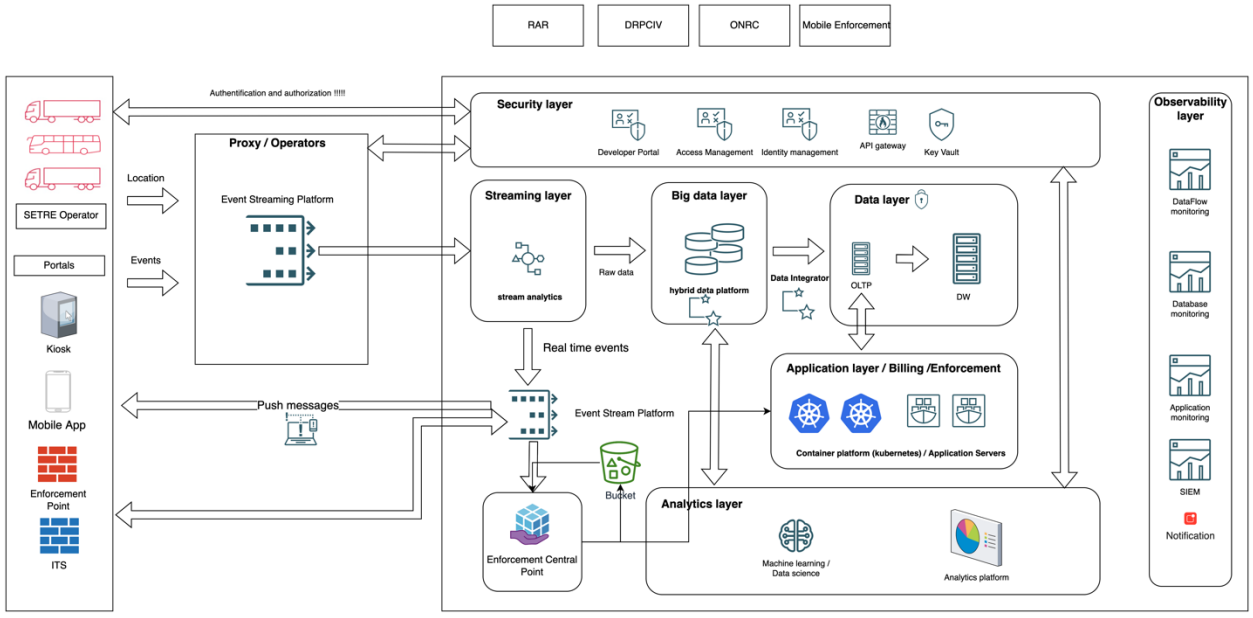



*Figura 3 - Diagrama flux tarifare bazata pe distanta parcursa*

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 Amazon S3 Object Storage)
- Procesează imaginile recepționate si efectuează o noua identificare a numerelor auto înglobând un sistem de tip ALPR – Automatic License Plate Recognition
- 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 contravenții expune servicii către:

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

Modulul de procesare contravenții consuma servicii de la:

- DRPCIV
- Registrul Auto Roman
- Oficiul National Registrul Comerțului
- Sistemul Național de Evidenta a Persoanelor
- Banca Națională a României – Curs Valutar

### *4.5.3 Funcționalități servicii web pentru colectare date de la operatorii SETRE*

Pentru achiziția datelor transmise de catre operatorii SETRE despre poziția si deplasarea autovehiculelor înregistrate in sistem se vor dezvolta interfețe specializate.

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

### *4.5.4 Funcționalități 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 dorește 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 funcționala a sistemelor integrate se va dezvolta având la baza standardul STN ISO 17573-1.

### *4.5.5 Funcționalități aplicație mobila pentru înregistrare si transmitere date privind traseul parcurs de un autovehicul*

Pentru a oferii soluții 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 și servicii trebuie să ia în considerare cerințele referitoare la politicile instituțiilor cu atribuții privind actualizarea informațiilor despre persoană și accesul la date cu caracter personal;
- în scopul realizării și menținerii unui nivel adecvat de acces la date și servicii, se vor lua în considerare cel puțin următoarele:
- soluție de tip Single-Sign-On pentru autentificarea unitară și managementul sesiunilor utilizatorilor din sistem;
- cerințele de securitate ale aplicațiilor;
- politicile departamentale și de instituții publice privind diseminarea informațiilor;
- cerințele contractuale și legale ale organizațiilor nonguvernamentale, în vederea protejării împotriva accesului neautorizat la date și servicii.
- capabilitatea de a înregistra operațiile/tranzacțiile 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 aplicația, pentru a preîntâmpina accesul neautorizat la sistem al altor persoane;
- capabilitatea de a înregistra evenimente definite de securitate și să transmită mesaje de alertă administratorilor de securitate;
- să permită prin monitorizarea accesului și 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 unidirecțional sau bidirecțional pe protocoale standardizate cu respectarea cerințelor de securitate prin interfețe de acces programatic, de tip API / WebServices (transfer de date / mesaje via XML, JSON, SOAP, standarde de tip openAPI).

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

Sistemul se va integra cu următoarele entități:

- Registrul Auto Roman
- D.R.P.C.I.V.

- Sistemul National Integrat de Evidenta a Populației
- Oficiul National Registrul Comerțului
- Institutul Național de Cercetare - Dezvoltare în Informatică

### 4.6 CERINȚE NON-FUNCȚIONALE

Toate soluțiile ofertate cu excepția celor dezvoltate personalizat trebuie să fie de tip COTS (commercial off the shelf), modulare, integrate, consacrate și recunoscute pe plan internațional. Ele trebuie să aducă valoare adăugată sistemului informatic prin cele mai bune practici internaționale specializate și 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, însoțit de scenariile de testare, va fi realizat de către Prestator și 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 și testele de acceptanță specifice. Ofertantul trebuie să prezinte metodologia de testare după care se vor realiza activitățile de testare în timpul desfășurării proiectului. Ofertantul trebuie să prezinte instrumentele de testare folosite.

## 5.5 MIGRAREA DATELOR ISTORICE

Se vor derula activități de preluare a datelor din sistemele operaționale existente și încărcare a lor în noua soluție, urmata de verificarea și validarea încărcării corecte (testare).
Vor fi considerate dezvoltarea de scripturi dedicate pentru preluarea datelor din sistemele operaționale existente și încărcarea lor în modulele corespunzătoare din noua soluție.
Vor fi considerate activități de analiza, de mapare/proiectare, de dezvoltare, testare și implementare.
Vor fi considerate și 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 aplicațiile existente la Beneficiar precum și să țină cont de un plan de migrare automată a datelor în noul sistem integrat.

## 5.6 PUNEREA ÎN PRODUCȚIE

Ofertanții trebuie să prezinte planul care va fi utilizat la trecerea în producție a sistemului, atașat procedurii de acceptanta.

Planul de trecere în producție trebuie să țină cont de legăturile logice între subsisteme/componente ale sistemului astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activităților zilnice a angajaților Beneficiarului.

Înainte de trecerea efectivă în producție, va avea loc pilotarea sistemului pentru o perioadă de minim 4 săptămâni.

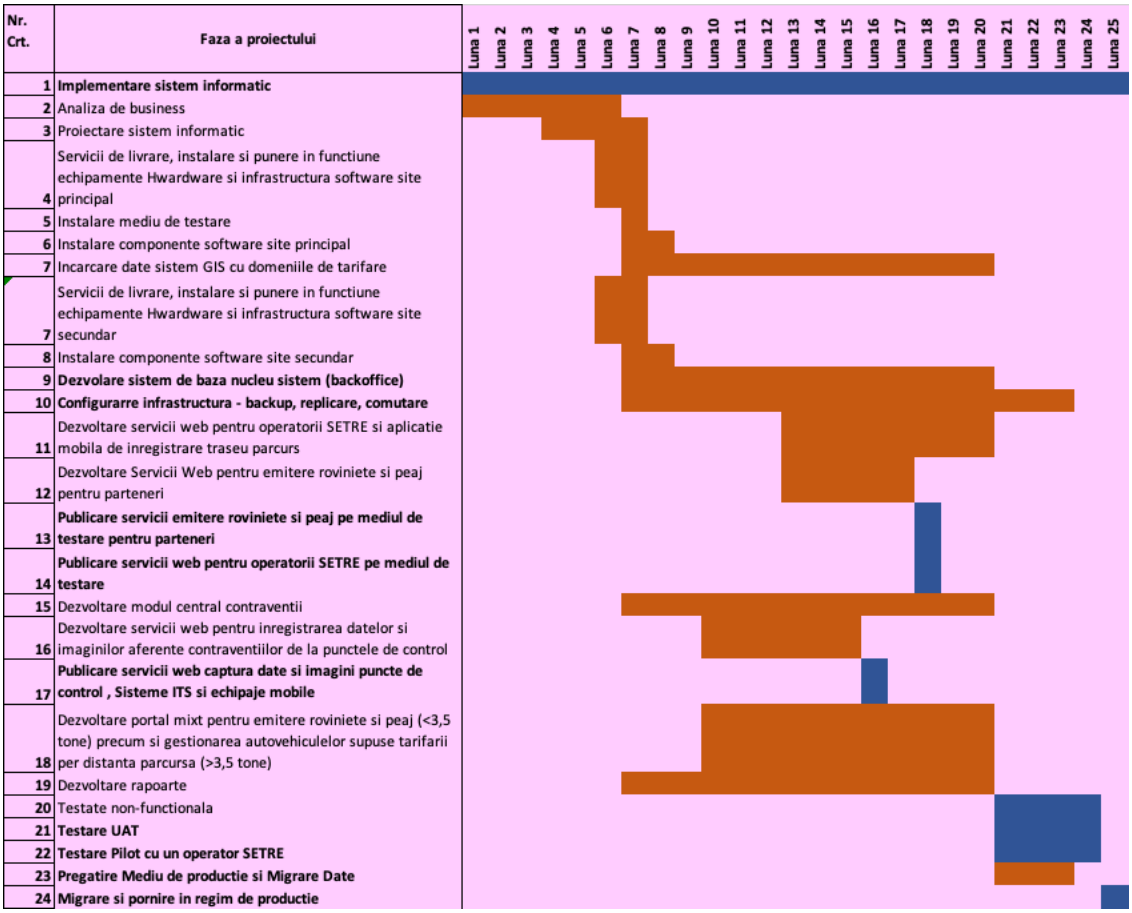
Concluziile rezultate în urma pilotării vor fi utilizate pentru ajustarea proceselor și fluxurilor implementate și va avea ca obiectiv optimizarea funcționării și exploatării sistemului.

Codul sursă al aplicației informatice dezvoltate pentru funcționarea sistemului integrat rămâne în proprietatea Beneficiarului, pentru fiecare versiune a sistemului din producție.

Data trecerii în producție 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 |
| 7 | Servicii de livrare, instalare si punere in functiune echipamente Hwardware si infrastructura software site secundar |
| 8 | Instalare componente software site secundar |
| 9 | **Dezvolare sistem de baza nucleu sistem (backoffice)** |
| 10 | **Configurarre infrastructura - backup, replicare, comutare** |
| 11 | Dezvoltare servicii web pentru operatorii SETRE si aplicatie mobila de inregistrare traseu parcurs |
| 12 | Dezvoltare Servicii Web pentru emitere roviniete si peaj pentru parteneri |
| 13 | **Publicare servicii emitere roviniete si peaj pe mediul de testare pentru parteneri** |
| 14 | **Publicare servicii web pentru operatorii SETRE pe mediul de testare** |
| 15 | Dezvoltare modul central contraventii |
| 16 | Dezvoltare servicii web pentru inregistrarea datelor si imaginilor aferente contraventiilor de la punctele de control |
| 17 | **Publicare servicii web captura date si imagini puncte de control , Sisteme ITS si echipaje mobile** |
| 18 | Dezvoltare portal mixt pentru emitere roviniete si peaj (<3,5 tone) precum si gestionarea autovehiculelor supuse tarifarii per distanta parcursa (>3,5 tone) |
| 19 | Dezvoltare rapoarte |
| 20 | Testate non-functionala |
| 21 | **Testare UAT** |
| 22 | **Testare Pilot cu un operator SETRE** |
| 23 | **Pregatire Mediu de productie si Migrare Date** |
| 24 | **Migrare si pornire in regim de productie** |



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 draft de 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 declarării câștigătorului licitației.

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.

*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 funcționării sistemului<br>Problema împiedică desfășurarea activității instituției, procesul de activitate este serios afectat și nu mai poate continua, pierderea funcționalităților devenind critică.<br>Sistem total nefuncțional |
| Critic | Impact Semnificativ asupra funcționării sistemului<br>Problema împiedică desfășurarea în condiții normale a activității utilizatorilor. Nicio soluție alternativă nu este disponibilă iar activitatea utilizatorilor poate totuși continua, însă într-un |

| | |
|---|---|
| | mod restrictiv.<br>Eroare ce afectează majoritatea funcționalităților sistemului |
| Major | Impact Mediu asupra funcționării sistemului<br>Problema afectează minor funcționalitățile sistemului.<br>Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.<br>Eroare apărută la o funcție, proces sau componentă, sistem parțial nefuncțional. |
| Minor | Impact Minim asupra funcționării sistemului<br>Problema nu afectează funcționalitățile sistemului.<br>Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității utilizatorilor.<br>Eroare care afectează o funcție dar funcționarea întregului sistem nu este afectată semnificativ. |

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

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

*Timpi de răspuns și rezoluții*

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

| Nivel prioritate | Timp de răspuns | Timp maxim soluție 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 calculați din momentul în care Prestatorul a fost înștiințat de apariția problemelor.

La sfârșitul fiecărui caz deschis, Prestatorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului și o va include în recomandarea finală. Fiecare intervenție în sistem va fi documentată de către Prestator prin elaborarea unei fișe de intervenție care va conține cel puțin următoarele detalii: data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției, durata intervenției; fișa 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 și 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 și upgrade-uri ce includ funcționalități, îmbunătățiri și performante, lansate oficial de către producătorii acestora.

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de suport.
Ofertanții trebuie să prezinte împreună cu oferta procedurile suport din cadrul propriei organizații.

# 9 METODOLOGIA ȘI PLANUL DE LUCRU

Metodologia și planul de lucru sunt componente-cheie și 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 și organizarea acestuia.

## 9.1 METODOLOGIA

În această secțiune Ofertantul va prezenta modul în care înțelege:

- obiectivele contractului și 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 activităților în scopul obținerii rezultatelor așteptate.

Cel puțin următoarele informații vor fi prezentate:

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

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

- Managementul de Proiect
- Managementul Schimbării
- Dezvoltarea de soluții software

- Testare
- Management al Riscurilor și Asigurarea Calității
- 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.

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 (în original sau copie autentificată notarial), 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.

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

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

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

Responsabilități:

- Definirea, împreuna cu Expertul Integrare si Expertul 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

Responsabilități:

- Coordonează activitățile de analiza a cerințelor de business, elaborare a documentelor de specificații funcționale si a scenariilor de testare
- Activități de implementare, asistenta si suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanta a sistemului

### *9.3.3 Experții non-cheie*

#### *9.3.3.1 Expert Analist de business – 3 persoane*

- Absolvent studii superioare finalizate cu diploma de licența
- Competente privind analiza de business dovedite prin certificare in domeniu
- Experiența specifica in cel puțin un proiect sau contract in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.2 Expert Analist date – 1 persoana*

- Absolvent studii superioare finalizate cu diploma de licența
- Competente privind tehnici de analiza multi-dimensionala utilizate in analiza datelor dovedite prin diploma/certificare in domeniu
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.3 Coordonator dezvoltare software – 1 persoana*

- Absolvent studii superioare finalizate cu diploma de licența;
- Competente privind o metodologie de dezvoltare software, recunoscuta la nivel național/ internațional, dovedite prin certificare in domeniu
- 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).
- Competente privind dezvoltarea de aplicații bazate pe tehnologii BigData (precum Hadoop, Spark, etc) dovedite prin certificare recunoscuta la nivel național/internațional

- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.4 Specialist Dezvoltare software – 18 persoane*

- Absolvent studii superioare finalizate cu diploma de licență;
- 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.5 Expert Coordonator testare – 1 persoana*

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.6 Specialist testare – 6 persoane*

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel național/ internațional
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.7 Expert integrare – 2 persoane*

- Absolvent studii superioare finalizate cu diploma de licență;
- Competente in domeniul modulelor de integrare in proiecte cu arhitectura de tip Enterprise
- Experiența specifica in cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

#### *9.3.3.8 Expert baze de date relaționale – 1 persoana*

- Absolvent studii superioare finalizate cu diploma de licență;

- 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

***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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care 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 proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

# 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 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 acuratețe 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 și prezentare etc) vor face obiectul dreptului exclusiv de proprietate (inclusiv, dar fără a se limita la drepturi de autor și/sau orice alte drepturi de proprietate intelectuală) al Autorității Contractante, care le poate utiliza, publica sau transfera după cum consideră necesar, fără nicio limitare geografică sau de alta natură.

Drepturile patrimoniale de autor asupra soluției tehnice create de către Prestator (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, CNAIR (cf. art. 12, alin. (1) din Ordonanța de urgență nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative: ”Instituțiile publice și organele de specialitate ale administrației publice centrale au obligația de a prevedea explicit în caietele de sarcini și în contractele aferente procedurilor de achiziție publică demarate de la dat intrării în vigoare a prezentei ordonanțe de urgență, care includ dezvoltări de programe informatice la solicitarea instituției sau autorității, faptul că toate drepturile patrimoniale de autor asupra tuturor operelor create de către contractant sau membrii asocierii, aferente produsului sau serviciului livrat, se transferă către autoritatea contractantă”.

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

Înainte de plata facturii finale, autoritatea contractanta preia integral codul sursă al aplicațiilor informatice dezvoltate, documentația aferentă și kit-urile de instalare.

## 11 ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI

### 11.1 CONȚINUTUL PROPUNERII TEHNICE

CNAIR va îndeplini rolul de Autoritate Contractantă în prezenta procedura de achiziție publică și va fi Ofertantul va descrie în detaliu modul de îndeplinire a cerințelor de realizare a activităților.

Oferta tehnică va cuprinde următoarele:

1. Metodologia de prestare a serviciilor constituie acea parte a propunerii tehnice care prezintă strategia propusă de ofertant pentru prestarea serviciilor solicitate prin specificațiile tehnice incluse în documentația de atribuire.

Metodologia trebuie să cuprindă minimum următoarele informații:

- descrierea de ansamblu a abordării propuse de ofertant pentru prestarea serviciilor, precum și a riscurilor aferente implementării proiectului;
- descrierea cât mai detaliată a activităților propuse de ofertant pentru prestarea serviciilor solicitate, cu indicarea oricăror etape / stadii considerate ca esențiale, a rezultatelor și efectelor așteptate și estimate ale fiecărei activități, precum și a riscurilor specifice fiecărei activități;
- 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 licențelor ofertate, specificând în clar numele licenței de la producător, ediția, producătorul, cantitatea și unitățile de licențiere specifice producătorului precum „User" sau „Processor Core" precum și corelarea acestora cu cerințele caietului de sarcini.

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

*Produse software propuse*

| Nr. Crt. | Denumire componentă (*) | Producător | Nume produs propus (**) | Descriere produs | Cantitate | Unitate de măsură | Modul de licențiere (***) | Garanție și/sau mentenanță |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

*(*) Denumirea componentei conform Caietului de Sarcini.*
*(**) Denumirea completă dată de producător, inclusiv ediția (exemplu „Standard", „Enterprise", dacă este cazul). Se va insera câte un singur produs pe un rând.*
*(***) Va conține detalierea modului de licențiere al producătorului cu explicații privind modalitatea de îndeplinire a cerințelor caietului de sarcini.*

4. Lista echipamentelor hardware specificând în clar identificatorul unic producător (part-number) asociat fiecărui echipament și componenta, numărul de echipamente ofertate pentru fiecare tip de echipament, configurația acestora, precum și corelarea acestora cu cerințele 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 | Garanție și/sau mentenanță |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

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

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

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

5. Fişele tehnice ale tuturor materialelor, instrumentelor şi utilajelor propuse de ofertant pentru desfăşurarea activităților proiectului din care să reiasă conformitatea cu cerințele documentației de atribuire.

6. Propunerea tehnica va fi elaborata punctual, într-o anexă sub forma de tabel de conformitate (în format editabil) in care va fi înscris, in partea stingă, cerințele tehnice din caietul de sarcini (cu precizarea capitolului și a paginii) iar, in partea dreapta modul concret de îndeplinire a cerințelor 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**. Identificarea elementelor de conținut copiat va face obiectul unei solicitări de clarificări în care ofertantul va trebui să demonstreze pe baza documentelor transmise în cadrul ofertei sale că a descris clar și relevant modul de îndeplinire a cerinței.

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

Lipsa oricăreia din secțiunile de mai sus sau a oricărei informații solicitată în cadrul acestor cerințe va duce la descalificarea ofertei.

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 va 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 va duce la descalificarea ofertantului. De asemenea, un simplu răspuns (afirmație) de confirmare din partea operatorului economic cu privire la

respectarea cerințelor din Caietul de Sarcini, fără precizarea exactă a modalității de îndeplinire, nu va fi acceptat. 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 va 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, cu evidențierea separată a TVA, pe fiecare activitate/subactivitate, cu evidențierea unităților de măsură și a valorilor unitare, conform anexei la formularul de ofertă financiară
Bugetul de cheltuieli incidentale nu va fi inclus în propunerea financiară.
Nu există suprapuneri între costurile logistice/cheltuieli incidentale de cheltuieli directe (precum onorariile experților.)
Orice alt document al propunerii financiare se va prezenta corespunzător astfel încât acesta să furnizeze toate informațiile cu privire la prețurile și tarifele respective (exprimate în Lei, fără TVA) precum și la alte condiții financiare și comerciale astfel încât aceasta să asigure prestarea întregilor/tuturor cantităților/serviciilor solicitate prin caietul de sarcini

## 12 MODALITĂȚI ȘI CONDIŢII DE PLATĂ

Plata se va face eșalonat în funcție de livrări și recepții parțiale sau recepție finală. 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<br>Probabilitate: mică | Impact: semnificativ<br>Consecințe: apariția unor disfuncționalități în gestionarea proiectului și în coordonarea echipei de proiect.<br>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.<br>Responsabili: Director General CNAIR |
| 2 | Descompletarea echipelor pe durata ciclului de viața al proiectului<br>Probabilitate: medie | Impact: mediu<br>Consecințe: un posibil impact semnificativ asupra activităților proiectului, livrabilelor cheie, finalizării etapelor proiectului. Pierderea unor abilitați cheie în momente critice.<br>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.<br>Responsabili: manager de proiect CNAIR, Director General CNAIR |
| 3 | Rezistenta personalului beneficiarului la schimbare<br>Probabilitate: medie | Impact: mediu<br>Consecințe: Probleme operaționale. Beneficiile sistemului nu pot fi valorificate complet din cauza folosirii practicilor vechi de lucru.<br>Acțiuni corective: problema va fi escaladată către Comitetul Director al Proiectului. Ar putea fi necesare programe de instruire suplimentare.<br>Acțiuni preventive: obținerea angajamentului conducerii beneficiarului că personalul său va fi informat despre importanta proiectului.<br>Responsabili: manager de proiect CNAIR, Director General CNAIR |
| 4 | Modificări în aria de cuprindere a proiectului<br>Probabilitate: medie | Impact: mediu<br>Consecințe: Posibile reevaluări ale obiectivului, costurilor și/sau etapelor proiectului.<br>Acțiuni corective: Reprogramarea componentelor non-critice ale proiectului pentru etapa ulterioara. Acest proces va fi desfășurat în concordanta cu procedura de control a modificărilor.<br>Acțiuni preventive: Asigurarea acordului tuturor factorilor decizionali importanți în privința acoperirii sistemului din faza inițială a proiectului.<br>Responsabili: manager de proiect CNAIR / manager de proiect prestator |
| 5 | Lipsa cooperării din partea utilizatorilor<br>Probabilitate: mica | Nivelul de implicare a utilizatorilor este esențial atât pentru succesul sistemului cât și pentru acceptanța finală.<br>Impact: mediu<br>Consecințe: costuri suplimentare pentru proiect, cauzate de eventuala apariție a unor noi cerințe. Definirea eronată a unor cerințe funcționale.<br>Acțiuni corective: Escaladarea către nivelurile conducerii superioare și obținerea unui angajament puternic din partea Comitetului Director.<br>Acțiuni preventive: Utilizatorii trebuie implicați în activitățile proiectului. Dacă este necesar se vor efectua analize ale proiectului.<br>Responsabili: manager de proiect CNAIR / manager de proiect |

| | | |
|---|---|---|
| | | prestator |
| 6 | Nu se respecta termenul de implementare tehnică al proiectului.<br>Probabilitate: medie | Impact: mediu<br>Consecințe: imposibilitatea respectării termenului de implementare specificat în Contractul de finanțare<br>Acțiuni preventive: Respectarea perioadei de analiză pentru stabilirea tuturor detaliilor pentru desfășurarea dezvoltării în parametri stabiliți. Verificarea periodica a taskurilor în derulare.<br>Acțiuni corective: stabilirea măsurilor pentru recuperarea timpului pierdut în etapele anterioare. Încheierea de acte adiționale la contractul de finanțare.<br>Responsabili: manager de proiect CNAIR / manager de proiect prestator |
| 7 | Produsul nu respectă întocmai cerințele clientului<br>Probabilitate: medie | Riscul apare atunci când Prestatorul nu a înțeles exact ce dorește clientul sau când nu sunt respectate specificațiile funcționale ale proiectului.<br>Impact: Semnificativ<br>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.<br>Responsabili: manager de proiect CNAIR / manager de proiect prestator |
| 8 | Produsul final conține bug-uri<br>Probabilitate: medie | Impact: Mediu<br>Acțiuni preventive: stabilirea unei etape de testare internă a fiecărei componente, apoi a unei testări integrate.<br>Acțiuni corective: Asigurarea unei marje de timp pentru rezolvarea bug-urilor, existenta unei echipe de testare care să descopere toate bug-urile existente.<br>Responsabili: manager de proiect CNAIR / manager de proiect prestator |
| 9 | Domeniu nou pentru dezvoltatori<br>Probabilitate: medie | Fiind un produs inovator pe piață, dezvoltatorii sistemului pot avea dificultăți în a-și desfășura munca.<br>Impact: Mare<br>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.<br>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 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.<br>Probabilitate: medie | Impact: Mediu<br>Acțiuni preventive: Stabilirea unei strategii de testare și acceptanță imediat după demararea proiectului de implementare a soluției informatice.<br>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.<br>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.<br>Probabilitate: medie | Impact: Mediu<br>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.<br>Acțiuni corective: Implicarea managerului de proiect al CNAIR și a managerului de proiect al prestatorului pentru medierea eventualelor dispute.<br>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.<br>Probabilitate: medie | Impact: Mare<br>Consecințe: Dacă Ofertanții nu reușesc să obțină finanțări naționale/internaționale nu se vor putea plasa comenzile de echipamente.<br>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.<br>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.