

Secțiunea IV

Caiet de sarcini

SII ANALYTICS
**Sistemul Informatic de integrare
și valorificare operațională și analitică
a volumelor mari de date, formare
personal și interconectare rețele
LAN și SAN**

LOTUL I.....	5
1. SUBSISTEM - COMPONENTA DE ACCES SECURIZAT ÎN CONDIȚII DE MOBILITATE – 1 BUC.....	10
1.1 <i>Smart Card și middleware pentru platformele mobile - (750 pachete).....</i>	11
1.2 <i>Echipamentele de tip Traffic Access Point (TAP) - (4 buc.).....</i>	11
1.3 <i>Soluție de monitorizare a utilizării resurselor de comunicare colaborativă - (1 pachet).....</i>	12
1.4 <i>Soluție de monitorizare tehnică a comunicațiilor, la nivel de metadată, prin mecanisme de tip NetFlow - (1 pachet).....</i>	13
1.5 <i>Echipamente de tip Switch Ethernet.....</i>	16
1.6 <i>Echipamente de tip Next Generation IPS - (1 pachet).....</i>	18
1.7 <i>Complete hardware de tip Diodă de Date - (7 pachete).....</i>	19
1.8 <i>Echipamente de tip Next Generation Firewall.....</i>	20
1.9 <i>Echipamente de tip DNS Server/DNS Firewall - (1 pachet).....</i>	23
1.10 <i>Echipamente de tip Application Delivery Controller - (1 pachet).....</i>	25
1.11 <i>Echipamente de tip Secure Web Gateway - (1 pachet).....</i>	26
1.12 <i>Echipamentele de tip Gateway WS/API - (2 pachete).....</i>	27
1.13 <i>Soluția de asigurare a serviciilor criptografice centralizate - (3 pachete).....</i>	28
1.14 <i>Componente de tip Server.....</i>	29
1.15 <i>Licență - Suita de tip Enterprise Mobility Management (EMM) - (750 buc.).....</i>	33
1.16 <i>Licență - Componentă de tipVPN pentru terminale mobile - (750 buc.).....</i>	35
1.17 <i>Licență platformă de virtualizare – componenta de acces securizat în condiții de mobilitate - 20 pachete.....</i>	36
1.18 <i>Servicii de instalare și configurare infrastructură - componentă acces securizat în condiții de mobilitate - (1 serviciu).....</i>	39
1.19 <i>Servicii de implementare – componentă de acces securizat în condiții de mobilitate - (1 serviciu).....</i>	40
2. PLATFORMA BIG DATA.....	65
2.1 <i>Șasie de servere - pentru mediul de producție - (1 pachet).....</i>	66
2.2 <i>Șasie de servere - pentru mediul de test / dezvoltare - (1 pachet).....</i>	67
2.3 <i>Servere “blade” (Configurație A), pentru mediul de producție - (16 buc.).....</i>	68
2.4 <i>Servere “blade” (Configurație A), pentru mediul de testare/dezvoltare - (4 buc.).....</i>	69
2.5 <i>Servere “blade” (Configurație B), pentru mediul de producție - (8 buc.).....</i>	70
2.6 <i>Servere “blade” (Configurație B), pentru mediul de testare/dezvoltare - (2 buc.).....</i>	70
2.7 <i>Storage de mare performanță - (1 pachet).....</i>	71
2.8 <i>Storage de uz general, pentru mediul de producție - (1 pachet).....</i>	73
2.9 <i>Storage de uz general, pentru mediul de test/dezvoltare - (1 pachet).....</i>	75
2.10 <i>Interconectare privată (top-of-rack) - (4 pachete).....</i>	77
2.11 <i>LAN Fabric - (2 buc.).....</i>	79
2.12 <i>Platforma de back-up - (1 pachet).....</i>	80

2.13 Licențe platformă Big Data - (1 pachet).....	82
2.14 Licențe sistem monitorizare - (1 pachet).....	83
2.15 Licențe modul Face Recognition, pentru 3.000.000 de subiecți - (1 pachet).....	84
2.16 Licențe platformă de virtualizare - platforma Big Data - (30 buc.).....	84
2.17 Licențe sistem de operare - platforma Big Data - (40 bucăți).....	86
2.18 Instalare și configurare infrastructură platformă Big Data - (1 serviciu).....	87
2.19 Servicii de implementare platformă Big Data - (1 serviciu).....	87
2.20 Servicii de implementare modul Face Recognition - platforma Big Data - (1 serviciu).....	130
2.21 Servicii de implementare sistem monitorizare - (1 serviciu).....	135
2.22 Servicii de integrare cu portalul și access management - (1 serviciu).....	140
3. SECURITATEA SISTEMULUI.....	141
3.1. Nivel echipamente de rețea.....	142
3.2 Nivel de date.....	143
3.3 Nivel aplicație.....	143
3.4 Backup și restaurare a datelor.....	144
3.5 Confidențialitatea datelor.....	144
4. SERVICII DE INSTRUIRE.....	146
4.1 Desfășurarea instruirii.....	146
4.2 Cursuri utilizatori finali - (1 pachet).....	147
4.3 Cursuri, concepte și modele teoretice pentru modulele aferente platformei Big Data - (1 pachet).....	147
4.4 Cursuri, concepte și modele teoretice pentru modulul de Face Recognition - (1 buc.).....	148
4.5 Cursuri administrare, referință, operare și utilizare pentru modulele aferente Big Data - (1 pachet).....	148
4.6 Cursuri administrare, referință, operare și utilizare pentru modulul de Face Recognition - (1 buc.).....	149
4.7 Cursuri administrare, referință, operare și utilizare pentru aplicațiile componente de acces în condiții de mobilitate - (1 buc.).....	149
4.8 Cursuri administrare, referință, operare și utilizare pentru infrastructura Componentei de Acces în condiții de mobilitate - (1 pachet).....	149
4.9 Cursuri tehnologii - (1 pachet).....	150
4.10 Cursuri management - (1 pachet).....	151
5. INSTALARE ECHIPAMENTE ÎN CENTRUL DE DATE.....	151
6. MANAGEMENTUL PROIECTULUI.....	153
7. CRITERII DE ACCEPTANȚĂ.....	153
7.1 Criterii acceptanță Componentă de Acces.....	154
7.2 Criterii de acceptanță - Platforma Big Data.....	154
7.3 Criterii de acceptanță - Servicii de Instruire.....	156
7.4 Livrabile.....	156

8. FACILITĂȚI PUSE LA DISPOZIȚIA FURNIZORULUI.....	157
9. DREPTURI DE PROPRIETATE INTELECTUALĂ.....	157
10. GARANȚIE ȘI SUPORT TEHNIC.....	158
11. SERVICE LEVEL AGREEMENT (SLA) - MEDIU DE PRODUCȚIE ȘI DE DEZVOLTARE/TESTARE.....	160
LOTUL II – INTERCONECTARE REȚELE LAN ȘI SAN.....	168
1. SAN FABRIC (2 BUC.).....	168
2. INTERCONECTARE LAN EXISTENT (2 PACHETE).....	168
3. CRITERII DE ACCEPTANȚĂ.....	170
4. GARANȚIE ȘI SUPORT TEHNIC.....	170
ANEXA 1 - SPECIFICAȚII SESIUNE DEMONSTRATIVĂ.....	172
ANEXA 2 - DIAGRAMA GANTT.....	183

LOTUL I

În cadrul prezentului caiet de sarcini, nominalizarea unui producător sau a unei mărci înregistrate aparținând unui anumit producător este doar cu titlu orientativ, pentru a indica tipul de tehnologie sau o specificație tehnică / cerință minimă solicitată. În zonele unde nu a fost posibilă evitarea unei denumiri tehnologice, pentru a respecta cu strictețe principiul neutralității tehnologice, s-a precizat „și / sau echivalentul” acesteia.

Pentru o cât mai bună descriere a funcționalităților solicitate și pentru a evita, pe cât de mult posibil, o percepție greșită a furnizorului asupra cerințelor definite de către beneficiar prin intermediul prezentului caiet de sarcini, în cadrul documentului au fost folosiți termenii consacrați în limba engleză. Pentru funcționalitățile rezumate prin utilizarea unor astfel de termeni, furnizorul va trebui să asigure soluții recunoscute pe plan intern și internațional ca "best practices", chiar și în condițiile în care acestea implică existența unor cerințe nementionate în mod explicit în cadrul prezentului caiet de sarcini.

Proiectul propus are ca scop:

a) dezvoltarea funcției de prevenție, detectare și luare de măsuri pentru reducerea redundanței plăților în zona publică, prevenirea fraudei și abuzurilor și creșterea eficienței în actul guvernamental;

b) creșterea gradului de utilizare a serviciilor de eguvernare din prisma procesării și interpretării datelor;

prin modernizarea și eficientizarea activităților interne ale instituțiilor cu atribuții în prevenirea și combaterea fenomenelor de terorism, crimă organizată, corupție sau evaziune fiscală, denumite în continuare **instituții publice beneficiare**, precum și optimizarea cooperării între acestea, în efortul comun de identificare, cunoaștere, documentare, prevenire și diminuare a situațiilor generatoare de fenomene de criminalitate organizată și evaziune fiscală la nivel național, precum și a faptelor asociate fenomenului de corupție și de finanțare a terorismului.

Obiectivul proiectului "SII ANALYTICS" susține scopul menționat prin **implementarea unui sistem informatic de integrare și valorificare operațională și analitică a volumelor mari de date**, sub forma unui ansamblu de echipamente hardware și instrumente software, în vederea transformării datelor din bazele de date consolidate urmare a implementării

proiectului “SII INFRASTRUCTURĂ¹” (fără a se limita la acestea) în informații și în cunoștințe, prin mecanisme avansate de prelucrare a datelor.

Implementarea întregului sistem informatic presupune implementarea unei **platforme Big Data** și a unei **componente de acces securizat în condiții de mobilitate (Componenta de Acces)**, extensie a platformei Big Data.

Sistemul informatic trebuie să cuprindă infrastructurile de comunicații, hardware și software atât pentru platforma Big Data cât și pentru Componenta de Acces, astfel încât să asigure instrumente software de valorificare operațională și analitică și să permită interoperabilitate cu mediul IT administrat de beneficiar², achiziționat și configurat în cadrul proiectului “SII INFRASTRUCTURĂ”.

Arhitectura logic-funcțională generală a sistemului informatic este prezentată, într-o manieră sumară, în figura 1, în care sunt evidențiate cele două componente majore ale sistemului: **componenta de acces securizat în condiții de mobilitate** și **platforma Big Data**.

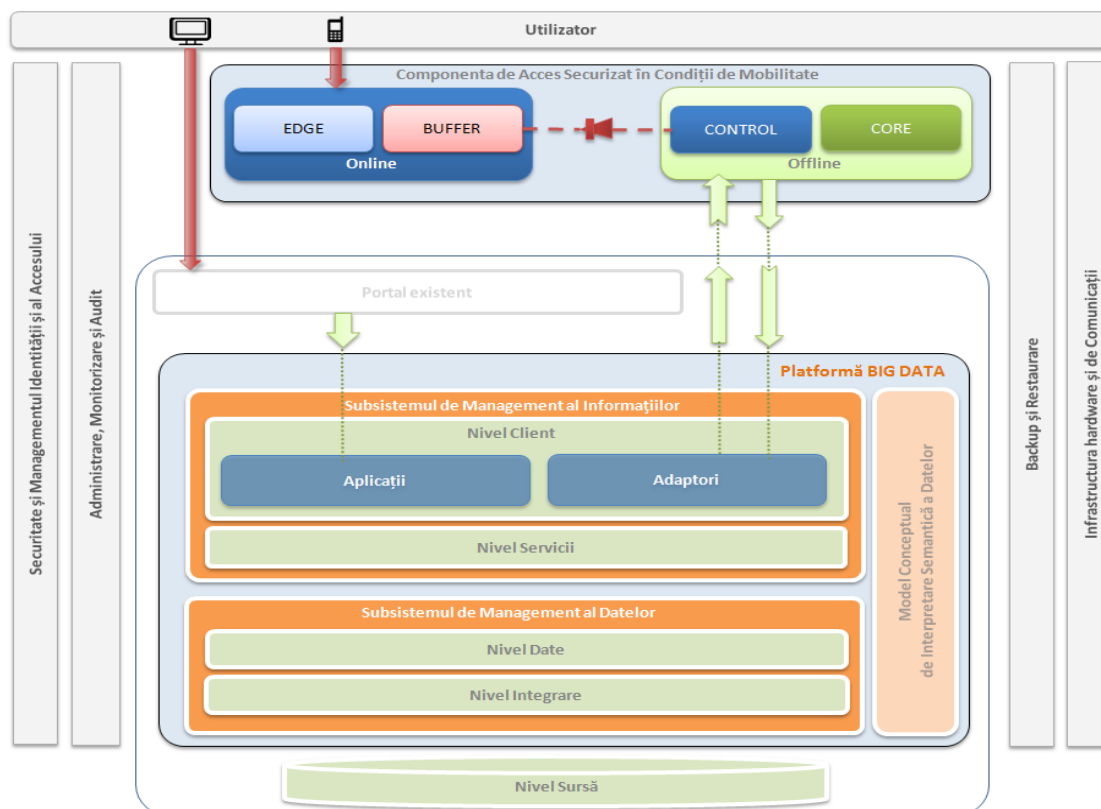


Figura 1: Arhitectura logic-funcțională generală a sistemului informatic

¹ cod proiect SMIS-CSNR 56954, finanțat prin POSCCE 2007 - 2013 Program Operațional Sectorial Creșterea Competitivității Economice;

² vezi capitolele 2.22 Servicii de integrare cu portalul și access management și 2. Interconectare LAN existent

La baza sistemului informatic, și implicit a celor două componente, se află *nivelul surse de date*³. Acesta cuprinde depozitele de date comune - definite în cadrul proiectului, ca totalitatea depozitelor de date structurate, semi-structurate și nestructurate, formă consolidată a datelor furnizate de instituțiile cu rol de furnizor în cadrul proiectului “SII INFRASTRUCTURĂ” - fără a se limita la acestea, precum și seturile de date individuale - definite în cadrul proiectului, ca totalitatea seturilor de date semi-structurate și nestructurate, aflate în posesia utilizatorilor finali.

Platforma Big Data, la nivel macro, este constituită din *două subsisteme interconectate*:

- subsistemul de management al datelor, care asigură un lanț de fluxuri și procese de integrare, distribuite de-a lungul a două niveluri arhitecturale: nivel de integrare și nivel de date propriu platformei Big Data, astfel încât să coreleze volumele mari de date existente în depozitele de date comune și seturile de date individuale sub o formă unică de vizualizare;
- subsistemul de management al informațiilor, care asigură un lanț de procese distribuite de-a lungul a două niveluri arhitecturale: nivel servicii și nivel client, astfel încât, pe baza formei unice de vizualizare, să permită valorificarea operațională și analitică a volumele mari de date existente în depozitele de date comune și seturile de date individuale, prin instrumente grafice (aplicații) ce permit interacțiunea cu utilizatorii finali și prin adaptori ce permit interacțiunea cu Componenta de Acces, precum și cu alte sisteme informatice.

Componenta de acces securizat în condiții de mobilitate - la nivel macro, este organizată pe patru niveluri funcționale:

- nivelul EDGE (online) — grupează resursele online ale Componentei de Acces destinate managementului mobilității utilizatorilor, din perspectiva asigurării accesului securizat la date și la serviciile de aplicație protejate;
- nivelul BUFFER (online) — grupează resursele online ale Componentei de Acces destinate interacțiunii cu aplicațiile mobile autorizate de pe terminalele mobile inteligente și procesării în mod transparent a cererilor de acces la date din nucleul intern protejat (offline) și la serviciile modulelor platformei Big Data;
- nivelul de CONTROL (offline) — grupează resursele independente offline ale Componentei de Acces destinate autorizării explicite a cererilor de acces la date, respectiv

³ vezi cap. 2.19.3.1 Nivel surse de date

controlului replicării autorizate a datelor către componentele online ale Componentei de Acces;

- nivelul CORE (offline) — grupează resursele offline ale Componentei de Acces destinate interacțiunii cu sursele de date protejate, respectiv cu componentele funcționale ale platformei Big Data, pentru generarea seturilor de date în răspuns la cererile autorizate de acces securizat în regim de mobilitate.

Soluția de implementare a sistemului informatic “SII ANALYTICS”, se va conforma următoarelor **cerințe generale minime**, sens în care trebuie să asigure:

- infrastructurile de comunicații, hardware și software care să susțină scopul și obiectivele prezentului proiect;
- doar echipamente de ultima generație care să beneficieze de suport din partea producătorului;
- interoperabilitatea cu mediul IT administrat de beneficiar⁴, achiziționat și configurat în cadrul proiectului “SII INFRASTRUCTURĂ”;
- licențierea software pentru toate produsele care vor rula pe infrastructura hardware;
- administrarea centralizată a platformei tehnologice aferente și a aplicațiilor, prin intermediul unor interfețe de management;
- componente specifice pentru monitorizarea infrastructurilor de comunicații, hardware și software;
- administrarea, monitorizarea și configurarea noului sistem informatic integrat, la nivel de platformă tehnologică, structură de date și interfață cu utilizatorul;
- o arhitectură scalabilă, modulară, flexibilă și deschisă, cu posibilități de extindere a funcționalităților prin intermediul unor librării API bine documentate, care să permită configurări și dezvoltări ulterioare, în funcție de necesitățile instituțiilor publice beneficiare;
- un grad înalt de securitate, asigurând cel puțin protejarea datelor sensibile, controlul accesului prin autentificarea și autorizarea utilizatorilor, precum și auditarea, respectiv trasabilitatea activității acestora;
- mecanisme moderne de efectuare a copiilor de siguranță, cu posibilitatea efectuării unei restaurări rapide în cazul unei defecțiuni temporare sau permanente;
- mecanisme moderne de asigurare a confidențialității datelor;

⁴ vezi capitolele 2.22 Servicii de integrare cu portalul și access management și 2. Interconectare LAN existent

- un punct unic de acces securizat și auditat atât pentru platforma Big Data cât și pentru componenta de acces securizat în condiții de mobilitate;
- un mediu de lucru integrat și centralizat pentru toți utilizatorii noului sistem informatic, indiferent de drepturile de acces asociate acestora;
- o interfață grafică consistentă de interacțiune cu utilizatorul, care să respecte aceeași logică de prezentare a informației, cu facilități avansate de navigare între ecrane prin mecanisme de tip înainte-înapoi, link-uri și/sau tab-uri, fără a se limita la acestea;
- implementarea mecanismelor de internaționalizare și localizare, astfel încât toate mesajele, textele, etichetele, data, timpul, valorile numerice și orice alte aspecte ce țin de cultura locală, vizibile la nivelul interfeței grafice, să fie afișate și în limba română;
- evitarea percepției de ecran înghețat, prin furnizarea unui răspuns intermediar imediat, ulterior fiecărei interacțiuni a utilizatorului cu interfața grafică, sub forma unui text sau simbol grafic determinat sau nedeterminat (*“progress bar”*, *“progress wheel”*);
- feedback către utilizator, pentru toate interacțiunile finalizate cu eșec, prin emiterea unui mesaj relevant de eroare, însoțit de instrucțiuni clare privind modul de continuare;
- manuale de ajutor în limba română, integrate în cadrul aplicațiilor și accesibile utilizatorilor la nivel de interfață grafică, cu privire la prezentarea funcționalităților expuse, precum și a modului de utilizare a acestora;
- scenarii de utilizare în limba română, sub forma unor tutoriale video care să sprijine utilizatorul în procesul de instruire în ceea ce privește modul de navigare prin/utilizare a funcționalităților existente;
- posibilitatea utilizatorului de a accesa în orice moment, cu minimum de efort, manualele de ajutor și scenariile de utilizare a funcționalităților.

În continuare, în textul caietului de sarcini, pentru referențierea colectivă la modulele și funcționalitățile de asigurare a accesului securizat în condiții de mobilitate se va utiliza și sintagma prescurtată Componenta de Acces.

Această componentă, parte integrantă a sistemului informatic de integrare și valorificare operațională și analitică a volumelor mari de date (“SII ANALYTICS”), va permite accesul utilizatorilor autorizați, pe baza unui model riguros de autorizare de tip *“need to know”*, la resurse interne protejate - date și servicii de aplicație.

1. Subsistem - Componenta de acces securizat în condiții de mobilitate – 1 buc.

În figura 1, Componenta de Acces securizat în condiții de mobilitate apare ca și parte integrantă a sistemului informatic de integrare și valorificare operațională și analitică a volumelor mari de date ("SII ANALYTICS"). Aceasta trebuie să se conformeze cerințelor generale trasate în actualul caiet de sarcini, iar suplimentar trebuie să se bazeze pe o soluție tehnică "end-to-end" modernă și customizabilă. De asemenea, Componenta de Acces trebuie să asigure o infrastructura hardware și software de acces securizat în condiții de mobilitate, prin intermediul platformei Big Data, la datele și funcționalitățile autorizate în vederea accesului, și acces partajat la modulele funcționale expuse pe dispozitivele mobile inteligente.

Accesul utilizatorilor autorizați la resurse interne protejate - date și servicii de aplicație - se va face exclusiv pe baza unui model riguros de autorizare de tip "need to know".

1.1 Smart Card și middleware pentru platformele mobile - (750 pachete)

1.1.1 Rol și context:

- componentele hardware de tip smart card vor fi instalate și se vor utiliza pe terminalele mobile autorizate înrolate în sistem și vor permite ridicarea nivelului de încredere în calitatea identificării, autentificării multi-factor și autorizării accesului de pe terminalele mobile astfel echipate.

1.1.2 Configurație și dimensionare

750x pachete compuse din smartcard, dintre care 700 în format microSD și 50 în format ISO (ISO/IEC 7810 ID-1, sau echivalent), și software utilitare/middleware

1.2 Echipamentele de tip Traffic Access Point (TAP) - (4 buc.)

1.2.1 Rol și context

- echipamentele de tip "Traffic Access Point" (TAP) multi-segment vor asigura acces la trafic, în mod offline, pentru monitorizarea comunicațiilor;
- echipamentele de tip TAP vor asigura agregarea ambelor sensuri de comunicație ale fluxului de comunicare full-duplex, pentru captura, duplicarea și agregarea traficului

bidirecțional, pe liniile de comunicație monitorizate, pentru analiza offline (respectiv față de contextul segmentelor de rețea monitorizate).

- traficul astfel agregat va fi transmis către analizoare prin cel puțin câte 1 port de monitorizare pe fiecare echipament de tip TAP.

1.2.2 Configurație și dimensionare

4x bucăți, integrate hardware/software

- fiecare echipament de tip *“Traffic Access Point”* (TAP) va putea monitoriza cel puțin 2 interconexiuni (segmente de rețea) de 10Gbps și va fi configurat și echipat cel puțin cu:
 - 2 porturi de rețea de 10Gbps (intrare și ieșire), echipate cu transceiver optic short-range, pentru fiecare segment de 10Gbps monitorizat;
 - 1 port monitor 10 Gbps pentru traficul agregat, pe relația cu sondele de analiză/monitorizare;
- vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.3 Soluție de monitorizare a utilizării resurselor de comunicare colaborativă - (1 pachet)

1.3.1 Rol și context

- soluție de monitorizare, la nivel de aplicație și de utilizator, prin funcționalități de valorificare analitică extinsă a datelor de trafic, care va permite decodarea, retenția selectivă, capacitatea de replay și analiza modelelor de utilizare a resurselor de comunicare colaborativă.

1.3.2 Cerințe funcționale și specificații tehnice

- soluția va asigura identificarea protocoalelor specifice de comunicare colaborativă în tehnologie Web, inclusiv a mesageriei electronice "instant" și a celei tradiționale (de tip email și asimilată), precum și a tehnologiilor conexe de schimb de informație nestructurată, indiferent dacă serviciile de acest tip vor fi accesate și utilizate prin aplicații dedicate, sau prin pagini Web, în instanțe de tip browser;

- va permite identificarea, decodarea și salvarea, la cerere, precum și vizualizarea artefactelor asociate (inclusiv a fișierelor text și multimedia atașate);
- va permite analiza și retenția selectivă a sesiunilor de comunicare respective, respectiv generarea de structuri de date (metadata) specifice care vor permite descrierea contextului comunicării colaborative și chiar derularea conversațiilor, în mod replay, pentru a prezenta sesiunile din perspectiva participanților la acestea;
- va permite reconstrucția și vizualizarea contextului comunicării colaborative în mod time-line și în mod graf, pentru identificarea rapidă a secvenței operațiilor și, respectiv, a relațiilor între participanți;
- va implementa mecanisme de control strict al accesului la datele generate și la funcțiile de monitorizare a comunicațiilor și de vizualizare a contextului comunicării colaborative, pe bază de roluri.

1.3.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x soluție integrată de monitorizare;
- soluția va include cel puțin:
 - 1x senzor de captură, care va asigura filtrarea și preprocesarea datelor, și care va dispune de cel puțin 2 porturi 10Gbps modulare echipate cu transceiver optic (*“short range”*), și surse de alimentare redundante;
 - 1x platformă de retenție și reconstrucție trafic , care va permite procesarea în timp real asimilat (*“near realtime”*) la nivel de 2Gbps trafic efectiv (valori medii susținute) și stocarea metadata generate pentru cel puțin 10 zile de trafic agregat pe conexiunile monitorizate;
 - 1x consolă cu capacități de replay, pentru traficul analizat, și de vizualizare a contextului interacțiunii.
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.4 Soluție de monitorizare tehnică a comunicațiilor, la nivel de metadată, prin mecanisme de tip NetFlow - (1 pachet)

1.4.1 Rol și context

- asigură monitorizarea fluxurilor de comunicații prin preluarea traficului de la dispozitive de tip TAP, procesarea acestuia în timp real, prin probe dedicate, pentru extragerea, analiza și vizualizarea informației de tip “NetFlow”;
- asigură colectarea și valorificarea analitică a informației de tip “NetFlow” generate, pentru identificarea modului de utilizare a resurselor de comunicații interne oferite ca parte a componentelor online ale platformei tehnice de suport pentru operatorii mobili, pentru detecția prezenței malware și pentru detecția timpurie a atacurilor avansate.

1.4.2 Cerințe funcționale și specificații tehnice

- soluția trebuie să permită preluarea și prelucrarea de seturi metadata de trafic de rețea în format NetFlow (inclusiv versiunea 9) și IPFIX;
- soluția trebuie să permită preluarea și prelucrarea de flow-uri complete (unsampled) și eșantionate (sampled), inclusiv înregistrarea, corelarea, stocarea și extragerea de informații despre tipul și nivelul de utilizare a resurselor din infrastructura de rețea;
- soluția va asigura următoarele capacități:
 - monitorizarea continuă a traficului, cu identificarea tuturor informațiilor de telemetrie necesare pentru analiza și descrierea componentei utile a acestuia, recunoașterea infrastructurii de rețea implicate și înregistrarea continuă a tipului și a nivelului de utilizare a acesteia;
 - monitorizarea continuă a traficului, cu identificarea tuturor informațiilor de telemetrie necesare pentru analiza și descrierea componentei utile a acestuia, recunoașterea infrastructurii de rețea implicate și înregistrarea continuă a tipului și a nivelului de utilizare a acesteia;
 - deduplicarea, în topologia de rețea monitorizată, și corelarea fluxurilor individuale de comunicații care fac parte din aceeași sesiune de comunicație bidirecțională, indiferent de numărul de echipamente implicate;
 - detectarea și corelarea fluxurilor de comunicație care implică routing asimetric și prezentarea unitară și coerentă a sesiunii bidirecționale respective;

- detectarea contextelor de comunicație care implică transformări de tip NAT, respectiv prezentarea unitară și coerentă a sesiunii respective “*end-to-end*”;
 - determinarea modelului normal de trafic, inclusiv a nodurilor implicate și a aplicațiilor/protocoalelor utilizate, precum și detectarea, calificarea și semnalizarea excepțiilor și a anomaliilor;
 - detecția va fi corelată cu modele statistice cunoscute pentru evenimente de securitate și apoi încadrate în categoriile de amenințări cunoscute, dacă există indicația unei compromiteri de sistem informatic, a unei încercări de exfiltrare de informații, sau a unui atac;
 - identificarea prezenței, în traficul monitorizat, a manifestărilor specifice acțiunii componentelor active de tip malware sau care pot fi asimilate atacurilor informatice, inclusiv prin valorificarea surselor globale de informație de tip “*threat intelligence*”;
 - mecanisme integrate, configurabile, de notificare a administratorilor prin multiple canale de alertare , în caz de anomalie severă sau de incident de securitate;
- soluția va dispune de funcționalități de integrare și de valorificare analitică a informației de tip “*threat intelligence*”, din surse globale, și va include subscripția de acces la surse de actualizare a acestora;
 - soluția va fi compusă din instanțe centralizate de configurare și de management, pentru corelarea și prezentarea de evenimente NetFlow, și din colectoare de NetFlow, distribuite în infrastructura de rețea.

1.4.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x soluție integrată de monitorizare;
- soluția va include cel puțin:
 - 1x senzor de captură și procesare trafic, care va asigura generarea de metadata de tip “*NetFlow*” în timp real la nivel de 2Gbps trafic efectiv (valori medii susținute), și care va dispune de cel puțin 2 porturi 10Gbps modulare echipate cu transceiver optic (short-range), și surse de alimentare redundante;
 - 1x platformă de retenție și analiză de metadata în format NetFlow, care va permite stocarea înregistrărilor de tip Netflow pentru cel puțin 10 zile de trafic la

nivel de 2Gbps trafic efectiv (valori medii susținute) agregat pe conexiunile monitorizate;

- 1x consolă cu capacități de coordonare a procesării distribuite a datelor colectate de către senzori/colectori, și de vizualizare a fluxurilor de comunicație și a proprietăților asociate acestora;
- configurația inclusă va asigura cel puțin:
 - preluarea traficului până la cel puțin 8Gbps de trafic efectiv (valori maxime suportate);
 - prelucrarea eficientă a cel puțin 2Gbps de trafic efectiv (valori medii susținute), agregat pe conexiunile cu încapsulare 10Gbps Ethernet monitorizate;
 - preluarea și corelarea a cel puțin 20,000 de înregistrări NetFlow pe secundă;
- vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN;
- configurația va include subscripțiile de acces la actualizările de cataloage de referință de tip *“threat intelligence”* și de tip reputațional, pe perioada asumată prin contract.

1.5 Echipamente de tip Switch Ethernet

Echipamentele de tip Switch Ethernet sunt componentă a infrastructurii de interconectare. În cadrul proiectului vor fi utilizate echipamente de tip Switch Ethernet – Tip 1 și echipamente de tip Switch Ethernet – Tip 2.

1.5.1 Echipamente de tip Switch Ethernet (Tip 1) - (6 pachete)

1.5.1.1 Rol și context

- echipamentele de tip Switch Ethernet (Tip 1), cu funcții de dirijare a traficului inter-VLAN, vor fi regrupate în perechi pentru a implementa interconectarea locală a componentelor interne ale sub-sistemului funcțional în care se află instalate și, acolo unde este cazul, dirijarea traficului către sub-sistemele funcționale direct conectate;
- subsistemele funcționale al Componentei de Acces nu vor partaja aceeași pereche de echipamente de tip Switch Ethernet (Tip 1), cu excepția subsistemului de logică de aplicație și a subsistemului de management al datelor (care vor utiliza în comun aceeași pereche) și a

subsistemului de acces la date (care va folosi mediul de rețea locală LAN, de la nivelul infrastructurii partajate a mediului de producție al platformei Big Data).

1.5.1.2 Cerințe funcționale și specificații tehnice

- arhitectura internă și funcționalitățile echipamentelor de tip Switch Ethernet vor oferi o capacitate de comutare la viteza maximă suportată pe toate interfețele simultan, precum și comutare de tip “*cut-through*” care să asigure latențe mai mici de 1000 nanosecunde.

1.5.1.3 Configurație și dimensionare

6x pachete, integrate hardware/software

- fiecare pachet va include 1x stack de echipamente hardware de tip switch Ethernet;
- fiecare stack va include 2x echipamente Switch Ethernet (Tip 1);
- fiecare echipament Switch Ethernet (Tip 1) va fi licențiat (în cazul în care este necesară licențierea), configurat și echipat cel puțin cu:
 - 16x 10Gbps Ethernet cu interfețe modulare, echipate cu transceiver optic SFP+ (short-range);
 - 8x 1Gbps Ethernet cu interfețe modulare, echipate cu transceiver optic sau electric SFP;
 - 2x surse de alimentare, în configurație redundantă;
 - 2x module de răcire / ventilare, în configurație redundantă.
- vor fi incluse toate reперele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.5.2 Echipamente de tip Switch Ethernet (Tip 2) (3 pachete)

1.5.2.1 Rol și context

- echipamentele de tip Switch Ethernet (Tip 2), cu funcții de dirijare a traficului inter-VLAN, vor fi regrupate în perechi pentru a implementa interconectarea locală a componentelor de monitorizare și management “*out-of-band*”.

1.5.2.2 Cerințe funcționale și specificații tehnice

- asigură implementarea unui mod de funcționare de tip cluster (sau echivalent) care să ofere o singură interfață de administrare pentru o pereche de două sau mai multe switch-uri;
- oferă interfețe capabile să suporte tehnologii de tip 1 Gigabit Ethernet și 10 Gigabit Ethernet atât optice (10GbaseSR) cât și electrice (1000BaseT, 10GBase-T);
- implementează în modulele de interfață funcții de control al traficului folosind politici și liste de control a accesului pentru niveluri ISO OSI 2, 3 și 4, atât pentru protocolul IPv4 cât și pentru protocolul IPv6;
- oferă capacități avansate de monitorizare a traficului folosind tehnologii ca SPAN și ERSPAN, precum și modalități de a monitoriza și apoi de exporta informații despre toate comunicația care traversează switch-ul folosind protocoale de tip Netflow/sFlow (sau echivalente).

1.5.2.3 Configurație și dimensionare

3x pachete, integrate hardware/software

- fiecare pachet va include, 1x stack de echipamente hardware de tip switch Ethernet;
- fiecare stack va include 2x echipamente Switch Ethernet (Tip 2);
- fiecare echipament Switch Ethernet (Tip 2) va fi licențiat (în cazul în care este necesară licențierea), configurat și echipat cel puțin cu:
 - 4x 10Gbps Ethernet cu interfețe modulare, echipate cu transceiver optic SFP+ (short-range);
 - 24x 1/10Gbps Ethernet cu interfețe RJ45;
 - 1x surse de alimentare (configurație activ redundantă, la nivel de stack);
 - 2x module de răcire / ventilare, în configurație redundantă.
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN (.

1.6 Echipamente de tip Next Generation IPS - (1 pachet)

1.6.1 Rol și context

- soluție de protecție anti-intruziune, de tip “Next Generation IPS”;

- implementează protecția activă anti-intruziune, în mod transparent pentru traficul legitim, la intrarea în subsistemul pe care îl deservește, și asigură protecția antimalware a acestuia, în caz de atacuri cu vectori de propagare activi la nivel de rețea;
- implementează funcționalități de tip *“sand-boxing”* pentru decelarea acțiunii codului activ de tip malware avansat (APT) și *“0-day”*, iar analiza încărcăturilor suspecte se va asigura local — *“on-premise”*, fără a fi nevoie de acces la servicii de tip *“cloud”*;
- actualizarea cataloagelor specifice antimalware și a bazelor de date de tip reputațional (*“cyberthreat feeds”*) se va putea face în mod offline, pe interfețele dedicate de management.

1.6.2 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x echipament hardware de tip *“Next Generation IPS”* (NGIPS);
- fiecare echipament de tip NGIPS va fi echipat și configurat pentru a asigura cel puțin următoarele capabilități:
 - capabilitatea de extindere, prin adăugare de componente modulare dedicate a numărului și tipului de porturi suportate, cel puțin pentru porturi 10Gbps și 40Gbps;
 - 8 Gbps throughput, în regim de procesare IPS, cu funcțiile de standard de protecție anti-intruziune activate;
 - 8 porturi modulare de 10Gbps Ethernet, echipate cu interfețe optice de tip SFP+ (short-range);
 - interfața de management *“out-of-band”*;
 - 1x 200GB SSD intern;
 - surse de alimentare și ventilatoare redundante;
- fiecare echipament de tip NGIPS va permite monitorizarea și protejarea pentru cel puțin o interconectare dual-redundantă, respectiv pentru o pereche de echipamente ADC legate dual, prin conexiuni 10Gbps Ethernet, la o pereche de echipamente Switch Ethernet (Tip 1);
- se va asigura echiparea și licențierea (acolo unde este cazul) pentru un minim de 2Gbps de trafic efectiv (valori medii susținute), agregat pe conexiunile cu încapsulare 10Gbps Ethernet protejate;

- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN;
- configurația va include subscripțiile de acces la actualizările de cataloage de referință de tip *“threat intelligence”* și de tip reputațional, pe perioada asumată prin contract.

1.7 Complete hardware de tip Diodă de Date - (7 pachete)

1.7.1 Rol și context

- implementează tehnologie de control activ al comunicației unidirecționale, prin componenta centrală (hardware) de tip Data Diode (Diodă de Date) și separă tehnic subsistemele între care facilitează transferul de informație, respectiv expune interfețe de servicii dedicate (de tip proxy) către fiecare subsistem..
- soluția va fi certificată Common Criteria, la nivel minim CC EAL 7, cel puțin pentru componentele centrale hardware de tip Diodă de Date.

1.7.2 Configurație și dimensionare

7x pachete, integrate hardware/software

- fiecare pachet va include 2x echipamente hardware dedicate de tip Diodă de Date;
- fiecare pachet va include 4x echipamente de tip server appliance de tip proxy, dispuse câte 1x de fiecare parte a fiecărui echipament de tip Diodă de Date;
- fiecare pachet va fi echipat și configurat în mod redundant pentru a nu avea componente interne de tip single-point-of-failure;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.8 Echipamente de tip Next Generation Firewall

1.8.1 Echipamente de tip Next Generation Firewall (Tip 1) - (1 pachet)

1.8.1.1 Rol și context:

- implementează segmentarea rețelelor protejate ale Componentei de Acces, și asigură protecția acestora față de atacurile la nivel de rețea.

1.8.1.2 Cerințe funcționale și specificații tehnice

- implementează cel puțin mecanisme de protecție la nivel de rețea (filtru de pachete), firewall de aplicație, mecanisme anti-intruziune (IPS) integrate, filtru antimalware, filtrare de adrese URL, identificare de utilizator și de terminal;
- va asigura separarea la nivel hardware a nivelului de comunicații și a celui de control, iar actualizarea cataloagelor specifice antimalware și a bazelor de date de tip reputațional (“*cyberthreat feeds*”) se va putea face în mod offline, pe interfețele dedicate de management;
- soluția suportă configurații de tip cluster activ-activ și activ-pasiv, și va putea fi implementată configurabil, la nivel de layer 2, de layer 3 sau în mod transparent față de contextul de comunicații, în care caz va putea asigura segmentarea de securitate fără a necesita și segmentarea suplimentară în rețele și sub-rețele.

1.8.1.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x cluster de echipamente hardware de tip “*Next Generation Firewall*” (NGFW);
- fiecare cluster va include 2x echipamente NGFW (Tip 1);
- fiecare echipament de tip NGFW (Tip 1) va asigura cel puțin următoarele capabilitati:
 - 8 Gbps throughput de baza, în mod firewall de aplicații;
 - 4 Gbps throughput, în condiții de activare concurentă a filtrelor anti-intruziune și antimalware;
 - până la 2,000,000 de sesiuni susținute, în condiții de trafic normal și în condiții de atac;
 - respectiv cu până la 100,000 noi sesiuni deschise, per second;
 - susținerea traficului pentru 10,000 utilizatori SSL VPN concurenți;

- posibilitatea de creare și de utilizare a 100 instanțe virtuale de tip router;
 - posibilitatea de creare și de utilizare a 25 partiții interne administrativ independente;
 - definirea și gestionarea a 500 zone de securitate;
 - definirea și aplicarea a 20,000 politici;
 - interfața de management *“out-of-band”*;
 - 4 interfețe de 1Gbps, pentru trafic, cu conectorizare RJ45;
 - 8 porturi de 1Gbps, pentru trafic, echipate cu module optice de tip SFP (*“short range”*);
 - 4 interfețe de 10Gbps, pentru trafic, echipate cu module optice de tip SFP+ (*“short range”*);
 - 2x 200GB SSD intern;
 - surse de alimentare redundante;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN;
 - configurația va include subscripțiile de acces la actualizările de cataloage de referință de tip *“threat intelligence”* și de tip reputațional, pe perioada asumată prin contract.

1.8.2 Echipamente de tip Next Generation Firewall (Tip 2) - (1 pachet)

1.8.2.1 Rol și context

- implementează segmentarea rețelelor protejate ale Componentei de Acces, și asigură protecția acestora față de atacurile la nivel de rețea.

1.8.2.2 Cerințe funcționale și specificații tehnice

- implementează cel puțin mecanisme de protecție la nivel de rețea (filtru de pachete), firewall de aplicație, mecanisme anti-intruziune (IPS) integrate, filtru antimalware, filtrare de adrese URL, identificare de utilizator și de terminal;
- va asigura separarea la nivel hardware a nivelului de comunicații și a celui de control, iar actualizarea cataloagelor specifice antimalware și a bazelor de date de tip reputațional (*“cyberthreat-feeds”*) se va putea face în mod offline, pe interfețele dedicate de management;

- soluția suportă configurații de tip cluster activ-activ și activ-pasiv, și va putea fi implementată configurabil, la nivel de layer 2, de layer 3 sau în mod transparent față de contextul de comunicații, în care caz va putea asigura segmentarea de securitate fără a necesita și segmentarea suplimentară în rețele și sub-rețele.

1.8.2.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x cluster de echipamente hardware de tip Next Generation Firewall (NGFW);
- fiecare cluster va include 2x echipamente NGFW (Tip 2);
- fiecare echipament de tip NGFW (Tip 2) va asigura cel puțin următoarele capabilitati:
 - 4 Gbps throughput de baza, în mod firewall de aplicații;
 - 2 Gbps throughput, în condiții de activare concurentă a filtrelor anti-intruziune și antimalware;
 - până la 500,000 de sesiuni sustinute, în condiții de trafic normal și în condiții de atac;
 - respectiv cu până la 50,000 noi sesiuni deschise, per second;
 - susținerea traficului pentru 2,000 utilizatori SSL VPN concurenți;
 - posibilitatea de creare și de utilizare a 10 instanțe virtuale de tip router;
 - posibilitatea de creare și de utilizare a 5 partitii interne administrativ independente;
 - definirea și gestionarea a 25 zone de securitate;
 - definirea și aplicarea a 5,000 politici;
 - interfața de management out-of-band;
 - 4 interfețe de 1Gbps, pentru trafic, cu conectorizare RJ45;
 - 8 porturi de 1Gbps, pentru trafic, echipate cu module optice de tip SFP (short range);
 - 2 interfețe de 10Gbps, pentru trafic, echipate cu module optice de tip SFP+ (short range);
 - 1x 100GB SSD intern;
 - surse de alimentare redundante;

- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN;
- configurația va include subscripțiile de acces la actualizările de cataloage de referință de tip *“threat intelligence”* și de tip reputațional, pe perioada asumată prin contract.

1.9 Echipamente de tip DNS Server/DNS Firewall - (1 pachet)

1.9.1 Rol și context

- asigură susținerea tranzacțională a serviciilor de tip *“Domain Name Service”* (DNS), de translație între adresele Internet și descriptorii simbolici calificați de tip *“Fullz Qualified Domain Name”* (FQDN), sau derivați, ai punctelor de acces la servicii, precum și protecția acestora împotriva atacurilor specifice.

1.9.2 Cerințe funcționale și specificații tehnice

- sistemul de suport tranzacțional și de protecție a serviciilor de DNS (de tip DNS firewall) trebuie să fie capabil să asigure cel puțin următoarele funcționalități generale:
 - protecție împotriva atacurilor de tip DoS/DDoS la nivel de rețea sau la nivel de serviciu (cel puțin de tip: inclusiv UDP packet floods, fragment floods);
 - protecție împotriva atacurilor, inclusiv de tip DoS/DDoS, care exploatează vulnerabilități specifice serviciului DNS (cel puțin de tip: query floods, nxdomain floods, zone transfer requests, invalid requests);
 - posibilitatea de a certifica modificările sau actualizările, precum și de a proteja zonele DNS deservite folosind tehnologii, arhitecturi și protocoale specifice (inclusiv DNSSEC);
 - suport pentru operarea infrastructurii de serviciu în mod dual-stack (IPv4 și IPv6);
 - performanță tranzacțională superioară (inclusiv suport pentru concurențialitate ridicată și timp de răspuns specific foarte redus/liniar) față de implementarea tradițională pe bază de servere standalone de tip de DNS;
 - posibilitatea de a asigura serviciile de DNS într-un mod inteligent ce ține cont de arhitectura infrastructurii de aplicații, logica de interconectare a componentelor

acesteia, configurația echipamentelor de procesare, nivelul de încărcare a serverelor de aplicații sau chiar de tipul/profilul și locația utilizatorului.

1.9.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x cluster de echipamente hardware de tip DNS Server / DNS Firewall;
- fiecare cluster va include 2x echipamente DNS Server / DNS Firewall;
- fiecare echipament DNS Server / DNS Firewall va fi configurat și echipat pentru a asigura cel puțin:
 - 4Gbps throughput, în regim de procesare generală L4/L7;
 - 4Gbps compresie hardware internă integrată;
 - 4Gbps procesare criptografică hardware internă integrată;
 - 4000 tranzacții pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
 - până la 100,000 noi sesiuni L4 deschise, pe secundă;
 - 8x porturi 10/100/1000Mbps Ethernet RJ45;
 - 2x porturi 10Gbps Ethernet SFP+;
 - 1x 100GB HDD sau SSD;
 - 2x surse de alimentare interne, în configurație redundantă;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.10 Echipamente de tip Application Delivery Controller - (1 pachet)

1.10.1 Rol și context

- "reverse proxy", de tip "Application Delivery Controller" (ADC), cu funcții de firewall de layer 3, "Load-Balancer" și "Web Application Firewall" (WAF);
- va fi configurabil în mod bastion-host, cu servicii de firewall de layer 3, fără a avea nevoie de alt echipament de tip firewall în fața sa;

- implementează o arhitectura hardware dedicată, inclusiv procesarea criptografică și compresia, care asigură integritatea procesării, latență specifică redusă, și care suportă tranzaționalitate ridicată în condiții de deservire cu impact liniar, inclusiv la nivel de vârf de sarcină, a apelurilor autorizate de acces la resurse;
- va putea funcționa ca proxy hardware permanent, putând fi configurat pentru funcționare strictă în mod “*reverse proxy*” și va integra funcționalități hardware de protecție împotriva atacurilor de tip DDoS;
- va putea fi configurat atât “*service provider*”, cât și ca “*identity provider*” — inclusiv pentru interoperabilitate SAML2 — și va putea acționa direct ca “*enforcement point*” (manager de autorizare) compatibil cu infrastructura de management al identității existentă, aflată în exploatarea beneficiarului.

1.10.2 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x cluster de echipamente hardware de tip “*Application Delivery Controller*” (ADC);
- fiecare cluster va include 2x echipamente ADC;
- fiecare echipament ADC va fi configurat și echipat pentru a asigura cel puțin cu:
 - suport asigurat și licențiat (acolo unde este cazul) pentru cel puțin 750 utilizatori concurenți;
 - 32Gbps throughput, în regim de procesare generală L4;
 - 16Gbps throughput, în regim de procesare generală L7;
 - 16Gbps compresie hardware internă integrată;
 - 16Gbps procesare criptografică hardware internă integrată;
 - 16000 tranzații pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
 - procesarea de trafic până la cel puțin 4M noi conexiuni L4 HTTP deschise pe secundă;
 - procesarea de trafic până la cel puțin 1M noi conexiuni L7 deschise pe secundă;
 - 2x 400GB SSD;
 - 4x porturi 10/100/1000Mbps Ethernet RJ45;
 - 8x porturi 10Gbps Ethernet SFP+;

- 2x surse de alimentare interne, în configurație redundantă;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN;
- configurația va include subscripțiile de acces la actualizările de cataloage de referință de tip *“threat intelligence”* și de tip reputațional, pe perioada asumată prin contract.

1.11 Echipamente de tip Secure Web Gateway - (1 pachet)

1.11.1 Rol și context

- gateway Web de tip *“forward proxy”*, cu funcții de autentificare a utilizatorilor interni și de protecție a accesului autorizat la rețele externe prin mecanisme de validare a protocoalelor de rețea permise, precum și prin aplicarea de filtre antimalware și prin filtrarea de adrese URL.

1.11.2 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x cluster de echipamente hardware de tip Secure Web Gateway (SWG);
- fiecare cluster va include 2x echipamente SWG;
- fiecare echipament SWG va fi configurat și echipat pentru a asigura cel puțin cu:
 - suport asigurat și licențiat (acolo unde este cazul) pentru cel puțin 100 utilizatori concurenți;
 - 4Gbps throughput, în regim de procesare generală L4/L7;
 - 4Gbps compresie hardware internă integrată;
 - 4Gbps procesare criptografică hardware internă integrată;
 - 4000 tranzacții pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
 - până la 100,000 noi sesiuni L4 deschise, pe secundă;
 - 1x 400GB HDD sau SSD;
 - 4x porturi 10/100/1000Mbps Ethernet RJ45;

- 2x porturi 10Gbps Ethernet SFP+;
- 2x surse de alimentare interne, în configurație redundantă;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.12 Echipamentele de tip Gateway WS/API - (2 pachete)

1.12.1 Rol și context

- implementează o arhitectura de tip proxy de servicii web — de tip Web Services (WS) — și de medii de acces programatic neasistat la serviciile de aplicație — de tip *"Application Programming Interface"* (API) —, cu capabilitati de transformare de date *"on-the-fly"* și de integrare de servicii (*"front-end to back-end"*, și reciproc);
- implementează servicii de tip WS/API firewall, inclusiv cu funcții native (*"on-device"*) de detecție și de tratare a prezenței de sarcină activă de tip malware injectată la nivel de protocol și de *"payload"* (inclusiv antivirus/antimalware, anti-intruziune, și de protecție împotriva scurgerii de informație);
- funcțiile de control al accesului vor include suport pentru politici de acces bazate pe modele bazate pe roluri (de tip RBAC) și pe attribute (de tip ABAC), precum și pentru politici bazate pe inspecția și validarea de date;
- funcțiile de tip Single-Sign-On vor include cel puțin suport pentru SAML, OAuth, SSO fără agent;
- funcțiile native de integrare securizată vor acoperi cel puțin transformările de tip *"REST-to-SOAP"*, transformarea de protocoale și utilizare de mix de protocoale, extragere și asociere de attribute (între serviciile conectate, respectiv în front-end și în back-end).
- soluția va fi certificată FIPS 140-2, cel puțin pentru componentele hardware de procesare criptografică.

1.12.2 Configurație și dimensionare

2x pachete, integrate hardware/software

- fiecare pachet va include 1x cluster de echipamente hardware de tip Gateway pentru servicii web (WS) și pentru acces la nivel de interfață programabilă (API);

- fiecare cluster va include 2x echipamente Gateway WS/API;
- Fiecare echipament va dispune de 2x interfețe de 1Gbps, pentru trafic, cu conectare RJ45;
- vor fi incluse toate rețerele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.13 Soluția de asigurare a serviciilor criptografice centralizate - (3 pachete)

1.13.1 Rol și context

- instanța server care expune interfața de tip Web Services (WS) sau API, pentru generarea de semnături electronice asociate setului de date generate în răspuns la cererile autorizate, în scopul certificării autenticității răspunsului;
- datele generate, în răspuns la fiecare cerere, vor fi criptate cu cheile publice ale solicitantului și ale instanțelor de audit din subsistemul Replication, pentru a asigura ca datele nu vor fi disponibile în clar fără autorizare prealabilă la nivelul sistemelor și rețelelor deschise, respectiv ca numai beneficiarul autorizat și mecanismele interne de control împotriva scurgerilor de informații vor avea acces la date în clar;
- operațiunile de semnare electronică se vor efectua exclusiv la nivelul componentei de asigurare a serviciilor criptografice, iar protecția cheilor private și accelerarea procesărilor criptografice se vor asigura pe baza de componente hardware de tip HSM certificate FIPS 140-2.

1.13.2 Cerințe funcționale și specificații tehnice

- soluția va permite instanțierea de autorități de emisie și de validare de certificate digitale, inclusiv pe bază de perechi de chei publice și private de până la 4096 bit;
- soluția va fi dimensionată și licențiată pentru implementarea unei infrastructuri PKI multi-nivel (care va include entități de *“policy CA”* și *“issuing CA”*), destinată asigurării suportului pentru accesul securizat în condiții de mobilitate, și care va include cel puțin 3 instanțe de tip CA și una de tip VA (autoritate de validare a stării certificatelor).

1.13.3 Configurație și dimensionare

3x pachete, integrate hardware/software

- fiecare pachet va include 1x cluster format din 2x noduri de tip *"appliance"*, fizic sau virtual;
- fiecare nod va dispune de un echipament hardware de tip HSM în format PCIe și va expune servicii criptografice centralizate (generare de cheie și procesare de algoritmi criptografici), accesibile prin interfețe de tip WS/API fără restricție de număr de identități de sistem sau de utilizator certificate deservite, și fără restricție de număr de tranzacții prelucrate;
- vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.14 Componente de tip Server

Echipamentele de tip Server sunt parte componentă a infrastructurii de stocare și procesare virtualizată.

1.14.1 Componente de tip Server (Tip 1) - (12 buc.)

1.14.1.1 Rol și context

- echipamentele server (Tip 1) vor rula nativ instanțe ale soluției de virtualizare și vor fi grupate în perechi pentru a susține procesarea componentelor arhitecturii funcționale a Componentei de Acces, cu excepția celor de la nivel CORE (offline);
- subsistemele funcționale al Componentei de Acces nu vor partaja aceeași pereche de echipamente server (Tip 1), cu excepția subsistemului de logică de aplicație și a subsistemului de management al datelor, care vor putea utiliza în comun aceeași pereche.

1.14.1.2 Configurație și dimensionare

12x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament hardware server (Tip 1);
- fiecare server (Tip 1) va fi configurat și echipat cel puțin cu:

- 2 procesoare fizice Intel Xeon E5 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 512GB RAM DDR3 sau DDR4;
 - 2x 32GB medii de stocare locale, amovibile, pentru instalarea hypervisorului;
 - 1TB Flash PCIe card;
 - 4x 10Gbps CNA cu interfețe modulare, echipate cu transceiver optic SFP+ (short-range);
 - 1x 12Gbps SATA RAID card cu 4GB cache;
 - 8x 400GB 2.5in / 6Gbps SATA / Enterprise Performance SSD;
 - 2x surse interne de alimentare redundante;
 - 2x unități interne de răcire / ventilare redundante;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.14.2 Componente de tip Server (Tip 2) - (4 buc.)

1.14.2.1 Rol și context

- echipamentele server (Tip 2) vor rula nativ instanțe ale soluției de virtualizare și vor fi grupate în perechi pentru a susține procesarea componentelor arhitecturii funcționale a Componentei de Acces, la nivel CORE (offline).

1.14.2.2 Configurație și dimensionare

4x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament hardware server (Tip 2);
- fiecare server (Tip 2) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E5 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 512GB RAM DDR3 sau DDR4;
 - 2x 32GB medii de stocare locale, amovibile, pentru instalarea hypervisorului;
 - 1TB Flash PCIe card;

- 2x 40Gbps CNA cu interfețe modulare, echipate cu transceiver optic QSFP (short-range);
- 1x 12Gbps SATA RAID card cu 4GB cache;
- 8x 400GB 2.5in / 6Gbps SATA / Enterprise Performance SSD;
- 2x surse interne de alimentare redundante;
- 2x unități interne de răcire / ventilare redundante;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN

1.14.3 Componente de tip Server (Tip 3) - (4 buc.)

1.14.3.1 Rol și context

- echipamentele server (Tip 3) vor rula nativ instanțe ale soluției de virtualizare și vor fi grupate în perechi pentru a susține procesarea componentelor de monitorizare și management “*out-of-band*” ale Componentei de Acces.

1.14.3.2 Configurație și dimensionare

4x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament hardware server (Tip 3);
- fiecare server (Tip 3) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E5 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 256GB RAM DDR3 sau DDR4;
 - 2x 32GB medii de stocare locale, amovibile, pentru instalarea hypervisorului;
 - 1TB Flash PCIe card;
 - 4x 10Gbps CNA cu interfețe modulare, echipate cu transceiver optic SFP+ (short-range);
 - 1x 12Gbps SATA RAID card cu 4GB cache;
 - 8x 400GB 2.5in / 6Gbps SATA / Enterprise Performance SSD;
 - 16x 600GB 2.5in / 6Gbps SATA / 15K rpm / Enterprise Performance HDD;
 - 2x surse interne de alimentare redundante;

- 2x unități interne de răcire / ventilare redundante;
- vor fi incluse toate reперele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.14.4 Componente de tip Server (Tip 4) - (2 buc.)

1.14.4.1 Rol și context

- echipamentele server (Tip 4) vor rula nativ instanțe de tip server (instalate nativ sau virtualizate), care vor fi grupate în perechi pentru a susține procesarea instanțelor active de management și de tip concentrator ale soluției de tip VPN pentru terminale mobile, care se va integra în subsistemul de management al mobilității, la nivel EDGE (online).

1.14.4.2 Configurație și dimensionare

2x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament hardware server (Tip 4);
- fiecare server (Tip 4) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E5 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 64GB RAM DDR3 sau DDR4;
 - 2x 32GB medii de stocare locale, amovibile, pentru instalarea hypervisorului;
 - 4x 1Gbps Ethernet cu interfețe RJ45;
 - 2x 10Gbps Ethernet cu interfețe modulare, echipate cu transceiver optic SFP+ (short-range) 1x 12Gbps SATA RAID card cu 4GB cache;
 - 2x 400GB 2.5in / 6Gbps SATA / Enterprise Performance SSD;
 - 6x 600GB 2.5in / 6Gbps SATA / 15K rpm / Enterprise Performance HDD;
 - 2x surse interne de alimentare redundante;
 - 2x unități interne de răcire / ventilare redundante;
- vor fi incluse toate reперele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN.

1.15 Licență - Suita de tip Enterprise Mobility Management (EMM) - (750 buc.)

1.15.1 Rol și context

- la acest nivel se regăsesc instalate componentele client de tip *“Mobile Device Management”* (MDM) și *“Mobile Application Management”* (MAM) ale suitei de tip *“Enterprise Mobility Management”* (EMM).

1.15.2 Cerințe funcționale și specificații tehnice

- componentele client ale suitei EMM, vor implementa *“off-the-shelf”* cel puțin următoarele funcții de tip MDM:

- configurare dispozitiv;
- resetare securizată (*“secure wipe”*), la nivel de dispozitiv;
- resetare securizată de credențiale de acces, la nivel de dispozitiv;
- detecția condițiilor de tip *“jailbreak/root”* și aplicarea de contramăsuri specifice;
- detecția încălcării altor politici, configurabile centralizat, de utilizare a dispozitivului;

- componentele client ale suitei EMM, vor implementa *“off-the-shelf”* cel puțin următoarele funcții de tip MAM:

- configurare centralizată, la nivel de aplicații specifice controlate;
- configurare centralizată de politici de utilizare a aplicațiilor controlate;
- resetare securizată (*“secure wipe”*) a datelor și/sau a profilelor de utilizare a aplicațiilor;
- resetare securizată de credențiale de acces la nivel de aplicație;
- administrare a mediului protejat de executare a aplicațiilor controlate pe bază de roluri;

- componentele client ale suitei EMM, vor implementa *“off-the-shelf”* cel puțin următoarele funcții avansate de tip MAM:

- aplicație unificată, controlată, de tip client de servicii de colaborare (cel puțin calendar, agendă de contacte și calendar partajat);
- browser securizat, care va rula exclusiv în mediu protejat, odată asociat terminalul cu sistemele centrale de configurare și control;

- mecanisme de preluare în control și de protejare specifice (*“wrapping”*) pentru aplicațiile terțe, precum și — în general — a aplicațiilor dezvoltate *“in-house”*;
- mecanisme de tip *“Software Development Kit”* (SDK) pentru containerizare de aplicații, inclusiv API-uri de extindere accesului controlat la funcții externe;
- mediu de publicare a aplicațiilor, de tip *“enterprise app store”*, customizabil și mecanism unificat de lansare a aplicațiilor pe terminalul controlat;
- componentele client ale suitei EMM, vor implementa *“off-the-shelf”* cel puțin următoarele funcții de securitate:
 - procesare criptografică independentă de serviciile oferite de sistemul de operare și/sau de aplicații terțe, în implementare certificată FIPS 140-2;
 - protecția, inclusiv prin mecanisme criptografice (inclusiv prin implementarea de algoritmi standard precum AES 256 și/sau curbe ECC), a datelor stocate, aflate în utilizare sau transmise pe canalele de comunicații;
 - integrare cu medii de management al identității și al politicilor de acces la resurse;
- suport pentru o varietate de sisteme de operare client, inclusiv pentru Apple iOS, Microsoft Windows Phone și diverse distribuții Android.

1.15.3 Configurație și dimensionare

750x bucăți de licențe software

- fiecare bucată va include câte 1x licență EMM, iar fiecare licență va acoperi utilizarea soluției de către 1x utilizator unic, de pe cel puțin 1x terminal mobil inteligent;
- este considerată echivalentă varianta în care, datorită specificului licențierii producătorului respectiv, se va oferta cel puțin 1x complet care va include licențiere dimensionată pentru utilizarea soluției de către 750x utilizatori unici;
- licențierea va include implicit și instanțele funcționale centrale de tip *“reverse proxy”* pentru accesul mobil, pentru asigurarea funcționalităților centralizate de control al accesului mobil, precum și pentru asigurarea funcționalităților de legătură (*“relay”*) cu serviciile interne de mesagerie colaborativă structurată, în scenariul care comportă instalarea și exploatarea soluției de tip EMM on-site (*“on-premise”*) la beneficiar;

- configurația va permite extinderea ulterioară a licențelor și va include garanția pentru dreptul de utilizare software, precum și serviciile de mentenanță și de suport tehnic pe perioada asumată prin contract.

1.16 Licență - Componentă de tipVPN pentru terminale mobile - (750 buc.)

1.16.1 Rol și context

Reunește componentele client și server de tip VPN pentru aplicații mobile, care vor asigura o anvelopă de protecție, independentă de funcționalitățile de tip MAM ale suitei EMM și de sistemul de operare la terminalele mobile inteligente la nivelul fiecărui terminal.

Va asigura protecția datelor transmise pe canalele de comunicații prin metode criptografice, inclusiv prin implementarea de algoritmi standard precum AES 256 și/sau curbe ECC.

1.16.2 Configurație și dimensionare

750x bucăți licențe software

- fiecare bucată va include câte 1x licență VPN, iar fiecare licență va acoperi utilizarea soluției de către 1x utilizator unic, de pe cel puțin 1x terminal mobil inteligent;
- este considerată echivalentă varianta în care, datorită specificului licențierii producătorului respectiv, se va oferta cel puțin 1x complet care va include licențiere dimensionată pentru utilizarea soluției de către 750x utilizatori unici.

1.17 Licență platformă de virtualizare – componenta de acces securizat în condiții de mobilitate - 20 pachete

1.17.1 Soluție de virtualizare - (20 buc.)

1.17.1.1 Rol și context

- soluția de virtualizare va putea fi instalată pe tipurile de servere ale Componentei de Acces, pentru a asigura abstractizarea infrastructurii hardware față de mașinile virtuale configurate, respectiv pentru a reduce dependența, în exploatare, a instanțelor funcționale virtualizate de starea echipamentelor hardware, precum și pentru a implementa

funcționalitățile de management (inclusiv pe cele de asigurare a disponibilității operaționale) și de securitate la acest nivel.

1.17.1.2 Cerințe funcționale și specificații tehnice

- virtualizare sistem bazată pe hypervisor de Tip 1 (*“bare-iron”*) sau echivalent, optimizat pentru platforme de clasă server;
- management integrat, pentru configurații scalabile eterogene (de tip multi-nod, multi-hypervisor, multi-instanță) al nivelului virtualizare;
- soluția va oferi un mediu intern de comunicație de rețea integrat, distribuit între toate serverele interconectate care rulează instanțe hypervisor administrate de același centru de management;
- soluția va asigura posibilitatea de configurare a relocării dinamice automate a instanțelor de mașini virtuale, între serverele care rulează instanțe hypervisor administrate de același centru de management, în funcție de indicatori de stare, de încărcare sau de disponibilitate;
- soluția va asigura monitorizarea și administrarea alocării și utilizării resurselor disponibile, cel puțin în ceea ce privește:
 - identificarea și limitarea utilizării de resurse de stocare și de procesare, de către mașinile virtuale, pe bază de politici;
 - identificarea consumului de resurse specifice, la nivel de mașină virtuală și, respectiv, pe categorii de resurse;
 - identificarea de resurse, inclusiv de tip RAM și procesor, ne-alocate sau supra-rezervate, pentru a permite optimizarea alocării acestora;
 - corelarea schimbărilor de configurație, la nivelul sistemelor virtualizate, cu impactul acestora asupra nivelului de utilizare a resurselor;
 - urmărirea evoluției nivelului de utilizare a resurselor și semnalizarea situațiilor de depășire a limitelor de capacitate;
 - asigurarea disponibilității operaționale a mașinilor virtuale și *“load-balancing”*, pe bază de politici, între instanțele de hypervisor (*“hypervisor host”*);
 - reconfigurarea, realocarea și migrarea mașinilor și a discurilor virtuale, pentru a optimiza performanța acestora și utilizarea resurselor hardware alocate;

- soluția va asigura funcționalități integrate de tip “*Software Defined Network*” (SDN), “*Software Defined Storage*” (SDS) și mecanisme integrate de “*host provisioning*”;
- funcționalitățile de tip SDS vor fi independente de echipamentele hardware de tip server pe care rulează, vor fi independente de suportul funcțional de stocare (de tip HDD, sau SSD/Flash) și se vor integra cu platforma de virtualizare;
- funcționalitățile de tip SDS vor crea o arhitectură hiperconvergentă, scalabilă și elastică, cel puțin în sensul că va permite adăugarea de noduri de tip server și, respectiv, de capacitate de stocare pe acestea, fără întreruperea serviciului;
- componenta funcțională de tip SDS va asigura procesarea paralelă a cererilor de I/O, cu echilibrarea automată a sarcinii de lucru între nodurile implicate, protecția datelor prin replicarea/distribuirea acestora între mai multe noduri de tip server, respectiv refacerea automată a disponibilității datelor în cazul căderii unui nod de tip server;
- componenta funcțională de tip SDS va permite:
 - definirea și, în funcție de necesități, izolarea de domenii de stocare, la nivel de server și la nivel de set de date;
 - asocierea de resurse de stocare (“*storage-pools*”) în funcție de performanță, pentru optimizarea stocării (mecanisme de tip “*storage tiering*”);
 - definirea de politici de acces, de tip QoS, inclusiv limitarea sau garantarea nivelului de performanță de acces (IOPS) asigurat, la nivel de aplicație deservită;
 - crearea de copii de siguranță editabile, de tip snapshot, care vor putea fi utilizate ca stări stabile (de tip “*consistency points*” - puncte de coerență) pentru backup;
 - mecanisme de tip portal de self-service, cu sistem integrat de acces la resurse pe bază de roluri și cu posibilitatea de definire de limite (cote);
- platforma de virtualizare va permite managementul și optimizarea alocării de resurse partajate, cel puțin la nivel de RAM și de discuri, respectiv:
 - posibilitatea de partajare granulară, la nivel de unitate de alocare, între mașinile virtuale definite;
 - posibilitatea de supra-alocare logică flexibilă, peste limitele nominale ale echipamentului hardware;

- interfața de management va permite controlul și automatizarea configurării, operării și migrării de componente, respectiv pentru mașinile virtuale și pentru infrastructurile virtuale;
- soluția oferită va asigura accesarea și automatizarea utilizării tuturor comenzilor de management ale platformei de virtualizare prin interfețe de control API.

1.17.1.3 Configurație și dimensionare

20x bucați licențe software

- fiecare bucată va include câte 1x licență, iar fiecare licență va acoperi instalarea soluției de virtualizare pe un echipament hardware de tip server dual-socket, cu procesoare de tip x86_64;
- este considerată echivalentă varianta în care, datorită specificului licențierii producătorului respectiv, se va oferta cel puțin 1x complet care va include licențiere dimensionată pentru instalarea soluției de virtualizare pe cel puțin 20 de echipamente hardware de tip “server dual-socket”, cu procesoare de tip x86_64;
- licențierea va include și cel puțin 6 instanțe de tip consolă de management pentru soluția de virtualizare.

1.17.2 Sisteme de operare - (20 buc.)

1.17.2.1 Rol și context

- soluția software de tip sistem de operare va putea fi instalată pe tipurile de servere ale Componenta de Acces, precum și la nivelul instanțelor de mașini virtuale configurate, pentru a asigura abstractizarea infrastructurii hardware față de infrastructura software de aplicație (SGBD, middleware), precum și pentru a implementa funcționalitățile de management și de securitate la acest nivel.

1.17.2.2 Configurație și dimensionare

20x bucați licențe software

- fiecare bucată va include câte 1x licență, iar fiecare licență va acoperi o instanță software pentru sistem de operare de tip server, respectiv instalată pe echipament hardware de tip “server dual-socket”, cu procesoare de tip x86_64, sau pe sistem virtual echivalente;
- este considerată echivalentă varianta în care, datorită specificului licențierii producătorului respectiv, se va oferta cel puțin 1x complet care va include licențiere

dimensionată pentru cel puțin 20 de instanțe software de tip sistem de operare pentru server, care vor fi respectiv instalate pe echipamente hardware de tip “*server dual-socket*”, cu procesoare de tip x86_64, sau pe sisteme virtuale echivalente.

1.18 Servicii de instalare și configurare infrastructură - componentă acces securizat în condiții de mobilitate - (1 serviciu)

Serviciul de instalare și configurare al infrastructurii Componentei de Acces este strâns legat de arhitectura conceptuală a acesteia. Pentru realizarea serviciului se vor desfășura următoarele activități:

- livrarea licențelor necesare punerii în funcțiune a Componentei de Acces și instalarea acestora;
- instalarea și configurarea tuturor echipamentelor hardware (menționate în secțiunile 1.1 – 1.14) și produselor software (menționate în secțiunile 1.15 – 1.17).
- pentru a asigura funcționarea optimă a sistemului integrat rezultat, alegerea tipului și a calității componentelor pasive de interconectare (inclusiv cabluri electrice și fibre optice, terminarea acestora și reperatele pasive de tip patch-panel sau cross-connect necesare), respectiv conectorizarea activă a porturilor (inclusiv tipul și performanțele specifice ale modulelor de tip transceiver optic sau electric) din echipamentele astfel interconectate, vor avea în vedere corespondența între porturi.

1.19 Servicii de implementare – componentă de acces securizat în condiții de mobilitate - (1 serviciu)

1.19.1 Cerințe generale

Utilizatorii vor solicita accesul la resursele interne protejate de la nivelul terminalelor mobile inteligente (de tip smartphone sau tabletă) aflate în dotare, conectate la rețelele deschise de comunicații mobile de voce și date, și care sunt înrolate în sistemul de protecție de tip “*Mobile Device Management*” (MDM).

Inițierea accesului la resursele interne protejate se va face prin instrumente integrate la nivelul aplicațiilor mobile — inclusiv instanțe de tip browser web, aplicații de tip HTML5 sau aplicații native — înrolate în sistemul de protecție de tip “*Mobile Application Management*” (MAM).

Funcționalitățile de management al mobilității, inclusiv cele de tip MDM și MAM, precum și cele de comunicare colaborativă online între utilizatorii autorizați, respectiv prin aplicații mobile specifice de pe terminalele mobile inteligente înrolate, vor fi integrate în nivelul EDGE (online) al Componentei de Acces.

Resursele interne protejate la care accesul va fi autorizat vor fi făcute disponibile numai pe terminale mobile autorizate, numai pentru utilizatorii autorizați, exclusiv pe baza solicitării explicite a accesului și numai în urma autorizării explicite a acestuia.

Datele la care s-a autorizat accesul vor fi efectiv disponibile pe terminalele mobile inteligente — precum și la nivelul Componentei de Acces — numai pe durata autorizată, vor fi primite și stocate pe terminal numai în formă criptată și vor putea fi accesate în clar numai de către utilizatorul autorizat.

La nivel central și la nivelul terminalului mobil inteligent pe care se autorizează accesul, resursele tehnice implicate vor putea asigura distrugerea automată a datelor furnizate la expirarea termenului de acces autorizat sau chiar înainte de expirare, în cazul revocării autorizării.

Funcționalitățile care vor mijloci accesul controlat, în regim de mobilitate, la datele și la serviciile interne protejate vor fi integrate în nivelul BUFFER (online).

Funcționalitățile care vor asigura etajul de autorizare a accesului și pe cel de control independent al furnizării datelor către resursele online, inclusiv către nivelul BUFFER (online) și, prin intermediul acestuia, către terminalele mobile inteligente autorizate, vor fi integrate în nivelul de CONTROL (offline).

La nivelul rețelei interne sursă, resursele tehnice dedicate ale Componentei de Acces vor fi integrate în nivelul funcțional CORE (offline) al acesteia și vor interacționa direct cu sursele de date existente și cu serviciile de aplicație prin intermediul componentelor de analiză avansată.

Resursele de date și serviciile de aplicație protejate vor fi rezidente în rețele interne offline, care nu vor putea fi interconectate la rețele deschise prin mijloace tehnice de comunicație bidirecțională de uz general.

Resursele tehnice ale Componentei de Acces care vor fi desemnate ca fiind online, inclusiv cele din nivelul EDGE (online) și din nivelul BUFFER (online), nu vor putea fi interconectate cu resursele desemnate ca fiind offline, inclusiv cu cele din nivelul CONTROL (offline) și din nivelul CORE (offline), prin mijloace tehnice de comunicație bidirecțională de uz general.

Schimbul de date între sistemele online și cele offline se va putea realiza în timp real asimilat (near real-time), în mod continuu (prin instanțe de servicii) și nu va presupune implicarea activă a factorului uman pentru ca schimbul de date să fie posibil din punct de vedere tehnic.

Prin utilizarea resurselor tehnice specifice de care dispun nivelurile și subsistemele Componentei de Acces, și care vor fi explicit alocate pentru managementul curent și pentru monitorizarea continuă a schimbului de date, se va asigura auditul periodic al autorizării și al replicării controlate a informației către resursele online.

1.19.2 Cerințe funcționale

Componenta de acces securizat în condiții de mobilitate, suplimentar faptului că *trebuie să se conformeze cerințelor generale definite în secțiunile și subsecțiunile anterioare*, trebuie să se bazeze pe o soluție tehnică “*end-to-end*” modernă și customizabilă, sens în care trebuie să asigure:

- o infrastructură hardware și software de acces securizat în condiții de mobilitate, prin intermediul platformei Big Data, la datele aferente depozitelor de date comune și seturilor de date individuale;
- acces partajat la funcționalitățile, blocurile și / sau modulele funcționale expuse pe dispozitivele mobile.

1.19.3 Arhitectura funcțională

Arhitectura Componentei de Acces prezentată în figura 2 este organizată pe patru niveluri funcționale, după cum urmează:

- *nivelul EDGE (online)* — grupează resursele online ale Componentei de Acces destinate managementului mobilității utilizatorilor, din perspectiva asigurării accesului securizat la date și la serviciile de aplicație protejate;
- *nivelul BUFFER (online)* — grupează resursele online ale Componentei de Acces destinate interacțiunii cu aplicațiile mobile autorizate de pe terminalele mobile inteligente și procesării în mod transparent a cererilor de acces la date din nucleul intern protejat (offline) și la serviciile modulelor platformei Big Data;
- *nivelul de CONTROL (offline)* — grupează resursele independente offline ale Componentei de Acces destinate autorizării explicite a cererilor de acces la date, respectiv

controlului replicării autorizate a datelor către componentele online ale Componentei de Acces;

- *nivelul CORE (offline)* — grupează resursele offline ale Componentei de Acces destinate interacțiunii cu sursele de date protejate, respectiv cu componentele funcționale ale platformei Big Data, pentru generarea seturilor de date în răspuns la cererile autorizate de acces securizat în regim de mobilitate.

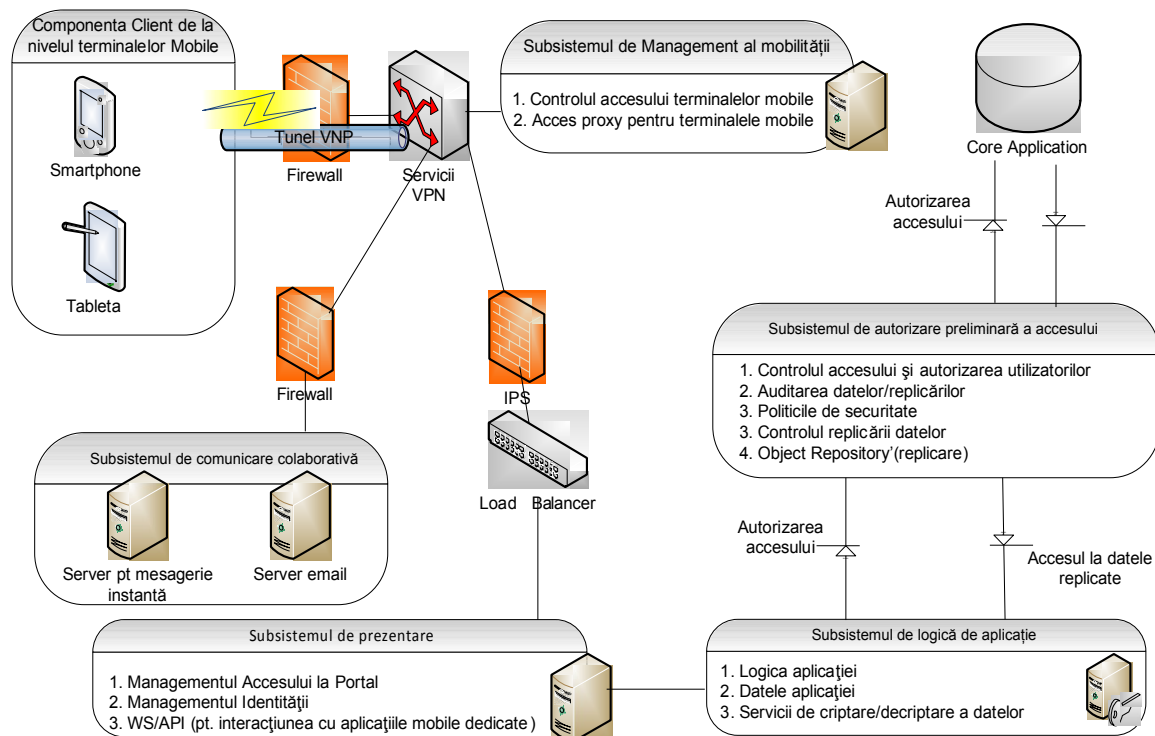


Figura 2: Arhitectura conceptuală a componentei de acces securizat în condiții de mobilitate

Fiecare *nivel* este organizat pe *subsisteme*, iar fiecare subsistem asigură *funcționalități specifice*, a căror descriere sumară face obiectul prezentului capitol de prezentare a arhitecturii modulare a Componentei de Acces.

Rolul specific și contextul operațional relevante, pentru fiecare componentă cheie a arhitecturii funcționale a Componentei de Acces, sunt prezentate pe larg ca parte a descrierii principalelor fluxuri de activități specifice în regim de mobilitate.

Componentele funcționale ale arhitecturii modulare a Componentei de Acces vor fi implementate ca instanțe virtuale, respectiv se vor baza pe echipamentele server pentru suportul hardware de procesare și de I/O, respectiv pe soluția de virtualizare, care va rula pe

acestea, și pe sistemele de operare, care vor rula în mașinile virtuale, pentru a constitui infrastructura sistem software necesară.

Pentru fiecare componentă funcțională, se vor implementa, într-una sau mai multe mașini virtuale, instanțele de servicii corespunzătoare, pe bază de middleware software open-source care va fi adaptat nevoilor proiectului, instalat și configurat pentru a implementa și pentru a expune logica necesară.

1.19.3.1 Nivelul EDGE (online)

1.19.3.1.1 Subsistemul de management al mobilității

1.19.3.1.1.1 Funcționalități la nivel de terminal mobil inteligent

La acest nivel se află instalate componentele client de tip *“Mobile Device Management”* (MDM) și *“Mobile Application Management”* (MAM) ale suitei de tip *“Enterprise Mobility Management”* (EMM).

De asemenea, în mediul controlat generat de componentele MDM și MAM ale suitei EMM se află instalate aplicațiile mobile prin intermediul cărora utilizatorii pot interacționa cu nivelul BUFFER (online), pentru accesul autorizat la datele protejate furnizate de nivelul CORE (offline).

Furnizorul trebuie să asigure cel puțin următoarele aplicații mobile:

- o versiune adaptată a componentei *“Enterprise search”* din cadrul platformei Big Data, cu soluții integrate de regăsire (*“full text search”*, *“spatial search”*, *“face recognition”*) și vizualizare corelată (*“guided navigation”*, *“detail view”*) a datelor accesibile la nivelul platformei;
- o versiune adaptată a modulelor de analiză avansată: *“link analysis”* și *“spatial analysis”*;
- o soluție de accesare a notificărilor cu evidențiere vizuală și / sau sonoră, transmise de către platforma Big Data;
- cel puțin 5 aplicații punctuale, independente de platforma Big Data, cu rol de testare a Componentei de Acces, aspect important în condițiile în care, conform planificării, componenta va fi implementată anterior finalizării platformei. Aceste aplicații vor fi livrate ca parte integrantă a Componentei de Acces și vor permite accesarea securizată în condiții de mobilitate a unor seturi de date existente în depozitele de date comune, seturi de date ce vor fi stabilite de către beneficiar în etapa de analiză, de comun acord cu furnizorul. Fiecare dintre

aceste aplicații de regăsire va valorifica date despre 1 entitate principală cu atributele aferente, respectiv alte entități cu care aceasta se află în relație, în condițiile în care atributele acestora sunt relevante pentru entitatea principală, dar nu pot fi asociate direct acesteia. Criteriile de regăsire și informațiile generate ca rezultat vor fi alese din cumulusul de atribute menționate anterior. Design-ul fizic și cel conceptual al aplicațiilor va fi propus de furnizor și agreat de beneficiar.

1.19.3.1.1.2 Funcționalități de tip reverse proxy pentru accesul mobil

Instanțele de tip “*reverse proxy*” pentru accesul mobil sunt componente server ale suitei EMM, iar rolul acestora este acela de punct de aplicare a politicii de acces (“*policy enforcement point*”) securizat al terminalelor mobile autorizate la celelalte servicii ale nivelului EDGE (online), pentru comunicare colaborativă, precum și la serviciile nivelului BUFFER (online), pentru acces la datele protejate și la platforma Big Data.

1.19.3.1.1.3 Funcționalități centralizate de control al accesului la rețea

Instanțele de control centralizat al accesului la rețea sunt componente server ale suitei EMM, iar rolul acestora este acela de a defini și de a administra, ca autoritate de referință, politicile de acces al terminalelor mobile autorizate la celelalte servicii ale nivelului EDGE (online), precum și la serviciile nivelului BUFFER (online).

1.19.3.1.1.4 Funcționalități de legătură (relay) cu serviciile de comunicare colaborativă

Instanțele de legătură (“*service relay*”) cu serviciile de comunicare colaborativă sunt componente server ale suitei EMM, iar rolul acestora este acela de a opera ca mecanism intermediar de transfer funcțional, între aplicațiile client disponibile la nivelul terminalului mobil inteligent și instanțele de tip server de contacte, calendar partajat și poștă electronică asigurate de nivelului EDGE (online).

1.19.3.1.2 Subsistemul de comunicare colaborativă

1.19.3.1.2.1 Instanțe de servicii de tip server de mesagerie instant

Servicii existente și/sau instalări noi de tip server de comunicare instant cu funcții avansate de protecție a caracterului privat al comunicației, pe grupuri de lucru structurate de tip *comunitate de interes*.

Instanțele de servicii de tip server de mesagerie instant ale subsistemului de comunicare colaborativă se va putea baza pe tehnologie de tip open-source și va implementa funcționalități specifice de tip “*Off-The-Record Messaging*” (OTR) și “*Extensible Messaging and Presence Protocol*” (XMPP), sau echivalente.

1.19.3.1.2.2 Instanțe de servicii de tip server de mesagerie colaborativă structurată

Servicii existente și/sau instalări noi de tip server de colaborare cu funcții de catalog de contacte și calendar partajat, pe grupuri de lucru structurate de tip *comunitate de interes*.

1.19.3.1.3 Componente de tip client back-office

1.19.3.1.3.1 Stație de lucru online

Post de lucru fix (echipamente existente) protejat, de tip back-office, conectat la rețeaua subsistemului de comunicare colaborativă și, prin intermediul acesteia, la rețelele deschise interconectate cu care aceasta interoperează.

1.19.3.1.3.2 Consolă de lucru offline

Post de lucru fix (echipamente existente) intern, de tip back-office, care funcționează în mod offline, relativ la rețelele din Componenta de Acces.

1.19.3.2 Nivelul BUFFER (online)

1.19.3.2.1 Subsistemul de prezentare

1.19.3.2.1.1 Instanțe de servicii de tip portal de acces

Implementează nivelul de prezentare, pentru scenariul în care utilizatorii se conectează la sistem prin intermediul unei aplicații de tip browser, respectiv în care cvasi-totalitatea elementelor funcționale care asigură suportul pentru logica de interacțiune rulează la nivelul instanței de tip server/portal.

În acest scenariu, comunicarea de back-end — între instanțele de servicii de tip portal de acces și instanțe de servicii de tip server de aplicații — se va efectua prin mecanisme de tip WS/API, respectiv protejate prin serviciile echipamentelor de tip Gateway WS/API din infrastructura Componentei de Acces.

În scenariul alternativ, în care o parte a elementelor funcționale care asigură suportul pentru logica de interacțiune rulează pe terminalul client mobil inteligent, la nivelul unei aplicații mobile, comunicarea se va putea derula direct, între aceasta și instanțe de servicii de tip server de aplicații, prin serviciile echipamentelor de tip Gateway WS/API din infrastructura Componentei de Acces.

1.19.3.2.2 Subsistemul de logică de aplicație

1.19.3.2.2.1 Instanțe de servicii de tip server de aplicații

Implementează logica de aplicație a nivelului BUFFER (online), respectiv cel puțin în ceea ce privește:

- managementul sesiunii de lucru, în mod sincron sau asincron;
- transformarea cererii de acces la date, ca parte a sesiunilor on-line, în mesaje (JSON sau XML) de tip “*manifest*”;
- transmiterea acestuia către subsistemul de autorizare preliminară a accesului;
- primirea, de la instanțe de servicii de tip server de obiecte, a datelor generate în răspuns la cererea transmisă;
- transmiterea datelor către solicitantul autorizat, ca parte a sesiunii sincrone;
- crearea unui mesaj de răspuns în așteptare, în cazul sesiunilor de lucru asincrone.

Implementarea acestora va fi protejată prin serviciile echipamentelor de tip Gateway WS/API din infrastructura Componentei de Acces.

1.19.3.2.3 Subsistemul de management al datelor

1.19.3.2.3.1 Instanțe de servicii de tip “*repository*” de fișiere

Instanțe de tip file-server, care expun la nivelul subsistemului de management al datelor seturile de date obiect primite, în răspuns la solicitările de acces autorizate, din subsistemul de control al replicării.

Se va implementa în mod tipic ca parte a funcționalității nodurilor proxy, pe partea dinspre subsistemul de management al datelor, ale completului de tip *diodă de date* corespunzător.

1.19.3.2.3.2 Instanțe de servicii de tip server de obiecte

Instanțe active de tip server care preiau datele obiect prezentate de repository, sub formă de fișiere, și le fac disponibile prin intermediul interfețelor de tip Web Services (WS) sau API.

Implementarea acestora va fi protejată prin serviciile echipamentelor de tip Gateway WS/API din infrastructura Componentei de Acces.

1.19.3.3 Nivelul de CONTROL (offline)

1.19.3.3.1 Subsistemul de autorizare preliminară a accesului

1.19.3.3.1.1 Instanțe de servicii de tip server de autorizare

Primește mesajele de tip *“manifest”* de la instanțele de servicii de tip server de aplicații, care încapsulează cererile de acces la resursele de date protejate.

Verifică încadrarea în limitele impuse de politicile de acces aplicabile, pe baza informației disponibile la nivelul instanțelor de servicii de politici de acces.

În cazul încadrării în limitele impuse de politicile de acces aplicabile:

- execută logica de autorizare și certifică cererea, pe care o trimite către instanțele de servicii de tip *“repository”* de fișiere de la nivel CORE (offline);
- generează informația de audit corespunzătoare, pe care o trimite către instanțele de servicii de audit ale subsistemului.

În cazul în care cererea nu se încadrează în limitele impuse de politicile de acces aplicabile:

- execută logica de reacție la anomalii și incidente, pe baza căreia generează și certifică un mesaj de alertă;
- generează informația de audit corespunzătoare, pe care o trimite către instanțele de servicii de audit ale subsistemului.

1.19.3.3.1.2 Instanțe de servicii de prelucrare criptografică

Instanță server care expune o interfață de tip WS/API, pentru generarea de semnături electronice asociate mesajelor de tip “*manifest*” autorizate, precum și anvelopei (“*header*”) cu parametrii deciziei care însoțește fiecare mesaj aprobat, în scopul certificării deciziei de autorizare a accesului.

Componenta criptografică a operațiunilor de semnare electronică se va efectua exclusiv la nivelul instanțelor active de servicii de prelucrare criptografică, iar protecția cheilor private și accelerarea procesărilor criptografice se vor asigura pe baza de componente hardware de tip HSM certificate FIPS 140-2.

1.19.3.3.1.3 Instanțe de servicii de audit al nivelului de autorizare

Primește, de la instanțele de servicii de tip servere de autorizare, și jurnalizează toate cererile și deciziile de autorizare sau neautorizare a accesului, respectiv atât pentru cererile aprobate, cât și pentru anomaliile identificate și incidentele semnalate.

Transmite anvelopa (“*header*”) și semnăturile electronice generate în scopul certificării autorizării de acces, pentru toate cererile autorizate, către instanțele de servicii de tip jurnal martor (replică) de audit, din subsistemul de control al replicării.

1.19.3.3.1.4 Instanțe de servicii de politici de acces la date

Replică (de tip LDAP, sau în tehnologie asemănătoare) a cataloagelor de identitate, pentru nivelul de back-end al sistemului, care va conține informația relevantă pentru identificarea utilizatorilor și pentru specificarea politicilor de autorizare a accesului.

Replica va fi filtrată, respectiv va conține exclusiv informație de identificare la nivel de pseudonim, fără corespondență cu identitatea reală a operatorilor și fără asocierea directă cu rolurile reale ale acestora.

Instanțele de servicii de politici de acces la date vor fi actualizate offline, prin pachete semnate electronic, pe măsura modificării informației de referință sistemul intern protejat, și vor opera în mod tranzacțional independent de acesta.

1.19.3.3.3 Subsistemul de control al replicării datelor

1.19.3.3.3.1 Instanțe de servicii de tip repository de fișiere

Instanțe de tip file-server, care expun la nivelul subsistemului de control al replicării datelor seturile de date obiect primite, în răspuns la solicitările de acces autorizate, din subsistemul de acces la date al nivelului CORE (offline).

Se va implementa în mod tipic ca parte a funcționalității nodurilor proxy, pe partea dinspre subsistemul de control al replicării datelor, ale completului de tip Diodă de Date corespunzător.

1.19.3.3.3.2 Instanțe de servicii de prelucrare criptografică

Instanță server care expune o interfață de tip WS/API, pentru generarea de semnături electronice asociate setului de date generate în răspuns la cererile autorizate, în scopul certificării autenticității răspunsului.

Datele generate, în răspuns la fiecare cerere, vor fi criptate cu cheile publice ale solicitantului și ale instanțelor de audit din subsistemul de control al replicării, pentru a asigura că datele nu vor fi disponibile în clar la nivelul sistemelor online și în rețelele deschise, respectiv că numai beneficiarul autorizat și mecanismele interne de control împotriva scurgerilor de informații vor avea acces la date în clar.

Componenta criptografică a operațiunilor de semnare electronică se vor efectua exclusiv la nivelul instanțelor active de servicii de prelucrare criptografică, iar protecția cheilor private și accelerarea procesărilor criptografice se vor asigura pe baza de componente hardware de tip HSM certificate FIPS 140-2.

1.19.3.3.3.3 Instanțe de servicii de tip jurnal martor (replică) de audit al autorizării

Primește, de la instanțele de servicii de audit al nivelului de autorizare din subsistemul de autorizare preliminară a accesului, anvelopa (*“header”*) și semnăturile electronice generate în scopul certificării autorizării de acces, pentru fiecare cerere autorizată.

1.19.3.3.3.4 Instanțe de servicii de tip server de control

Preia, de la instanțele de servicii de tip repository de fișiere, seturile de date primite din sistemul protejat, în răspuns la fiecare cerere autorizată, și folosește serviciile instanțelor de servicii de prelucrare criptografică pentru a verifica autenticitatea acestora.

Verifică, pe baza informației disponibile la nivelul instanțelor de servicii de tip jurnal martor (replică) de audit al autorizării, dacă există în sistem informație de audit cu privire la cererea de acces autorizată la care face trimitere anvelopa (*“header”*) ce însoțește setul de date răspuns preluat, respectiv dacă autorizarea corespunzătoare nu este expirată sau revocată.

În cazul în care identifică cererea de acces autorizată, neexpirată și nerevocată, corespunzătoare:

- execută logica de eliberare a răspunsului către instanțele de servicii de tip *“repository”* de fișiere din subsistemul de management al datelor, la nivel BUFFER (online);
- generează informația de audit corespunzătoare, pe care o trimite către instanțele de servicii de audit al nivelului de control.

Dacă (a) seturile de date răspuns nu sunt autentice, ori dacă (b) nu există în sistem informație de audit cu privire la cererea de acces autorizată la care face trimitere anvelopa (*“header”*) ce însoțește setul de date răspuns preluat, sau când informația de audit existentă indică faptul că cererea este expirată sau a fost revocată, atunci:

- execută logica de reacție la anomalii și incidente, pe baza căreia generează și certifică un mesaj de alertă;
- generează informația de audit corespunzătoare, pe care o trimite către instanțele de servicii de audit al nivelului de control.

1.19.3.3.3.5 Instanțe de servicii de audit al nivelului de control

Primește, de la instanțele de servicii de tip server de control, și jurnalizează toate cererile și deciziile de autorizare sau neautorizare a accesului, respectiv atât pentru cererile aprobate, cât și pentru anomaliile identificate și incidentele semnalate.

1.19.3.4 Nivelul CORE (offline)

1.19.3.4.1 Subsistemul de acces la date

1.19.3.4.1.1 Instanțe de servicii de tip repository de fișiere

Instanțe de tip file-server, care expun la nivelul subsistemului de acces la date solicitările de acces autorizate, primite din subsistemul de autorizare preliminară al nivelului CONTROL (offline).

Se va implementa în mod tipic ca parte a funcționalității nodurilor proxy, pe partea dinspre subsistemul de control al replicării datelor, ale completului de tip *diodă de date* corespunzător.

1.19.3.4.1.2 Instanțe de servicii de acces la date

Preia, de la instanțele de servicii de tip “*repository*” de fișiere, și decodează cererile autorizate de acces la date.

Execută, prin intermediul interfețelor de tip WS/API corespunzătoare, interogările necesare în aplicațiile existente și întoarce setul de date în răspuns la fiecare cerere autorizată de acces la date.

Trimite setul de date răspuns către instanțele de servicii de împachetare a datelor, ca mesaj (de tip JSON sau XML) care va conține în mod obligatoriu referințele necesare la cererea autorizată corespunzătoare și, respectiv, la decizia de autorizare.

1.19.3.4.1.3 Instanțe de servicii de împachetare a datelor

Primește, de la instanțele de servicii de acces la date, setul de date răspuns pe care îl certifică și îl împachetează, inclusiv în sensul protejării, cu ajutorul instanțelor de servicii de prelucrare criptografică, a integrității și a confidențialității datelor, prin utilizarea cheilor publice ale serviciului instanțelor de servicii de tip server de control și ale solicitantului cererii autorizate.

1.19.3.4.1.4 Instanțe de servicii de prelucrare criptografică

Instanță server care expune o interfață de tip WS/API, pentru generarea de semnături electronice asociate setului de date generate în răspuns la cererile autorizate, în scopul certificării autenticității răspunsului.

Datele generate, în răspuns la fiecare cerere, vor fi criptate cu cheile publice ale solicitantului și ale instanțelor de audit din subsistemul de control al replicării, pentru a asigura că datele nu vor fi disponibile în clar la nivelul sistemelor online și în rețelele deschise, respectiv că numai beneficiarul autorizat și mecanismele interne de control împotriva scurgerilor de informații vor avea acces la date în clar.

Componenta criptografică a operațiunilor de semnare electronică se vor efectua exclusiv la nivelul instanțelor active de servicii de prelucrare criptografică, iar protecția cheilor

private și accelerarea procesărilor criptografice se vor asigura pe baza de componente hardware de tip HSM certificate FIPS 140-2.

1.19.3.5 Fluxuri de lucru

Pentru a beneficia de funcționalitățile specifice oferite de Componenta de Acces, în urma serviciului de implementare a componentei de acces securizat în condiții de mobilitate, furnizorul trebuie să asigure funcționarea și operaționalitatea următoarelor fluxuri de lucru:

1.19.3.5.1 Fluxul de autentificare și autorizare inițială, la nivelul terminalului mobil

1. Pe terminalul mobil inteligent, utilizatorul interacționează cu mediul de lucru protejat prin aplicația de tip *“app launcher”* (parte a componentei client a suitei EMM), pentru a începe sesiunea de lucru;
2. Înainte de a permite accesul la resursele (date și aplicații protejate, pe terminalul mobil inteligent), componenta de control al mediului de lucru protejat declanșează automat secvența de acces și prezintă aplicația de autentificare (ambele, parte componentei client a suitei EMM);
3. Pentru scenariul de acces cu nivel de încredere implicit (mai redus; situație în principiu nerecomandată, din perspectiva asigurării nivelului ridicat de securitate dorit, dar care se poate dovedi practic necesară — în funcție de situație sau de constrângeri tehnice — și, în anumite condiții, chiar acceptabilă — cu asumarea riscurilor relevante), autentificarea se poate realiza exclusiv cu credențiale de tip *nume utilizator / parolă* (sau PIN);
4. Ca scenariu alternativ, pentru un nivel de încredere intermediar, autentificarea se va putea realiza prin mecanisme de tip *“soft-token”* OTP, dacă serviciul corespunzător este instalat;
5. Pentru scenariul de acces cu nivel de încredere ridicat, aplicația de autentificare va accesa în mod transparent componenta (hardware) de tip smartcard instalată, pe care se află resurse protejate criptografic (chei private, certificate, fișiere de politică etc.) necesare secvenței de autentificare multifactor;
6. Utilizatorul se va autentifica față de componenta hardware de tip smartcard, pentru a autoriza folosirea materialului criptografic pentru operațiunile subsecvente, pasive (prezentare certificat) sau active (secvențe de tip *“challenge response”*), de autentificare multifactor;

7. Dacă politica aplicabilă este de tip Single-Sign-On (SSO), componenta de control integrată a mediului de lucru protejat va asigura în mod transparent funcționalitățile necesare, în sensul și în limitele politicii configurate, iar utilizatorul nu va mai avea nevoie să se autentifice din nou la fiecare acces de resursă;

8. Pentru accesul utilizatorului autentificat și autorizat, accesul la resursele de pe terminalul mobil inteligent va fi gestionat în sensul și în limitele politicilor configurate prin instrumentele native ale suitei EMM;

9. Componentele client ale suitei EMM se vor sincroniza periodic cu componentele centrale de management ale acesteia, inclusiv în ceea ce privește politicile aplicabile, și vor asigura aplicarea lor inclusiv în cazul utilizării temporare a terminalului mobil inteligent fără legătură cu centrul de management;

10. Se vor putea configura, acolo unde este cazul, politici care să poată bloca selectiv accesul la resurse locale de pe terminalul mobil inteligent, în situația în care acesta a fost utilizat fără sincronizare cu sistemele centrale o perioadă mai mare decât cea limită prevăzută de politică.

1.19.3.5.2 Fluxul de utilizare a aplicațiilor în mediul protejat, pe terminalul mobil

1. Utilizatorul autentificat și autorizat va lansa aplicația obiect selectată, de care are nevoie;

2. În cazul în care — pentru aplicația obiect, lansată de utilizator — politica aplicabilă prevede o excepție de la regimul implicit de tip SSO sau dacă, de la cea mai recentă autentificare, a expirat durata de time-out preconfigurată, înainte de a permite accesul la aplicația obiect, componenta de control al mediului de lucru va prezenta utilizatorului, în mod automat, aplicația de autentificare pentru (re-) autentificare;

3. În scenariul de acces cu nivel ridicat de încredere, se vor executa pașii **5 - 7** din *3.2.3.5.1. Fluxul de autentificare și autorizare inițială, la nivelul terminalului mobil*, pentru autentificare multifactor cu implicarea componentei hardware de tip smartcard instalate;

4. În scenariile de acces cu nivel de încredere redus sau intermediar, pentru autentificare se aplică excepțiile descrise mai sus (la autentificarea inițială);

5. Utilizatorul autentificat și autorizat are acces la resursele oferite de aplicația obiect lansată;

6. Utilizatorul autentificat selectează o funcționalitate a aplicației obiect curente (de exemplu, o aplicație de căutare) și, dacă este cazul, introduce parametrii necesari (de exemplu, textul căutării) sau validează opțiunile relevante (de exemplu, filtrele aplicabile, în cazul unei căutări parametrizate semantic);

7. Dacă executarea funcționalității selectate va presupune schimbul de informație și înălțuirea de funcționalități cu alte aplicații locale controlate, disponibile în mediul de lucru protejat de pe terminalul mobil inteligent, componenta de control va asigura că aplicațiile din mediul protejat vor comunica între ele în mod securizat;

8. Aplicațiile controlate, disponibile în mediul de lucru protejat de pe terminalul mobil inteligent, vor putea comunica cu aplicații nesecurizate de pe același terminalul mobil inteligent numai în măsura în care există politici explicit configurate pentru a permite acest lucru, respectiv numai în limitele impuse de acestea;

9. Datele create temporar, la nivelul oricărei aplicații sau generate și stocate cu ocazia înălțuirii de funcționalități între aplicațiile controlate, precum și datele primite de la sistemele centrale, în răspuns la solicitarea/căutarea formulată, vor fi criptate.

1.19.3.5.3 Fluxul de acces securizat în regim de mobilitate

1. Utilizatorul autentificat și autorizat va lansa aplicația obiect selectată, de care are nevoie;

2. În cazul în care rularea aplicației lansate presupune, implicit sau explicit, utilizarea de resurse ale componentei centrale de acces în regim de mobilitate, componenta de control al mediului de lucru protejat (parte a componentei client a suitei EMM) instalată la nivelul terminalului mobil inteligent va asigura protecția comunicației între aplicație și sistemele centrale, în mod transparent pentru utilizator;

3. Componenta de control va administra, în mod automat și transparent, crearea și utilizarea conexiunilor criptate pe relația cu componenta de tip reverse proxy pentru accesul mobil (parte integrantă a componentei client a suitei EMM), pentru un prim nivel de protecție individuală, de tip *“VPN la nivel de aplicație”*;

4. În mod funcțional independent de funcționalitățile de tip MAM din suitea EMM, soluția de tip *VPN* pentru terminalele mobile inteligente va prelua toate conexiunile terminalelor mobile inteligente și le va acționa ca o anvelopă suplimentară de criptare, pentru un al doilea nivel de protecție exterioară, de tip *“VPN la nivel de terminal mobil inteligent”*;

5. La nivelul componentelor centrale, de tip concentrator pentru comunicația de tip VPN între terminalele mobile inteligente și componenta centrală de acces, se va realiza în mod transparent terminarea anvelopei exterioare de protecție de tip VPN;

6. Comunicația între terminalele mobile inteligente și componenta centrală de acces va traversa perimetrul extern de rețea al platformei, nivel la care echipamentele de tip “*Next Generation Firewall*” (NGFW) (Tip 1) vor asigura în mod transparent serviciile de segmentarea și protecție perimetrală, protecția împotriva atacurilor de rețea, precum și detecția și protecția anti-intruziune și anti-malware;

7. Toate componentele de automatizare și de protecție a comunicației terminalelor mobile inteligente autentificate și autorizate vor folosi serviciile de tip IPAM/DNS asigurate de echipamentele de tip DNS Server / DNS Firewall;

8. După trecerea de nivelul de protecție a rețelei, asigurat de componenta de tip NGFW (Tip 1), conexiunile individual protejate, de tip VPN, ale fiecărei aplicații vor ajunge la componenta centralizată de tip “*reverse proxy*” pentru accesul mobil (parte integrantă a componentei client a suitei EMM);

9. Autentificarea instanței de control care rulează pe terminalul mobil inteligent și autorizarea accesului de către componenta de tip “*reverse proxy*” pentru accesul mobil sunt gestionate transparent de către componenta centralizată de control al accesului la rețea (parte integrantă a componentei client a suitei EMM);

10. Conexiunile autorizate vor putea accesa, prin serviciile transparente de tip reverse proxy, resursele interne ale componentei centrale de acces în regim de mobilitate, iar încercările de acces care nu se autentifică cu succes sau care nu sunt autorizate vor fi auditate;

11. Toate formele de acces la acest nivel (atât conexiunile autorizate, cât și încercările de acces care nu s-au autentificat cu succes, sau care nu au fost autorizate) vor fi jurnalizate și auditate, periodic, în mod riguros.

1.19.3.5.4 Fluxul de comunicare colaborativă securizată în mediul online

1. Pentru comunicare colaborativă structurată, utilizatorul autentificat și autorizat va lansa aplicația corespunzătoare (parte a componentei client a suitei EMM) care implementează logica de tip client, pentru acces la serviciile de poștă electronică, management de contacte și servicii de calendar partajat;

2. Dacă pentru accesul la aplicația (client) de comunicare colaborativă structurată este configurată o politică de (re-)autentificare explicită, componenta de control va executa pașii **2 - 5** din 3.2.3.5.2. *Fluxul de utilizare a aplicațiilor în mediul protejat, pe terminalul mobil;*

3. Dacă validarea autenticității unui mesaj primit și/sau semnarea unui mesaj (nou, sau de răspuns) generat de utilizator vor necesita acces la materialul criptografic (de exemplu, chei private și certificate) și la funcționalitățile corespunzătoare (de exemplu, semnare electronică și verificare de semnătură), la nivelul componentei de tip smartcard instalate, componenta de control va executa pașii **5 - 6** din 3.2.3.5.1. *Fluxul de autentificare și autorizare inițială, la nivelul terminalului mobil;*

4. Dacă deschiderea mesajului primit, sau a unui document atașat acestuia, necesită acces la materialul criptografic (de exemplu, chei de cifru, simetric sau asimetric) și la funcționalitățile corespunzătoare (de exemplu, criptare/decriptare), la nivelul componentei de tip smartcard instalate, componenta de control va executa pașii **5 - 6** din 3.2.3.5.1. *Fluxul de autentificare și autorizare inițială, la nivelul terminalului mobil;*

5. Dacă crearea de mesaje va presupune preluarea de conținut (de exemplu, fișiere) de la alte aplicații disponibile în mediul de lucru protejat, componenta de control va aplica regulile de comunicare între aplicațiile mobile, pe terminalul mobil inteligent, precum și protecția informației, atât între aplicații (cel puțin, comunicare exclusiv criptată), cât și la nivelul acestora (stocare persistentă a datelor, atunci când este necesar, numai în formă criptată);

6. În acest sens, componenta de control va executa pașii **7 - 9** din 3.2.3.5.2. *Fluxul de utilizare a aplicațiilor în mediul protejat, pe terminalul mobil;*

7. Funcționalitățile centralizate de tip server (“*relay*”) de colaborare vor fi asigurate de componenta dedicată, la nivelul subsistemului management al mobilității, care va opera ca o componentă de securitate care va proteja serviciul și va stoca temporar mesajele, în postura asemănătoare unui server tradițional de relay pentru mesagerie (de exemplu, poșta electronică);

8. Comunicația între serverul de relay, de la nivelul subsistemului management al mobilității, și serverul de mesagerie colaborativă structurată, de la nivelul subsistemului de comunicare colaborativă, va traversa perimetrul de rețea intern, care separă cele două subsisteme, nivel la care echipamentele de tip “*Next Generation Firewall*” (Tip 2) vor asigura în mod transparent serviciile de segmentarea și protecție perimetrală, protecția împotriva atacurilor de rețea, precum și detecția și protecția anti-intruziune și antimalware;

9. Componenta internă dedicată, de tip server de mesagerie colaborativă structurată, la nivelul subsistemului de comunicare colaborativă, va stoca persistent mesajele și va constitui elementul funcțional principal de susținere a serviciului;

10. Pentru comunicare colaborativă ad-hoc, de tip *“instant messaging”*, utilizatorul autentificat și autorizat va lansa aplicația obiect corespunzătoare (dezvoltată și configurată, inclusiv prin utilizarea de tehnologie de tip open-source, ca parte a proiectului);

11. Aceasta va asigura atât suportul de tip client pentru semnalizarea de prezență și schimbul de mesaje instant (*“instant messaging”*), în arhitectură de serviciu de tip *“Extensible Messaging and Presence Protocol”* (XMPP), pentru comunicarea în grupuri de lucru tematice sau ad-hoc, de tip *“community-of-interest”*;

12. Aplicația client va asigura suport activ de protecție a confidențialității și a repudiabilității mesajelor, inclusiv prin protocoale criptografice de tip *“Off-the-Record Communication”* (OTR) și va putea utiliza inclusiv servicii de tip *“Cryptographic Service Provider”* (CSP) furnizate de componenta hardware de tip smartcard instalată;

13. La nivel funcțional specific, aplicațiile client pentru mesagerie instant vor comunica direct, în arhitectură XMPP, cu componenta internă dedicată de tip server de mesagerie colaborativă instant, respectiv fără implicarea nodului de relay care deservește numai mesageria structurată;

14. Comunicația între aplicația de mesagerie colaborativă instant, de la nivelul terminalului mobil inteligent, și serverul de mesagerie colaborativă instant, va traversa perimetrul de rețea intern care separă subsistemul de comunicare colaborativă, nivel la care echipamentele de tip *“Next Generation Firewall”* (Tip 2) vor asigura în mod transparent serviciile de segmentarea și protecție perimetrală, protecția împotriva atacurilor de rețea, precum și detecția și protecția anti-intruziune și antimalware;

15. Componenta internă de tip *“Secure Web Gateway”*, de la nivelul subsistemului de comunicare colaborativă, va asigura servicii de tip *“direct forward proxy”* permanent, pentru a proteja zona de lucru a utilizatorilor interni cu rol de suport sau de dispecerat, respectiv pentru a nu permite accesul inițiat din afara acesteia;

16. Utilizatorii interni de suport vor putea accesa serviciile de comunicare colaborativă, pentru a comunica în regim colaborativ, prin utilizarea unor aplicații de desktop dedicate sau prin intermediul unor interfețe corespunzătoare de acces la aceste servicii prin mediu de tip browser web.

1.19.3.5.5 Fluxul de acces la serviciile de aplicație și la resursele de date protejate

1. Utilizatorul autentificat și autorizat va lansa aplicația obiect selectată, de care are nevoie;
2. Componenta de control va executa implicit pașii **2 - 9** din 3.2.3.5.2. *Fluxul de utilizare a aplicațiilor în mediul protejat, pe terminalul mobil*;
3. În cazul în care rularea aplicației lansate presupune, implicit sau explicit, utilizarea de resurse ale platformei centrale de acces în regim de mobilitate, componenta de control al mediului de lucru protejat va executa pașii **2 - 11** din 3.2.3.5.3. *Fluxul de acces securizat în regim de mobilitate*;
4. Conexiunile între componentele subsistemului de management al mobilității și componenta de portal de acces traversează perimetrul de protecție al subsistemului de prezentare, nivel la care echipamentele de tip “*Next Generation IPS*”, împreună cu funcționalitățile de tip firewall ale echipamentelor “*Application Delivery Controller*”, vor asigura în mod transparent serviciile de segmentare și protecție perimetrală, protecția împotriva atacurilor de rețea, precum și detecția și protecția anti-intruziune și antimalware;
5. Funcționalitățile integrate de tip “*Web Application Firewall*” (WAF) ale echipamentelor “*Application Delivery Controller*” (ADC), vor asigura în mod transparent serviciile de protecție împotriva atacurilor specifice aplicațiilor web;
6. Funcționalitățile integrate de optimizare a serviciilor de aplicație, integrate la nivelul echipamentelor de tip ADC, vor asigura preluarea în hardware (“*offloading*”) a sarcinii de procesare a compresiei și a celei de procesare cryptographic SSL, precum și redistribuirea activă a sarcinii de procesare (“*load-balancing*”) între instanțele de servere de portal sau de aplicație;
7. Funcționalitățile integrate de tip “*reverse proxy permanent*”, asistat hardware, ale echipamentelor de tip ADC, vor asigura în mod transparent continuitatea aparentă, la nivel de logică de sesiune și de aplicație, a conexiunilor între aplicația mobilă lansată de utilizator pe terminalul mobil inteligent și serverele de prezentare și de aplicație, în timp ce, la nivel de rețea, comunicația între aplicația mobilă și ADC, pe de o parte (în front-end), și comunicația între ADC și serviciile relevante de prezentare și de aplicație, pe de altă parte (în back-end), sunt efectiv independente;

8. În cazul în care aplicația obiect lansată (cum ar fi cazul în care, de exemplu, aceasta va fi de tip browser) va depinde de implementarea la nivel de server a logicii de interacțiune, respectiv în care serviciile de portal vor fi cele care expun o interfață tradițională de prezentare și de interacțiune între utilizatorul uman și serviciile de aplicație, componenta ADC va extinde sesiunea de lucru către instanțele de servicii de tip portal de acces;

9. După procesarea logicii de prezentare și interacțiune, serviciile de portal vor comunica în back-end, cu serviciile de la nivelul subsistemului de procesare a logicii de aplicație, prin apeluri de interacțiune programatică neasistată la nivel WS/API către echipamentele de tip gateway pentru serviciile WS/API;

10. În cazul în care logica de interacțiune cu utilizatorul va fi implementată, total sau parțial, la nivelul aplicației obiect lansate, iar aceasta va fi concepută să interacționeze direct, la nivel WS/API, cu serviciile din subsistemul de procesare a logicii de aplicație, componenta ADC va extinde sesiunea de lucru direct către echipamentele de tip gateway pentru serviciile WS/API care protejează subsistemul de procesare a logicii de aplicație;

11. La nivelul subsistemului de prezentare, toate referințele la identitate și la politicile de acces aplicabile vor fi rezolvate de către instanțele de servicii pentru managementul identității de la nivelul subsistemului de prezentare;

12. La nivelul subsistemului de procesare a logicii de aplicație, echipamentele de tip gateway vor acționa ca *“reverse proxy”* pentru servicii de tip WS/API și vor extinde sesiunile de lucru (deschise așa cum se arată mai sus, la pașii **10 - 11** din 3.2.3.5.5. *Fluxul de acces la serviciile de aplicație și la resursele de date protejate*), către instanțele de servicii de tip server de aplicații, care vor iniția procesarea logicii de acces la date;

13. Instanțele de servicii de tip server de aplicații vor opera în mod transparent pentru a transforma comunicația între instanțele de tip browser/aplicație mobilă, lansate de la nivelul terminalelor mobile inteligente, și sursele de date protejate, aflate la nivelul CORE (offline), într-un flux asincron de mesaje;

14. Instanțele de servicii de tip server de aplicații vor opera cu un cod unic pentru fiecare pagină de portal, respectiv pentru fiecare element (câmp de interfață) din aplicațiile mobile care implementează logică de interacțiune cu utilizatorul;

15. Prin referențierea acestor coduri, aplicațiile mobile și paginile de portal accesate prin intermediul unui browser vor putea descrie sintetic, în mod neechivoc, natura și conținutul cererii de acces la date, prin indicarea câmpurilor de interfață care au fost folosite, respectiv a datelor și/sau a atributelor corespunzătoare introduse de utilizator;

16. Pentru fiecare sesiune activă, instanțele de servicii de tip server de aplicații vor genera un mesaj discret de tip “*manifest*”, cu reprezentare simplificată în format textual structurat (de tip JSON, XML sau asimilat), care va identifica cel puțin apelantul și codul sesiunii, și care va include natura, conținutul și atributele căutării;

17. Mesajul de tip manifest va fi transmis către instanțele de servicii de tip server de autorizare, prin intermediul completului de tip *diodă de date* care protejează, prin controlul comunicației unidirecționale, accesul la subsistemul de autorizare preliminară a accesului;

18. La nivelul subsistemului de procesare a logicii de aplicație, toate referințele la identitate vor fi rezolvate de către instanțele de servicii pentru managementul identității de la nivelul subsistemului de prezentare;

19. Instanțele de servicii de tip server de autorizare, de la nivelul subsistemului de autorizare preliminară a accesului, vor primi mesajele “*manifest*”, pe care le vor valida pe baza regulilor relevante (asociate solicitantului și, respectiv, datelor la care se solicită accesul);

20. La nivelul subsistemului de autorizare preliminară a accesului, toate referințele la identitate și la politicile de acces la date vor fi rezolvate de către instanțele de tip server de politici de acces la date, de la nivelul subsistemului de prezentare;

21. Cererile de acces validate vor fi autorizate preliminar și se va genera o înregistrare de audit tip *certificat de autorizare*, iar pentru cele invalide sau care nu au putut fi autorizate se vor genera coduri de eroare și (după caz) alerte;

22. Toate operațiunile de marcare temporală și de semnare digitală se vor procesa server-side, de către instanțele de servicii de prelucrare criptografică interne, la nivelul subsistemului de autorizare preliminară a accesului;

23. Înregistrările de audit generate pentru toate cererile de acces la date vor fi certificate prin marcă temporală și semnătură digitală și vor fi replicate, în mod obligatoriu, către instanțele interne de servicii de audit al autorizării, prin intermediul completului de tip *diodă de date* care protejează serverul de audit la nivelul subsistemului de autorizare preliminară a accesului;

24. Cel puțin înregistrările de audit generate pentru cererile de acces validate și aprobate vor fi replicate către instanțele de tip jurnal martor (replică) de audit al autorizării, prin intermediul completului de tip *diodă de date* care asigură controlul comunicației unidirecționale pentru separarea subsistemului de autorizare preliminară a accesului de subsistemul de control al replicării datelor;

25. Cererile de acces validate și autorizate vor fi însoțite de informație relevantă cel puțin cu privire la termenul de valabilitate asociat autorizării, care va putea fi exprimat ca dată, sau ca durată de timp, precum și a informațiilor pertinente referitoare la care câmpuri de date răspuns vor putea fi transmise în clar (necriptate), și în ce condiții;

26. Cererile de acces validate și autorizate vor fi însoțite de o marcă temporală și de o semnătură digitală, și vor fi transmise către instanțele de servicii de acces la date, prin intermediul completului de tip diodă de date care asigură controlul comunicației unidirecționale pentru accesul la nivelul CORE (offline);

27. În mod opțional, înregistrările de audit generate pentru cererile de acces invalide sau neautorizate vor fi și ele replicate către instanțele interne de servicii acces la date, la nivelul CORE (offline);

28. La nivel CORE (offline), instanțele de servicii de acces la date vor onora cererile autorizate preliminar pe care le-au primit, prin accesarea directă a surselor interne (servicii de aplicații și baze de date) protejate;

29. La acest nivel, toate referințele la identitate și la politicile de acces la date vor fi rezolvate de către instanțele de management al identității existente, aflate în exploatare;

30. Seturile de date generate în răspuns la cererile autorizate vor fi remise instanțelor de servicii de împachetare, care vor genera mesajele de răspuns cu reprezentare simplificată în format textual structurat (de tip JSON, XML sau asimilat), care vor identifica cel puțin apelantul și codul sesiunii, și care vor include datele de la care s-a solicitat accesul în format *“key/value pair”*;

31. Se va putea opta pentru o strategie de prestabilire a unei dimensiuni fixe, optimizate, a mesajelor, iar în cazul în care sunt necesare mai multe părți pentru a transmite tot conținutul de date solicitat (într-o cerere de acces autorizată), mesajele subsecvente vor include în mod obligatoriu referință la mesajul de bază și un număr de ordine, pentru a facilita reasamblarea;

32. Indiferent dacă se răspunde printr-un singur mesaj, sau printr-o succesiune de mesaje, se va putea opta pentru o strategie de stabilire a unei dimensiuni maxime totale a pachetului de răspuns, sau a unui număr maxim de mesaje subsecvente care se va trimite;

33. Dacă datele de răspuns includ obiecte (fișiere) multimedia, sau alt conținut de tip non-textual, acestora le vor putea fi asociați identificatori unici, care vor fi incluși ca referință în mesajul de bază, iar datele vor fi putea fi împachetate distinct, cu referință la mesajul de bază corespunzător;

34. Astfel, primirea mesajului de bază va putea fi prioritizată (inclusiv în mod *“push”*), iar datele non-textuale vor putea fi descărcate (în mod *“pull”*) ulterior, la solicitarea utilizatorului;

35. Ca politică implicită, datele de răspuns vor putea fi transmise în format protejat, criptate, iar excepțiile nu vor putea excede limitele impuse, în acest sens, de condițiile de autorizare primite;

36. Criptarea se va realiza (de exemplu, prin utilizarea de chei publice / certificate) astfel încât ele să poată fi accesate numai de către instanțele de servicii de control, de la nivelul subsistemului de control al replicării datelor, și de către beneficiarul final autorizat;

37. Împachetarea va presupune asocierea de informație relevantă despre solicitarea autorizată căreia răspunsul îi corespunde, precum și a unui termen de valabilitate, care va putea fi exprimat ca dată, ca durată de timp, sau ca număr de accesări (confirmate) de către beneficiarul autorizat;

38. În plus, la împachetare se vor asocia datelor, pentru fiecare mesaj, marcă temporală și semnături digitale pentru certificarea autenticității;

39. Toate operațiunile de marcare temporală și de semnare digitală se vor procesa server-side, de către instanțele de servicii de prelucrare criptografică interne, la nivel CORE (offline);

40. Datele de răspuns împachetate vor fi transmise către instanțele de servicii de control, de la nivelul subsistemului de control al replicării datelor, prin intermediul completului de tip diodă de date care asigură controlul comunicației unidirecționale pentru protecția schimbului de informație între nivelul CORE (offline) și subsistemului de control al replicării datelor;

41. Instanțele de servicii de control, de la nivelul subsistemului de control al replicării datelor, vor primi datele de răspuns generate și vor apela la instanțele de servicii criptografice pentru a verifica autenticitatea datelor primite (prin verificarea semnăturii digitale);

42. Se va verifica, prin consultarea instanțelor de tip jurnal martor (replică) de audit al autorizării, pentru a verifica faptul că există o aprobare de acces neexpirată căreia datele primite îi corespund;

43. Serviciile criptografice vor fi invocate în mod transparent pentru decriptarea câmpurile de date protejate, în măsura în care se impune verificarea acestora înainte de eliberarea mesajelor de răspuns către subsistemul de management al datelor;

44. Pentru fiecare mesaj de răspuns autorizat eliberat către subsistemul de management al datelor se generează o înregistrare de audit, iar în cazul în care nu există înregistrarea de audit pentru aprobarea de acces neexpirată corespunzătoare (sau în care eliberarea mesajelor nu poate fi efectuată din orice alt motiv), se generează o alertă;

45. Înregistrările de audit și alertele generate, pentru toate mesajele de răspuns autorizate, vor fi certificate prin marcă temporală și semnătură digitală și vor fi replicate, în mod obligatoriu, către instanțele interne de servicii de audit, prin intermediul completului de tip *diodă de date* care protejează serverul de audit la nivelul subsistemului de control al replicării;

46. Toate operațiunile de marcare temporală, de semnare digitală și de decriptare se vor procesa server-side, de către instanțele de servicii de prelucrare criptografică interne, la nivelul subsistemului de control al replicării datelor;

47. Mesajele autorizate la ieșire vor fi transmise către instanțele de servicii de tip server de obiecte, de la nivelul subsistemului de management al datelor, prin intermediul completului de tip *diodă de date* care asigură controlul comunicației unidirecționale pentru protecția schimbului de informație între subsistemului de control al replicării datelor și subsistemele online;

48. Pentru toate sesiunile de lucru active, instanțele de servicii de tip server de aplicație, de la nivelul subsistemului logică de aplicație, vor verifica periodic (*“polling”*) primirea mesajelor de răspuns de către instanțele de servicii de tip server de obiecte, de la nivelul subsistemului de management al datelor, prin medierea componentelor de tip gateway se servicii WS/API;

49. În cazul în care mesajul de răspuns este primit înainte de expirarea termenului de *“time-out”* al sesiunii de lucru, instanța de server de aplicație va întoarce răspunsul către terminalul mobil inteligent ca parte a sesiunii curente;

50. Pentru scenariul în care utilizatorul care a inițiat sesiunea a marcat explicit solicitarea ca fiind asincronă (răspunsul poate veni și după închiderea sesiunii curente), în cazul în care aplicația mobilă obiect pe care a lansat-o utilizatorul marchează implicit solicitarea ca putând fi și asincronă, sau în cazul în care mesajul de răspuns este primit după de expirarea termenului de time-out al sesiunii de lucru (sau după ce utilizatorul a închis aplicația), instanțele de portal sau serverul de aplicație generează o notificare care conține un hyperlink către mesajul răspuns, în format specific aplicației mobile sursă;

51. Notificarea este transmisă utilizatorului prin mijloace asimilate mesageriei colaborative structurate (printr-un mesaj de tip e-mail) sau prin intermediul unui apel la interfața de tip API oferită de componentele suitei EMM (care asigură și controlul aplicației obiect care a inițiat sesiunea, prin metode de tip wrapper sau prin integrare SDK), pentru accesare ulterioară;

52. După primirea notificării, fie prin mesageria colaborativă structurată, fie prin notificări mediate de suita EMM, utilizatorul va putea accesa referința de tip hyperlink care va

determina deschiderea aplicației obiect relevante (cu care s-a deschis sesiunea de lucru inițială) și mesajele de răspuns vor fi descărcate;

53. În cazul comunicării asincrone end-to-end, din rațiuni de securitate, se va putea configura o politică în limitele căreia mesajele vor putea fi descărcate exclusiv în mod “pull” (la solicitarea utilizatorului).

1.19.3.6 Aplicații

Furnizorul trebuie să asigure cel puțin 5 aplicații punctuale, accesibile de pe terminalele mobile, independente de platforma Big Data, cu rol de testare a Componentei de Acces, aspect important în condițiile în care, conform planificării, componenta va fi implementată anterior finalizării platformei. Aceste aplicații vor fi livrate ca parte integrantă a Componentei de Acces și vor permite accesarea securizată în condiții de mobilitate a unor seturi de date existente în depozitele de date comune, seturi de date ce vor fi stabilite de către beneficiar în etapa de analiză, de comun acord cu furnizorul. Fiecare dintre aceste aplicații de regăsire va valorifica date despre 1 entitate principală cu atributele aferente, respectiv alte entități cu care aceasta se află în relație, în condițiile în care atributele acestora sunt relevante pentru entitatea principală, dar nu pot fi asociate direct acesteia. Criteriile de regăsire și informațiile generate ca rezultat vor fi alese din cumulul de atribute menționate anterior. Design-ul fizic și cel conceptual al aplicațiilor va fi propus de furnizor și agreeat de beneficiar.

La sfârșitul perioadei de implementare a Componentei de Acces și a platformei Big Data, furnizorul trebuie să asigure cel puțin următoarele aplicații mobile:

- o versiune adaptată a componentei “*Enterprise search*” din cadrul platformei Big Data, cu soluții integrate de regăsire (“*full text search*”, “*spatial search*”, “*face recognition*”) și vizualizare corelată (“*guided navigation*”, “*detail view*”) a datelor accesibile la nivelul platformei;
- o versiune adaptată a modulelor de analiză avansată: “*link analysis*” și “*spatial analysis*”;
- o soluție de accesare a notificărilor cu evidențiere vizuală și / sau sonoră, transmise de către platforma Big Data.

2. Platforma Big Data

În vederea asigurării unei înalte disponibilități a sistemului, arhitectura tehnică va fi redundantă la nivelul componentelor sistemului, soluțiile furnizate fiind instalate și configurate pe echipamente în configurație tip cluster.

Infrastructura hardware a platformei Big Data prezentată în figura 3 este compusă din infrastructura mediului de producție și infrastructura mediului de testare/dezvoltare. Aceste infrastructuri sunt similare, diferența este făcută de performanțele echipamentelor hardware din componență. Descrierea, rolul și cerințele referitoare la toate componentele infrastructurii hardware ale platformei Big Data se găsesc în secțiunile ce urmează.

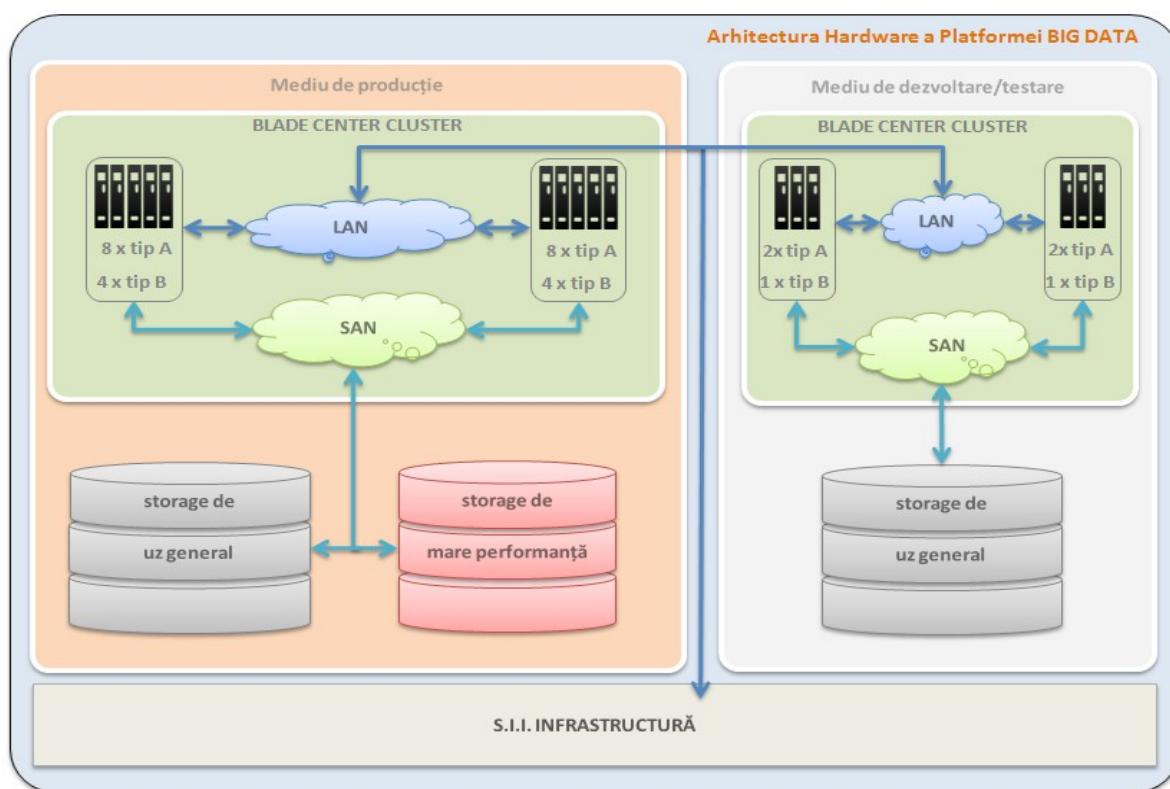


Figura 3: Infrastructura hardware conceptuală a platformei Big Data

Infrastructura software a platformei Big Data este bazată pe componente/module funcționale (respectiv, software COTS – *Commercial off the Shelf* – și/sau cod dezvoltat pe specificațiile proiectului) care să acopere toate funcționalitățile descrise, la nivel de arhitectură funcțională, în cadrul prezentului document.

2.1 Șasie de servere - pentru mediul de producție - (1 pachet)

2.1.1 Rol și context

- aceste șasie de servere vor face parte din infrastructura platformei Big Data, vor fi regrupate în perechi și vor acomoda modulele hardware de tip servere “blade” (Configurație A) și servere “blade” (Configurație B) alocate mediului de producție.

2.1.2 Cerințe funcționale și specificații tehnice

- unitățile de tip șasiu modular care fac parte din aceeași pereche vor fi echipate și configurate identic, și vor asigura în mod transparent, pentru serverele de tip “blade”, serviciile de alimentare cu energie, răcire/ventilare, serviciile de I/O, precum și serviciile de acces la platformele de management corespunzătoare;
- pentru legătura cu echipamentele de interconectare privată, de tip top-of-rack, fiecare unitate de tip șasiu modular va asigura un număr de porturi fizice cel puțin egal cu numărul maxim de servere de tip “blade” suportat, precum și o capacitate totală de I/O (throughput) extern cel puțin egală cu capacitatea totală a adaptoarelor din serverele instalate.

2.1.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va fi compus dintr-una sau mai multe perechi de unități de tip șasiu modular pentru servere de tip “blade”, iar șasiurile din fiecare pereche vor fi configurate și echipate identic;
- se va oferi o capacitate de I/O externă, către echipamentele de interconectare privată de tip top-of-rack, cel puțin egală cu cea configurată către serverele “blade” instalate în șasiu;
- fiecare șasiu modular va fi configurat și echipat cel puțin cu:
 - 2x module interne de I/O tip port-extender sau fabric extender;
 - fiecare modul intern de I/O va asigura cel puțin 4x căi de tip 40Gbps uplink către top-of-rack;
 - porturile de I/O se vor conecta la nivelul echipamentelor de interconectare privată (top-of-rack)
 - 4x surse de alimentare, în configurație redundată;
 - 4x module de racire / ventilare, în configurație redundată;

- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.2 Șasie de servere - pentru mediul de test / dezvoltare - (1 pachet)

2.2.1 Rol și context

- aceste șasie de servere vor face parte din infrastructura platformei Big Data, vor fi regrupate în perechi și vor acomoda modulele hardware de tip serverele “blade” (Configurație A) și serverele “blade” (Configurație B) alocate mediului de test / dezvoltare.

2.2.2 Cerințe funcționale și specificații tehnice

- unitățile de tip șasiu modular care fac parte din aceeași pereche vor fi echipate și configurate identic, și vor asigura în mod transparent, pentru serverele de tip “blade”, serviciile de alimentare cu energie, răcire/ventilare, serviciile de I/O, precum și serviciile de acces la platformele de management corespunzătoare;
- pentru legătura cu echipamentele de interconectare privată, de tip top-of-rack, fiecare unitate de tip șasiu modular va asigura un număr de porturi fizice cel puțin egal cu numărul maxim de servere de tip “blade” suportat, precum și o capacitate totală de I/O (“throughput”) extern cel puțin egală cu capacitatea totală a adaptoarelor din serverele instalate.

2.2.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va fi compus dintr-una sau mai multe perechi de unități de tip șasiu modular pentru servere de tip “blade”, iar șasiurile din fiecare pereche vor fi configurate și echipate identic;
- fiecare șasiu modular va fi configurat și echipat cel puțin cu:
 - 2x module interne de I/O tip port-extender sau fabric extender;
 - fiecare modul intern de I/O va asigura cel puțin 4x căi de tip 40Gbps uplink către top-of-rack;
 - porturile de I/O se vor conecta la nivelul echipamentelor de interconectare privată (top-of-rack)

- 4x surse de alimentare, în configurație redundată;
- 4x module de racire / ventilare, în configurație redundată;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.3 Servere “blade” (Configurație A), pentru mediul de producție - (16 buc.)

2.3.1 Rol și context

- serverele “blade” (Configurație A) alocate mediului de producție vor rula nativ instanțe ale soluției de virtualizare pentru a susține procesarea componentelor arhitecturii funcționale a platformei Big Data.

2.3.2 Configurație și dimensionare

16x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament de tip server “blade” (Configurație A);
- fiecare server “blade” (Configurație A) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E7 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 1TB RAM (scalabil la 2TB) DDR3 sau DDR4;
 - 2x 32GB medii de stocare de tip flash (sau echivalent) locale, amovibile, pentru instalarea hypervisorului;
 - 2x 40Gbps CNA;
 - porturile de I/O ale adaptoarelor CNA se vor conecta la nivelul șasiului de servere corespunzător;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, sau în șasiu modular pentru servere de tip “blade”, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.4 Servere “blade” (Configurație A), pentru mediul de testare/dezvoltare - (4 buc.)

2.4.1 Rol și context

- serverele “blade” (Configurație A și B) alocate mediului de test / dezvoltare vor rula nativ instanțe ale soluției de virtualizare pentru a susține mașinile virtuale care rulează mediile de dezvoltare integrate (IDE) și instanțele de test ale aplicațiilor necesare componentelor arhitecturii platformei Big Data.

2.4.2 Configurație și dimensionare

4x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament de tip server “blade” (Configurație A);
- fiecare server “blade” (Configurație A) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E7 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 1TB RAM (scalabil la 2TB) DDR3 sau DDR4;
 - 2x 32GB medii de stocare de tip flash (sau echivalent) locale, amovibile, pentru instalarea hypervisorului;
 - 2x 40Gbps CNA;
 - porturile de I/O ale adaptoarelor CNA se vor conecta la nivelul șasiului de servere corespunzător;
- vor fi incluse toate reperetele și subansamblurile necesare pentru montarea în rack, sau în șasiu modular pentru servere de tip “blade”, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.5 Servere “blade” (Configurație B), pentru mediul de producție - (8 buc.)

2.5.1 Rol și context

- serverele “blade” (Configurație B) alocate mediului de producție vor rula nativ instanțe ale soluției de virtualizare pentru a susține procesarea componentelor arhitecturii funcționale a platformei Big Data.

2.5.2 Configurație și dimensionare

8x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament de tip server “*blade*” (Configurație B);
- fiecare server “*blade*” (Configurație B) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E5 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 256GB RAM DDR3 sau DDR4;
 - 2x 32GB medii de stocare de tip flash (sau echivalent) locale, amovibile, pentru instalarea hypervisorului;
 - 2x 20Gbps CNA;
 - porturile de I/O ale adaptoarelor CNA se vor conecta la nivelul șasiului de servere corespunzător;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, sau în șasiu modular pentru servere de tip “*blade*”, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.6 Servere “*blade*” (Configurație B), pentru mediul de testare/dezvoltare - (2 buc.)

2.6.1 Rol și context

- serverele “*blade*” (Configurație A și B) alocate mediului de test/dezvoltare vor rula nativ instanțe ale soluției de virtualizare pentru a susține mașinile virtuale care rulează mediile de dezvoltare integrate (IDE) și instanțele de test ale aplicațiilor necesare componentelor arhitecturii platformei Big Data.

2.6.2 Configurație și dimensionare

2x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament de tip server “*blade*” (Configurație B);
- fiecare server “*blade*” (Configurație B) va fi configurat și echipat cel puțin cu:
 - 2 procesoare fizice Intel Xeon E5 (sau echivalent) 2GHz / 14-core / 35MB cache;
 - 256GB RAM DDR3 sau DDR4;

- 2x 32GB medii de stocare de tip flash (sau echivalent) locale, amovibile, pentru instalarea hypervisorului;
- 2x 20Gbps CNA;
- porturile de I/O se vor conecta la nivelul șasiului de servere corespunzător;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, sau în șasiu modular pentru servere de tip “blade”, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.7 Storage de mare performanță - (1 pachet)

2.7.1 Rol și context

- din rațiuni de asigurare a nivelului de performanță necesar, sistemul va fi alocat exclusiv componentelor critice de indexare a datelor în mediul de producție, respectiv pentru indecșii datelor obiect, pentru indexarea semantică, pentru suportul reprezentării dinamice a structurilor ierarhice și relaționale (de tip graf) și pentru reprezentarea dinamică GIS.

2.7.2 Cerințe funcționale și specificații tehnice

- cluster de tip “scale-out” format din perechi de unități active de tip controller, în care toate unitățile de tip controller din cluster vor opera în mod activ-activ, în arhitectură de tip “no single point of failure”;
- suport integrat pentru serviciu de stocare consolidată, care va putea aloca flexibil resursele disponibile, ca discuri virtuale, în arhitectură SAN, pentru toată capacitatea instalată;
- capacitate nativă de generare a copiilor de siguranță de tip snapshot, în puncte de consistență, pentru funcții de backup/recovery, cu suport nativ pentru platforme uzuale de virtualizare, de gestiune a bazelor de date și de aplicații;
- integrare la nivel API cu funcționalitățile de management al stocării oferite de soluția de virtualizare, precum și cu instanțele centrale de management general al acesteia;
- funcții integrate de compresie și deduplicare automată de date care să opereze inline, în timp real și la nivel global — pentru întreaga capacitate de stocare asigurată, inclusiv pentru datele reținute ca parte a copiilor de siguranță de tip snapshot —, precum și capacitate de supra-alocare nominală (thin provisioning) a capacității instalate;

- unități interne de stocare amovibile, exclusiv în tehnologie SSD de tip enterprise (componente optimizate pentru performanță individuală), care vor rezista la cel puțin 3-5 cicluri de scriere/ștergere pe zi, pe durata de viață;
- timp de răspuns specific liniar, sub 1ms, în mod independent de sarcina de I/O deservită, respectiv în condiții realiste de încărcare (efort tranzacțional susținut variabil, între minim și maxim);
- un mediu privat de back-end — dedicat, independent de mediile de tip LAN fabric și SAN fabric ale platformei Big Data —, de tip fabric redundant Infiniband, Ethernet, FC (sau echivalent), pentru interconectarea unităților de tip controller și partajarea metadate între toate nodurile active în cluster;
- cel puțin conectivitate 8Gbps FC și 10Gbps iSCSI în front-end, pentru acces tranzacțional de la nivel de host/server;
- posibilitatea de update și upgrade al elementelor software al platformei fără întreruperea serviciului, pentru asigurarea unui nivel optim de disponibilitate operațională, precum și creșterea capacității maxime de stocare prin adăugarea și reconfigurarea de componente hardware, fără a fi necesară ștergerea sau migrarea datelor stocate existente;
- funcționalități integrate, care să asigure o interfață unică de control și de gestiune centralizată a sistemului de stocare, care va putea fi accesată inclusiv folosind API-uri de tip REST, cu posibilitate de monitorizare și de administrare a configurării și reconfigurării, a alertelor specifice și a metricilor de performanță.

2.7.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x echipament de stocare de tip cluster cu 4 sau mai multe perechi de unități active, de tip controller;
- min. 240TB (raw, scalabilă la min. 320TB), prin utilizarea a cel puțin 150 unități SSD de tip enterprise, identice, distribuite echilibrat între perechile de unități active de tip controller;
- cel puțin 160TB capacitate utilă efectivă asigurată, fără a lua în calcul factori de multiplicare legați de deduplicare, compresie și thin-provisioning;
- min. 16 porturi 8Gbps FC, per cluster, pentru acces front-end;
- porturile de I/O FC se vor conecta la nivelul mediului de rețea dedicată SAN.
- min. 16 porturi 10Gbps iSCSI, per cluster, pentru acces front-end;

- porturile de I/O Ethernet se vor conecta la nivelul echipamentelor de interconectare privată (top-of-rack). throughput efectiv de min. 12GB/s pe total configurație;
- vor fi incluse toate reперele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.8 Storage de uz general, pentru mediul de producție - (1 pachet)

2.8.1 Rol și context

- sistemul va fi folosit pentru stocarea datelor obiect structurate (în sisteme de gestiune de baze de date) și nestructurate (cu acces la date la nivel de fișier), precum și pentru gestionarea imaginilor sistem (sistemele de operare ale serverelor).

2.8.2 Cerințe funcționale și specificații tehnice

- “*scale-up cluster model*” cu minim 1 pereche activă de unități de tip controller, în care toate unitățile de tip controller din cluster vor opera în mod activ-activ, în arhitectură de tip “*no single point of failure*”;
- suport integrat pentru serviciu de stocare consolidată și unificată, care va putea alocă flexibil resursele disponibile, între arhitecturi SAN și NAS — respectiv ca discuri virtuale, accesibile în rețea (fabric) SAN, și ca instanțe de tip file-server, cu acces partajat în rețea LAN —, pentru toată capacitatea instalată;
- capacitate nativă de generare a copiilor de siguranță de tip snapshot, în puncte de consistență, pentru funcții de backup/recovery, cu suport nativ pentru platforme uzuale de virtualizare, de gestiune a bazelor de date și de aplicații;
- integrare la nivel API cu funcționalitățile de management al stocării oferite de soluția de virtualizare, precum și cu instanțele centrale de management general al acesteia;
- funcții integrate de compresie și deduplicare automată de date care să opereze inline, în timp real și la nivel global — pentru întreaga capacitate de stocare asigurată, inclusiv pentru datele reținute ca parte a copiilor de siguranță de tip snapshot —, precum și capacitate de supra-alocare nominală (thin provisioning) a capacității instalate;

- unități interne de stocare amovibile, de tip SSD și HDD cu interfață SAS (optimizate pentru performanță individuală), precum și de tip SSD cu interfață SAS-NL (optimizate pentru capacitate individuală);
- protecția datelor stocate prin metode de tip RAID uzuale (cel puțin nivel 0, 1 și 6), precum și prin combinații ale acestora (cel puțin RAID 10), și utilizarea simultană a mai multe moduri de protecție RAID la nivelul aceluiași sistem;
- alocarea transparentă de resurse de tip “cache” de minim 2TB adresabil, pe baza de componente de tip flash/SSD dedicate incluse, pentru a facilita optimizarea accesului la date, în situații de vârf de sarcină și pentru schimbări bruște de regim de acces tranzacțional;
- funcționalități de tip QoS pentru funcțiile de stocare și de auto-tiering, care vor asigura prioritizarea selectivă a operațiilor de citire/scriere, la nivel de unități de stocare individuale de tip HDD și SSD, precum și relocarea transparentă a datelor în funcție de nivelul de utilizare a acestora, în funcție de necesarul de performanță al sarcinii active deservite, precum și în raport cu performanța și capacitatea componentelor sistemului de stocare respectiv implicate;
- pentru acces tranzacțional de la nivel de host/server, se va asigura cel puțin conectivitate 8/16Gbps FC sau 10Gbps iSCSI/Ethernet în SAN front-end, precum și 10Gbps pentru acces la servicii de tip NAS;
- posibilitatea de update și upgrade al elementelor software al platformei fără întreruperea serviciului, pentru asigurarea unui nivel optim de disponibilitate operațională, precum și creșterea capacității maxime de stocare prin adăugarea și reconfigurarea de componente hardware, fără a fi necesară ștergerea sau migrarea datelor stocate existente;
- funcționalități integrate, care să asigure o interfață unică de control și de gestiune centralizată a sistemului de stocare, care va putea fi accesată inclusiv folosind API-uri de tip REST, cu posibilitate de monitorizare și de administrare a configurării și reconfigurării, a alertelor specifice și a metricilor de performanță.

2.8.3 Configurație și dimensionare

1 1x pachet, integrat hardware/software

- fiecare pachet va include 1x echipament de stocare de tip cluster cu două sau mai multe unități active (de tip controller);
- configurație redundantă cu minim 2 unități de tip controller;
- min. 8 porturi de 16Gbps FC per controller;

- porturile de I/O FC se vor conecta la nivelul mediului de rețea dedicată SAN;
- min. 4 porturi de 10Gbps Ethernet per controller;
- porturile de I/O Ethernet se vor conecta la nivelul echipamentelor de interconectare privată (top-of-rack);
- min. 2TB cache, per configurație, pe baza a min. 10 unități Flash/SSD dedicate;
- min. 200TB (raw, dar nu mai puțin de 120TB capacitate utilă), prin utilizarea a cel puțin 25 unități SSD, 100 unități de disc SAS cu mecanica de 10K rpm și 25 unități de disc SAS-NL cu mecanică 7K rpm;
- vor fi incluse toate reперele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.9 Storage de uz general, pentru mediul de test/dezvoltare - (1 pachet)

2.9.1 Rol și context

- sistemul va fi folosit pentru stocarea datelor obiect și pentru gestionarea imaginilor sistem, ca sistem dedicat testării și dezvoltării aplicațiilor, separat de mediul de producție.

2.9.2 Cerințe funcționale și specificații tehnice

- “*scale-up cluster model*” cu minim 1 pereche activă de unități de tip controller, în care toate unitățile de tip controller din cluster vor opera în mod activ-activ, în arhitectură de tip “*no single point of failure*”;
- suport integrat pentru serviciul de stocare consolidată și unificată, care va putea alocă flexibil resursele disponibile, între arhitecturi SAN și NAS — respectiv ca discuri virtuale, accesibile în rețea (fabric) SAN, și ca instanțe de tip file-server, cu acces partajat în rețea LAN —, pentru toată capacitatea instalată;
- capacitate nativă de generare a copiilor de siguranță de tip snapshot, în puncte de consistență, pentru funcții de backup/recovery, cu suport nativ pentru platforme uzuale de virtualizare, de gestiune a bazelor de date și de aplicații;
- integrare la nivel API cu funcționalitățile de management al stocării oferite de soluția de virtualizare, precum și cu instanțele centrale de management general al acesteia;

- funcții integrate de compresie și deduplicare automată de date care să opereze inline, în timp real și la nivel global — pentru întreaga capacitate de stocare asigurată, inclusiv pentru datele reținute ca parte a copiilor de siguranță de tip snapshot —, precum și capacitate de supra-alocare nominală (thin provisioning) a capacității instalate;
- unități interne de stocare amovibile, de tip SSD și HDD cu interfață SAS (optimizate pentru performanță individuală), precum și de tip SSD cu interfață SAS-NL (optimizate pentru capacitate individuală);
- protecția datelor stocate prin metode de tip RAID uzuale (cel puțin nivel 0, 1 și 6), precum și prin combinații ale acestora (cel puțin RAID 10), și utilizarea simultană a mai multe moduri de protecție RAID la nivelul aceluiași sistem;
- alocarea transparentă de resurse de tip “cache” de minim 2TB adresabil, pe baza de componente de tip flash/SSD dedicate incluse, pentru a facilita optimizarea accesului la date, în situații de vârf de sarcină și pentru schimbări bruște de regim de acces tranzacțional;
- funcționalități de tip QoS pentru funcțiile de stocare și de auto-tiering, care vor asigura prioritizarea selectivă a operațiilor de citire/scriere, la nivel de unități de stocare individuale de tip HDD și SSD, precum și relocarea transparentă a datelor în funcție de nivelul de utilizare a acestora, în funcție de necesarul de performanță al sarcinii active deservite, precum și în raport cu performanța și capacitatea componentelor sistemului de stocare respectiv implicate;
- pentru acces tranzacțional de la nivel de host/server, se va asigura cel puțin conectivitate 8/16Gbps FC sau 10Gbps iSCSI/Ethernet în SAN “front-end”, precum și 10Gbps pentru acces la servicii de tip NAS;
- posibilitatea de update și upgrade al elementelor software ale platformei fără întreruperea serviciului, pentru asigurarea unui nivel optim de disponibilitate operațională, precum și creșterea capacității maxime de stocare prin adăugarea și reconfigurarea de componente hardware, fără a fi necesară ștergerea sau migrarea datelor stocate existente;
- funcționalități integrate, care să asigure o interfață unică de control și de gestiune centralizată a sistemului de stocare, care va putea fi accesată inclusiv folosind API-uri de tip REST, cu posibilitate de monitorizare și de administrare a configurării și reconfigurării, a alertelor specifice și a metricilor de performanță.

2.9.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x echipament de stocare de tip cluster cu două sau mai multe unități active (de tip *controller*);
- configurație redundantă cu minim 2 unități de tip controller;
- min. 4 porturi de 16Gbps FC per controller;
- porturile de I/O FC se vor conecta la nivelul mediului de rețea dedicată SAN;
- min. 2 porturi de 10Gbps Ethernet per controller;
- porturile de I/O Ethernet se vor conecta la nivelul echipamentelor de interconectare privată (top-of-rack);
- min. 2TB cache, per configurație, pe baza a min. 10 unități Flash/SSD dedicate;
- min. 100TB (raw, dar nu mai puțin de 60TB capacitate utilă), prin utilizarea a cel puțin 10 unități SSD, 50 unități de disc SAS cu mecanica de 10K rpm și 25 unități de disc SAS-NL cu mecanică 7K rpm;
- vor fi incluse toate repererele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.10 Interconectare privată (top-of-rack) - (4 pachete)

2.10.1 Rol și context

- la acest nivel se va asigura interconectarea locală a echipamentelor de tip șasiu de servere “*blade*”, între ele și cu sistemele de stocare, precum și cu infrastructura de rețea existentă (aflată în exploatare), prin intermediul echipamentelor din mediul de rețea locală LAN (parte a infrastructurii platformei Big Data).

2.10.2 Cerințe funcționale și specificații tehnice

- interconectarea privată se va realiza prin perechi de echipamente de tip switch, identic configurate, care vor îndeplini următoarele cerințe minime:
 - arhitectură internă care să ofere o capacitate de comutare la viteza maximă suportată pe toate interfețele simultan precum și latența minimă, folosind tehnologii de comutare de tip “*cut-through*”;

- pentru a asigura integrarea în arhitectura generală precum și transmiterea datelor în condiții de maximă calitate și eficiență, echipamentele vor suporta următoarele tehnologii și tipuri de interfețe:
 - *“Converged Enhanced Ethernet”* as *“Lossless Ethernet”* - suita de protocoale (IEEE 802.1Qbb, IEEE 802.1Qaz, IEEE 802.1Qau și DCBX) care facilitează transmiterea datelor în rețelele datacenter folosind interfețe de tip Ethernet 10 Gigabit sau 40 Gigabit;
 - interfețe unificate capabile să suporte atât tehnologii de tip Ethernet (10 Gigabit Ethernet, 40 Gigabit Ethernet, Fibre Channel over Ethernet) precum și Fibre Channel nativ la viteze de 8 Gbps și 16 Gbps;
- echipamentele vor funcționa în mod cluster de tip activ-activ, oferind administratorului o interfață unică de administrare precum și conectivitate de tip IP/Ethernet și de tip FC/FCoE serverelor instalate în *“Șasie de servere”* către restul componentelor de procesare și stocare ale sistemului;
- pe toate tipurile de comunicație pentru care se asigură suport, la nivelul fiecărei perechi de echipamente de tip switch top-of-rack, arhitectura de interconectare va presupune cel mult un hop intermediar între oricare șasiu și alt șasiu, respectiv între oricare șasiu și echipamentele de tip switch SAN existente.

2.10.3 Configurație și dimensionare

4x pachete, integrate hardware/software

- fiecare pachet va include 1x echipament de tip switch, de tip top-of-rack, pentru interconectare convergentă (multi-serviciu, respectiv cel puțin Ethernet și FC) în rețea locală;
- fiecare echipament va fi licențiat (în cazul în care este necesară licențierea), configurat și echipat cel puțin cu:
 - 24x porturi 40Gbps Ethernet cu interfețe modulare;
 - porturile de I/O de 40Gbps interconectează șasiile de servere și asigură uplink către mediul local LAN
 - 12x porturi 4/8/16Gbps FC cu interfețe modulare;
 - porturile de I/O FC se vor conecta la nivelul mediului de rețea dedicată SAN
 - 4x 1/10Gbps Ethernet cu interfețe modulare;

- porturile de I/O de 1/10Gbps interconectează porturile din echipamentele de stocare
 - 2x surse de alimentare, în configurație redundantă;
 - 2x module de racire / ventilare, în configurație redundantă.
- echipamentele vor fi echipate și configurate identic, și vor fi utilizate în perechi, pentru a asigura o structură de interconectare privată (top-of-rack) de tip fabric dual, redundant;
 - va fi inclusă licențierea necesară pentru componente și funcționalități software care să permită administrarea celor două perechi de echipamente switch ca un pe un tot unitar;
 - vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.11 LAN Fabric - (2 buc.)

2.11.1 Rol și context

- mediul de rețea locală LAN (parte a infrastructurii platformei Big Data) va asigura suportul de interconectare locală a echipamentelor de tip șasiu de servere “*blade*”, între ele și cu sistemele de stocare, precum și cu infrastructura de rețea existentă (aflată în exploatare).

2.11.2 Cerințe funcționale și specificații tehnice

- mediul de rețea locală LAN se va realiza din cel puțin două blocuri funcționale de tip switch, identic configurate, a căror arhitectură internă să ofere o capacitate de comutare la viteza maximă suportată pe toate interfețele simultan precum și latența minimă, folosind tehnologii de comutare de tip “*cut-through*”;
 - interfețe modulare capabile să suporte tehnologii de tip 40 Gigabit Ethernet;
 - să implementeze în modulele de interfață funcții de control al traficului folosind politici și liste de control a accesului pentru niveluri ISO OSI 2, 3 și 4, atât pentru protocolul IPv4 cât și pentru protocolul IPv6;
 - să ofere suport pentru protocolul Fibre Channel over Ethernet (FCoE);
 - să permită oricărui echipament extern conectarea la cele două blocuri funcționale cu multiple interfețe de 40 Gigabit Ethernet, ce fac parte dintr-un singur grup de agregare a porturilor;

- să suporte protocoalele de rutare OSPFv2, OSPFv3, BGPv4 și IS-IS, precum și protocoalele VXLAN, OpenFlow și Netconf.

2.11.3 Configurație și dimensionare

2x bucăți, integrate hardware/software

- fiecare bucată va include 1x echipament de tip switch de agregare;
- fiecare echipament de tip switch de agregare va fi configurat și echipat cel puțin cu:
 - 16x porturi 40Gbps Ethernet QSFP;
 - porturile de I/O de 40Gbps interconectează componentele de tip top-of-rack și serverele Tip 2;
 - legăturile (uplink) către rețeaua existentă se vor implementa tot prin porturi I/O de 40Gbps;
 - 2x surse de alimentare, în configurație redundantă;
 - 2x module de racire / ventilare, în configurație redundantă;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.12 Platforma de back-up - (1 pachet)

2.12.1 Rol și context

- bibliotecă de unități de bandă magnetică ("*tape library*"), pentru generarea și managementul copiilor de siguranță (back-up), ale imaginilor sistem și ale volumelor de date obiect, pe unități de bandă (tape media) amovibile;
- va asigura licențele software necesare realizării copiilor de siguranță a sistemelor/instanțelor virtuale, precum și a aplicațiilor din mediul de producție și din cel de testare/dezvoltare ale modulelor funcționale de analiză avansată a datelor, la nivelul platformei Big Data;
- va asigura licențele software necesare realizării copiilor de siguranță a sistemelor/instanțelor virtuale, precum și a aplicațiilor care fac parte din modulele funcționale ale nivelului CORE (offline), din Componenta de Acces.

2.12.2 Cerințe funcționale și specificații tehnice

- bibliotecă de unități de bandă, cu următoarele caracteristici:
 - suport pentru tehnologie LTO-7;
 - suport hardware intern pentru criptare AES-256;
 - suport pentru virtualizare (partiționare) internă;
 - 500TB capacitate de salvare (back-up) date în format nativ (fără compresie);
 - 1.5PTB capacitate de salvare (back-up) date comprimate;
 - 10 TB/Hr throughput, pentru date salvate în format nativ (fără compresie);
 - 25 TB/Hr throughput, pentru salvare date compimate;
 - interfețe de acces date de tip SAS (min. 6Gbps) și FC (min. 8Gbps);
 - suport pentru montare în rack standard de 19in;
- va fi instalată fizic și va funcționa în rack standard de 19in (existent la beneficiar);
- soluția va include componenta software de tip server de back-up, care va permite coordonarea generării și transferării pe bandă a imaginilor de back-up.
 - funcționalitățile de tip server de backup vor asigura compatibilitate cu sistemele de stocare de uz general și de mare performanță din infrastructura mediului de producție.
 - funcționalitățile de tip server de backup vor asigura suport specific pentru sisteme de aplicații, sisteme de gestiune a bazelor de date și pentru platforme de virtualizare.
 - integrarea va acoperi managementul generării de copii instant, de tip snapshot, pe sistemele de stocare și transformarea acestora în imagini de back-up valide (consistent).
 - generarea imaginilor de backup și scrierea se vor face direct de pe sistemele de stocare, fără trafic pe rețelele locale LAN și fără a fi necesar transferul datelor pe sisteme intermediare.

2.12.3 Configurație și dimensionare

1x pachet, integrat hardware/software

- fiecare pachet va include 1x echipament de tip bibliotecă de bandă pentru realizare de copii de siguranță (back-up) pe medii magnetice amovibile;
- echipamentul va fi configurat și echipat cel puțin cu:
 - 8 partiții interne;
 - 4 unități de bandă (tape drive) interne;

- 100 sloturi (pentru unități de bandă) interne;
 - 100 unități de bandă (tape media) LTO-7;
 - 10 unități de bandă de curățare;
 - 2x interfețe FC 8Gbps cu conectorizare optică;
 - porturile de I/O FC se vor conecta la nivelul mediului de rețea dedicată SAN
- licențierea componentei software de tip server de back-up nu va introduce limitări în legătură cu numărul sau cu calendarul operațiilor de generare și de transfer de imagini de back-up pe bandă.
 - licențierea componentei software de tip server de back-up nu va introduce limitări în legătură cu dimensiunea imaginilor de back-up ce pot fi generate și nici cu volumul total de date de vor putea fi arhivate
 - vor fi incluse toate reperatele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2.13 Licențe platformă Big Data - (1 pachet)

În funcție de modelul specific aplicabil, la nivel de componentă/modul, infrastructura software a platformei Big Data va fi licențiată pentru asigurarea nevoilor proiectului, respectiv cel puțin pentru utilizarea platformei, în mod concurent, de către cel puțin 500 de utilizatori. Licențierea nu va introduce limitări ale numărului total de utilizatori unici în catalog.

În cazul în care modelul specific aplicabil va presupune licențierea pe unitate de putere de calcul alocată — de exemplu, la nivel de număr de unități de tip procesor fizic (multi-nucleu), sau la nivel de număr de unități de tip nuclee de procesare (CPU-core) —, atunci:

- în infrastructura hardware se va aloca cel puțin puterea de calcul efectiv necesară pentru utilizarea platformei, în mod concurent, de către cel puțin 500 de utilizatori în condițiile de performanță optimă necesare proiectului;
- se va licenția utilizarea componentelor/modulelor funcționale vizate, fără alte restricții, pentru toată puterea de calcul respectiv alocată.

În cazul în care modelul specific aplicabil pentru anumite componente/module funcționale va presupune licențierea în funcție de volumul de metadate de lucru specifice — de exemplu, de tip indecși de date, indecși semantici sau de reprezentare — care vor fi create și utilizate de platformă, atunci:

- se vor asigura componentei/modulului funcțional resursele de stocare efectiv necesare;
- se va licenția utilizarea componentelor/modulelor funcționale vizate, fără alte restricții, pentru toată capacitatea de stocare necesară.

Infrastructura software a platformei Big Data va fi licențiată, în ansamblul său, pentru utilizarea completă a infrastructurii hardware de procesare alocate, dar nu mai puțin de 672 unități de tip nuclee de procesare (CPU-core).

Licențierea trebuie să acopere toate funcționalitățile descrise în caietul de sarcini - secțiunile 2.18 și 2.19.

2.14 Licențe sistem monitorizare - (1 pachet)

Licențierea trebuie să acopere toate funcționalitățile descrise în secțiunea 2.21, precum și echipamentul hardware dedicat ("*gateway*" de SMS):

- cu următoarele funcționalități:
 - funcționalitate "*email to SMS*" și "*SMS to Email*";
 - funcționalitate de monitorizare de servicii (web, mail) cu alertare pe SMS;
 - funcționalitate de "*auto-reply*" pentru SMS-urile primite;
 - suport pentru mai mulți utilizatori (casuță de mesaje proprie, Inbox/Outbox);
 - posibilitatea de importare a contactelor prin CSV;
 - posibilitatea de planificare a mesajelor transmise;
 - posibilitatea de definire de șabloane de mesaje;
 - suport pentru unicode;
 - suport pentru mesaje SMS formate din mai multe părți;
 - funcționalitate de HTTP API pentru folosirea în cadrul altor sisteme și aplicații;
 - interfață de management Web;
 - client NTP și SNMP;
 - mecanism de "*watchdog*" pentru modemul 3G;
 - suport pentru HTTPS;
 - suport "*clustering HA*" prin folosirea a două unități similare.
- cu următoarele specificații tehnice:

- 3G modem încorporat, UMTS 2100/900MHz, GSM/GPRS 850/900/1800/1900MHz;
- 1 Sim card;
- 4GB flash drive;
- antena omnidirecțională, 3.5dBi, conector SMA;
- alimentare 100–240V AC;
- temperatură de operare între 0 și 60°C.

2.15 Licențe modul Face Recognition, pentru 3.000.000 de subiecți - (1 pachet).

Licențierea va acoperi cel puțin 3.000.000 de regăsiri de subiecți unici, fără alte restricții, precum și toate funcționalitățile descrise în secțiunea 2.20.

2.16 Licențe platformă de virtualizare - platforma Big Data - (30 buc.)

2.16.1 Rol și context

- soluția de virtualizare va putea fi instalată pe tipurile de servere ale platformei Big Data, pentru a asigura abstractizarea infrastructurii hardware față de mașinile virtuale configurate, respectiv pentru a reduce dependența, în exploatare, a instanțelor funcționale virtualizate de starea echipamentelor hardware, precum și pentru a implementa funcționalitățile de management (inclusiv pe cele de asigurare a disponibilității operaționale) și de securitate la acest nivel.

2.16.2 Cerințe funcționale

- virtualizare sistem bazată pe hypervisor de Tip 1 (*“bare-iron”*) sau echivalent, optimizat pentru platforme de clasă server;
- management integrat, pentru configurații scalabile eterogene (de tip multi-nod, multi-hypervisor, multi-instanță) al nivelului virtualizare;
- soluția va oferi un mediu intern de comunicație de rețea integrat, distribuit între toate serverele interconectate care rulează instanțe hypervisor administrate de același centru de management;

- soluția va asigura posibilitatea de configurare a relocării dinamice automate a instanțelor de mașini virtuale, între serverele care rulează instanțe hypervisor administrate de același centru de management, în funcție de indicatori de stare, de încărcare sau de disponibilitate;

- soluția oferită va asigura monitorizarea și administrarea alocării și utilizării resurselor disponibile, cel puțin în ceea ce privește:

- identificarea și limitarea utilizării de resurse de stocare și de procesare, de către mașinile virtuale, pe bază de politici;
- identificarea consumului de resurse specifice, la nivel de mașină virtuală și, respectiv, pe categorii de resurse;
- identificarea de resurse, inclusiv de tip RAM și procesor, ne-alocate sau supra-rezervate, pentru a permite optimizarea alocării acestora;
- corelarea schimbărilor de configurație, la nivelul sistemelor virtualizate, cu impactul acestora asupra nivelului de utilizare a resurselor;
- urmărirea evoluției nivelului de utilizare a resurselor și semnalizarea situațiilor de depășire a limitelor de capacitate;
- asigurarea disponibilității operaționale a mașinilor virtuale și load-balancing, pe bază de politici, între instanțele de hypervisor (hypervisor host);
- reconfigurarea, realocarea și migrarea mașinilor și a discurilor virtuale, pentru a optimiza performanța acestora și utilizarea resurselor hardware alocate;
- funcționalități integrate de tip Software Defined Network, Software Defined Storage și mecanisme integrate de host provisioning;
- mecanisme de tip portal de self-service, cu sistem integrat de acces la resurse pe bază de roluri și cu posibilitatea de definire de limite (cote);
- platforma de virtualizare va permite managementul și optimizarea alocării de resurse partajate, cel puțin la nivel de RAM și de discuri, respectiv:
 - posibilitatea de partajare granulară, la nivel de unitate de alocare, între mașinile virtuale definite;
 - posibilitatea de supra-alocare logică flexibilă, peste limitele nominale ale echipamentului hardware;

- interfața de management va permite controlul și automatizarea configurării, operării și migrării de componente, respectiv pentru mașinile virtuale și pentru infrastructurile virtuale;

- soluția oferită va asigura accesarea și automatizarea utilizării tuturor comenzilor de management ale platformei de virtualizare prin interfețe de control API.

2.16.3 Configurație și dimensionare

30x bucăți licențe software

- fiecare bucată va include câte 1x licență, iar fiecare licență va acoperi instalarea soluției de virtualizare pe un echipament hardware de tip server dual-socket, cu procesoare de tip x86_64;
- este considerată echivalentă varianta în care, datorită specificului licențierii producătorului respectiv, se va oferta cel puțin 1x complet care va include licențiere dimensionată pentru instalarea soluției de virtualizare pe cel puțin 30 de echipamente hardware de tip server dual-socket, cu procesoare de tip x86_64;
- licențierea va include și cel puțin 2 instanțe de tip consolă de management pentru soluția de virtualizare.

2.17 Licențe sistem de operare - platforma Big Data - (40 bucăți)

2.17.1 Rol și context

- soluția software de tip sistem de operare va putea fi instalată pe toate tipurile de servere ale platformei Big Data, precum și la nivelul instanțelor de mașini virtuale configurate, pentru a asigura abstractizarea infrastructurii hardware față de infrastructura software de aplicație (SGBD, middleware), precum și pentru a implementa funcționalitățile de management și de securitate la acest nivel.

2.17.2 Configurație și dimensionare

40x bucăți licențe software

- fiecare bucată va include câte 1x licență, iar fiecare licență va acoperi o instanță software pentru sistem de operare de tip server, respectiv instalată pe echipament hardware de tip server dual-socket, cu procesoare de tip x86_64, sau pe sistem virtual echivalente;
- este considerată echivalentă varianta în care, datorită specificului licențierii producătorului respectiv, se va oferta cel puțin 1x complet care va include licențiere dimensionată pentru cel puțin 40 de instanțe software de tip sistem de operare pentru server,

care vor fi respectiv instalate pe echipamente hardware de tip server dual-socket, cu procesoare de tip x86_64, sau pe sisteme virtuale echivalente.

2.18 Instalare și configurare infrastructură platformă Big Data - (1 serviciu)

Infrastructura hardware (menționată în secțiunile 2.1 - 2.11) și software (menționată în secțiunile 2.13, 2.16 și 2.17), a platformei Big Data trebuie să fie astfel instalată și configurată încât să permită implementarea unei arhitecturi segregate pe verticală și pe orizontală, la un nivel optim de granularitate, astfel încât să poată fi anticipate, prin scalabilitate și flexibilitate, eventuale cerințe ulterioare ale beneficiarilor.

2.19 Servicii de implementare platformă Big Data - (1 serviciu)

Platforma Big Data sunt acceptate doar soluțiile care:

- implementează "*out-of-the-box*", cel puțin în proporție de 80%, un subset din cerințele funcționale aferente platformei Big Data, definite și cuantificate prin intermediul grilei de punctaj din cadrul **Anexei 1 - Specificații sesiune demonstrativă**;
- oferă o arhitectură scalabilă, modulară, flexibilă și deschisă, care să permită întregirea funcționalităților solicitate prin prezentul caiet de sarcini, prin dezvoltări pe perioada de implementare a proiectului.

2.19.1 Cerințe generale

Soluția tehnică de implementare a platformei de analiză avansată a volumelor mari de date - Big Data, se va conforma unui set minim de cerințe generale, sens în care trebuie:

- să se bazeze pe o platformă consacrată din punct de vedere tehnologic, care să permită customizări ulterioare astfel încât să poată asigura toate funcționalitățile solicitate de beneficiar prin intermediul prezentului caiet de sarcini;
- să utilizeze tehnologii moderne de stocare, indexare și procesare întâlnite preponderent în domeniul Big Data, precum MapReduce și calcul in-memory;
- să fie dimensionată din punct de vedere hardware și software astfel încât să asigure accesul unui număr minim de 500 utilizatori concurenți, la un volum de date de minim 30 TB, cu o creștere anuală de 6 TB;

- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"full text search"*;
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"spatial search"*;
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"query builder"*;
- să asigure o medie a timpului de răspuns de sub 10 secunde, în condițiile în care se vor efectua 10.000 de regăsiri într-un interval de 60 minute, pentru *"face recognition"*;
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"link analysis"*;
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"spatial analysis"*;
- să asigure o medie a timpului de răspuns de sub 30 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"semantic analytics"*;
- să asigure o medie a timpului de răspuns de sub 60 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru *"behavioral analytics"*;
- să asigure integrarea cu Portalului web existent⁵, administrat de beneficiar, achiziționat și configurat în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea unui punct unic de acces centralizat la instrumentele software grafice furnizate;
- să asigure integrarea cu soluția de control acces existentă⁶, administrată de către beneficiar, achiziționată și configurată în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea autentificării unice⁷ și autorizării pe bază de roluri și permisiuni;

⁵ Oracle WebCenter Portal, versiunea 11.1.1.8

⁶ Oracle Acces Manager, versiunea 11.1.2.2

⁷ Single Sign On

- să asigure integrarea cu soluția existentă de management al identității⁸, administrată de către beneficiar, achiziționată și configurată în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea condițiilor necesare unui management centralizat și reutilizare a utilizatorilor, profilurilor asociate acestora, respectiv organizațiilor existente.

2.19.2 Cerințe funcționale

Platforma Big Data, suplimentar faptului că *trebuie să se conformeze cerințelor generale definite în secțiunile și subsecțiunile anterioare*, trebuie să se bazeze pe o soluție tehnică *end-to-end* modernă și customizabilă, care să respecte cele mai bune practici în materie, sens în care trebuie să asigure:

- integrarea depozitelor de date comune, prin procese de accesare, preluare, transformare, procesare, încărcare și / sau indexare într-un nou depozit de date propriu platformei Big Data;
- integrarea depozitelor de date comune prin fluxuri de acces federativ, cu sau fără replicarea acestora într-o zonă tampon internă depozitului de date propriu platformei Big Data;
- mecanisme optime de sincronizare a depozitelor de date comune, cu depozitul de date propriu platformei Big Data și în condițiile în care acestea au o frecvență diferită de actualizare: în timp real sau aproape în timp real, în lot, masiv;
- integrare seturilor de date individuale, în depozitul de date propriu platformei Big Data;
- corelarea depozitelor de date comune și a seturilor de date individuale sub o formă unică de vizualizare;
- prelucrarea și procesarea pozelor existente în depozitele de date comune, respectiv indexarea acestora în depozitul de date propriu platformei Big Data, în vederea susținerii funcționalității *"face recognition"*;
- valorificarea, într-o manieră completă și coerent corelată a depozitelor de date comune și a seturilor de date individuale, oferind utilizatorului posibilitatea să interogheze întregul volum de date existent printr-o singură operație de regăsire, să exploreze rezultatul într-o manieră unificată, prin intermediul mai multor forme de vizualizare și analiză, respectiv să reseteze criteriile de filtrare utilizate;

⁸ Oracle Identity Management, versiunea 11.1.1.7

- adaptori standard de comunicare cu componenta de acces securizat în condiții de mobilitate, precum și cu alte sisteme informatice, prin schimb de mesaje în format XML și / sau JSON - fără a se limita la acestea;

- desfășurarea unui proces investigativ utilizând componente specializate ce asigură interacțiunea utilizatorilor finali cu platforma Big Data printr-un set de instrumente software avansate de regăsire, vizualizare, analiză, colaborare, avertizare și extragere a rezultatului obținut sub formă de rapoarte concise dar cuprinzătoare, precum:

- regăsirea informațiilor utilizând limbajul natural;
- regăsirea informațiilor folosind soluții de tip *"face recognition"*;
- rafinarea rezultatelor prin clasificarea informațiilor;
- navigarea în adâncime, printr-o parcurgere ierarhică nivel cu nivel a rezultatelor;
- vizualizarea tuturor detaliilor asociate fiecărei înregistrări din rezultat;
- analiza avansată prin dispunerea grafică a obiectelor, proprietăților și relațiilor;
- analiza avansată prin dispunerea pe hartă a metadatelor geospațiale aferente obiectelor, proprietăților și relațiilor;
- extragerea automată a obiectelor, proprietăților și relațiilor din conținut nestructurat;
- analiza semantică a datelor;
- analiza avansată utilizând comportamente pe baza cărora pot fi identificate, vizualizate și monitorizate obiecte ce se încadrează într-un tipar;
- generarea de notificări pe baza unui *"watchlist"* compus din entități, sau pe baza de comportamente;
- îmbogățirea procesului de analiză, prin achiziția unor seturi de date individuale, precum și prin etichetarea conținutului nestructurat;
- exportul informațiilor în diferite formate text sau imagine, funcție de tipul și forma de prezentate a acestora;
- construirea unui spațiu privat prin gruparea analizei în investigații, salvarea și administrarea rezultatului analizei, a căutărilor și a notificărilor proprii, precum și extragerea rezultatului analizei sub formă de rapoarte concise dar cuprinzătoare;

- identificarea / vizualizarea sursei de date aferentă fiecărei informații accesibilă utilizatorului final la nivelul platformei Big Data, indiferent de forma de prezentare a acesteia în cadrul soluțiilor de regăsire, vizualizare și / sau analiză;
- facilități avansate de personalizare a interfeței grafice, oferind utilizatorului acces la o zonă de preferințe care să permită, spre exemplu, configurarea paginii de reședință ("*home page*") și relevanța ce determină ordinea de afișare a înregistrărilor returnate de procesul de regăsire - fără a se limita la acestea;
- facilități avansate de personalizare a structurilor tabelare, oriunde apar ele la nivelul interfeței grafice ca, spre exemplu:
 - afișarea, ascunderea, re poziționarea și înghețarea coloanelor;
 - auto-dimensionarea și modificarea manuală a dimensiunii coloanelor;
 - configurarea modului de paginare a informației afișate;
- facilități avansate de procesare a datelor afișate în structuri tabelare, oriunde apar ele la nivelul interfeței grafice ca, spre exemplu:
 - funcții de agregare pe una sau mai multe dimensiuni (ex.: count, min, max, sum, average);
 - linii de rezumare a rezultatului agregării, funcție de valoarea unei dimensiuni sau funcție de valorile din tot tabelul;
Exemplu: - în cazul agregării datelor după oraș și județ, folosind ca metrică numărul de cetățeni, să se poată vizualiza, într-o linie de rezumare, valoarea totală a numărul de cetățeni grupat pe oraș, județ, respectiv la nivel național;
 - evidențierea grafică a unor valori ce respectă structuri condiționale complexe;
Exemplu: – evidențierea tuturor orașelor cu populație mai mare de x locuitori;
 - sortare simplă și sortare multiplă a datelor;
 - filtrare inline - structură specializată care apare ca o linie nouă în tabel:
 - pentru fiecare coloană se poate construi o condiție prin introducerea unui operator sub formă de caracter sau grup de caractere;
 - operatorul introdus se aplică diferențiat funcție de tipul de dată din coloană;
 - între valorile introduse în coloane, se aplică operatorul AND;
 - constructor de filtru - structură specializată care, în linii mari, permite construirea grafică a unui filtru complex folosind toate coloanele disponibile;

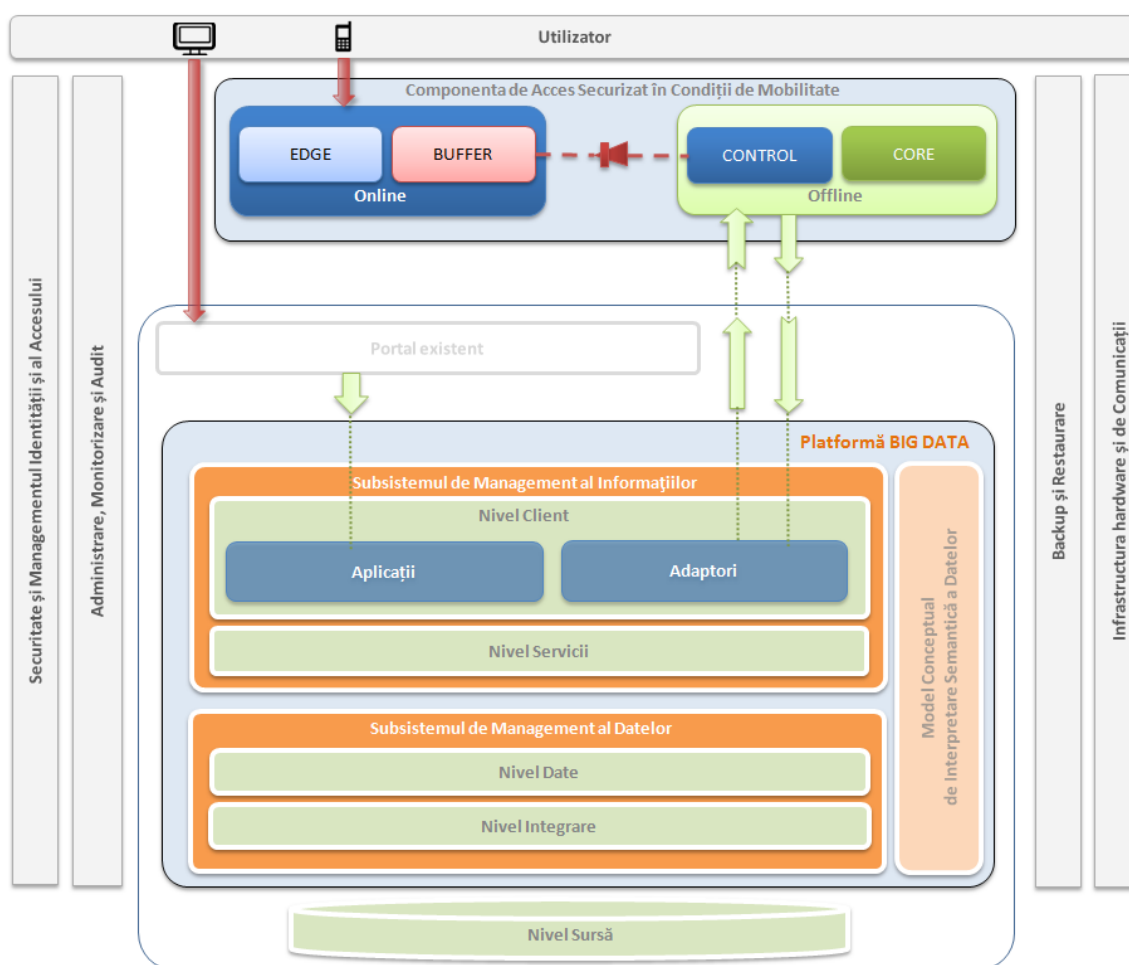
- pentru fiecare coloană se pot defini condiții multiple prin selectarea operatorilor dintr-o listă predefinită și introducerea unei valori;
 - lista de operatori este personalizată în funcție de tipul de dată din coloană;
 - operatorul ales se aplică diferențiat funcție de tipul de dată din coloană;
 - între condiții se aplică, la alegere, operatorii AND sau OR;
 - condițiile pot fi grupate astfel încât să permită construirea unor filtre imbricate;
- definirea unor noi coloane, prin intermediul cărora să poată fi vizualizat rezultatul aplicării unor formule asupra valorilor coloanelor fiecărei linii din tabel;
Exemplu: – definirea unei coloane NUME_PRENUME, prin concatenarea valorilor din coloanele NUME și PRENUME;
 - exportul setului de date în diferite formate, printre care: XLS, XML, HTML și PDF;
 - generarea unor forme grafice de vizualizare de tip CHART, prin alegerea dinamică a dimensiunilor aplicate pe fiecare axă;
- acces partajat la informații în funcție de sursa de date, mediat de interfața grafică;
 - acces partajat și securizat la funcționalități, blocuri și / sau module funcționale.

2.19.3 Arhitectura funcțională

Noul sistem informatic de integrare și valorificare operațională și analitică a volumelor mari de date, în ansamblul său, trebuie să susțină scopul și obiectivele proiectului. În acest sens trebuie să cuprindă infrastructurile de comunicații, hardware și software atât pentru platforma Big Data cât și pentru componenta de acces securizat în condiții de mobilitate, astfel încât să asigure instrumente software de valorificare operațională și analitică și să permită interoperabilitate cu mediul IT administrat de beneficiar⁹, achiziționat și configurat în cadrul proiectului "SII INFRASTRUCTURĂ".

Arhitectura logic-funcțională generală a sistemului informatic descris în cadrul acestui proiect, este prezentată, într-o manieră sumară, în figura următoare:

⁹ vezi capitolele 2.22 Servicii de integrare cu portalul și access management și 2. Interconectare LAN existent



Arhitectura logic-funcțională generală a sistemului informatic

Nivelul surse de date cuprinde depozitele de date comune, așa cum au fost ele definite în cadrul proiectului, ca totalitatea depozitelor de date structurate, semi-structurate și nestructurate - formă consolidată a datelor furnizate de instituțiile cu rol de furnizor în cadrul proiectului "SII INFRASTRUCTURĂ" - fără a se limita la acestea, precum și seturile de date individuale, așa cum au fost ele definite în cadrul proiectului, ca totalitatea seturilor de date semi-structurate și nestructurate, aflate în posesia utilizatorilor finali.

Platforma Big Data, la nivel macro, este constituită din două subsisteme interconectate:

- *subsistemul de management al datelor*, care asigură un lanț de fluxuri și procese de integrare, distribuite de-a lungul a două niveluri arhitecturale: *nivel de integrare* și *nivel de date* propriu platformei Big Data, astfel încât să coreleze volumele mari de date existente în depozitele de date comune și seturile de date individuale sub o formă unică de vizualizare;

- *subsistemul de management al informațiilor*, care asigură un lanț de procese distribuite de-a lungul a două niveluri arhitecturale: *nivel servicii* și *nivel client*, astfel încât, pe baza formei unice de vizualizare, să permită valorificarea operațională și analitică a volumele mari de date existente în depozitele de date comune și seturile de date individuale, prin *instrumente grafice* (aplicații) ce permit interacțiunea cu utilizatorii finali și prin *adaptori* ce permit interacțiunea cu Componenta de Acces, precum și cu alte sisteme informatice.

Modelul Conceptual de Interpretare Semantică a Datelor reprezintă parametrul fundamental al platformei Big Data, funcție de care volumul mare de date existent în depozitele de date comune și seturile de date individuale, este corelat într-o formă unică de vizualizare sub formă de obiecte, proprietăți și relații.

Infrastructura hardware și de comunicații trebuie să permită interoperabilitate cu mediul IT administrat de beneficiar, achiziționat și configurat în cadrul proiectului "SII INFRASTRUCTURĂ". Atât pentru platforma Big Data, cât și pentru componenta de acces securizat în condiții de mobilitate se vor asigura propriile infrastructuri hardware și de comunicații.

Referitor la *backup și restaurare*, sistemul informatic trebuie să asigure mecanisme moderne de efectuare a copiilor de siguranță, cu posibilitatea restaurării rapide a acestora în cazul unei defecțiuni temporare sau permanente.

Platforma Big Data trebuie să permită integrarea cu soluția existentă de *management al identității*, administrată de către beneficiar, achiziționată și configurată în cadrul proiectului "SII INFRASTRUCTURĂ". Componenta de Acces trebuie să asigure propria soluție de management al identității.

Platforma Big Data trebuie să permită integrarea cu soluția de *control acces* existentă, administrată de către beneficiar, achiziționată și configurată în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea autentificării unice și autorizării pe bază de roluri și permisiuni. Totodată, trebuie să permită integrarea cu portalul web existent, administrat de beneficiar, achiziționat și configurat în cadrul proiectului "SII INFRASTRUCTURĂ". Componenta de acces securizat în condiții de mobilitate trebuie să asigure propria soluție de control acces și Single Sign On, atât din perspectiva utilizatorului cât și din perspectiva terminalului mobil folosit.

Sistemul informatic trebuie să asigure mecanisme de *securitate* la nivel hardware și software, care să permită protejarea informației atât față de accesul neautorizat intern cât și

față de accesul neautorizat extern, atunci când informația este stocată pe medii magnetice sau când este transportată în rețea.

Sistemul informatic trebuie să asigure componente specializate pentru *administrarea* și *monitorizarea* centralizată a platformei tehnologice prin intermediul unor interfețe de management, precum și pentru *auditarea* și analiza activității utilizatorilor.

Sistemul informatic trebuie să ofere o arhitectură scalabilă, modulară, flexibilă și deschisă, cu posibilități de extindere a funcționalităților prin intermediul unor librării cu API-uri bine documentate, care să permită configurări și dezvoltări ulterioare, în funcție de necesitățile instituțiilor publice beneficiare.

2.19.3.1 Nivel surse de date

Nivelul surse de date cuprinde depozitele de date comune, așa cum au fost ele definite în cadrul proiectului, ca totalitatea depozitelor de date structurate, semi-structurate și nestructurate - formă consolidată a datelor furnizate de instituțiile cu rol de furnizor în cadrul proiectului "SII INFRASTRUCTURĂ" - fără a se limita la acestea, precum și seturile de date individuale, așa cum au fost ele definite în cadrul proiectului, ca totalitatea seturilor de date semi-structurate și nestructurate, aflate în posesia utilizatorilor finali.

Sistemul informatic trebuie să poată integra, prin intermediul platformei Big Data, depozite de date comune și seturi de date individuale.

2.19.3.1.1 Depozite de date comune

Volumul mare de date aferent depozitelor de date comune îmbracă o varietate de forme descrise în mod succint prin următoarele metrici:

- depozite de date structurate în cel puțin 15 pluggable-uri ORACLE 12c sau baze de date relaționale separate, ce conțin cel puțin 150 scheme de baze de date constituite din cel puțin 28.000 de tabele cu cel puțin 500.000 de coloane și cel puțin 35.000.000.000 de înregistrări;
- depozite de date semi-structurate și nestructurate, salvate în format text sau binar, sub forma unor fișiere pe disk sau sub forma unor obiecte CLOB, respectiv BLOB în SGBD ORACLE.

Un caz particular al datelor salvate în depozitele de date nestructurate îl reprezintă *imaginile de referință* utilizate în cadrul soluției "*face recognition*". Acest set de imagini va fi folosit ca *input* în procesul de antrenare a algoritmilor de recunoaștere facială. În prezent,

există *imagini de referință* alb-negru și color, cu o dimensiune medie de 16KB, ce ocupă cel puțin 950 GB spațiu pe disk în obiecte de tip BLOB distribuite în 6 tabele de-a lungul a 2 scheme din 2 pluggable-uri ORACLE 12c. O persoană poate avea asociate mai multe *imagini de referință*. În aceste imagini, subiectul nu prezintă ocluzii sau variații ale aspectului și expresiei faciale, respectiv ale rotației capului față de poziția frontală. Rezoluția nativă este de minim 200 x 240 pixeli.

În prezent, depozitele de date comune sunt evidențe aferente activităților specifice instituțiilor publice, consolidate într-o bază de date prin instrumente de replicare online, în timp real sau periodic (o dată pe zi / săptămână / lună) în loturi incrementale sau integrale, sau prin instrumente offline.

Numărul și varietatea depozitelor de date comune este prevăzut să crească în continuare, fapt ce va conduce la creșterea valorilor anterioare și diversificarea formatelor conținutului structurat, semi-structurat și nestructurat - inclusiv în ceea ce privește *imaginile de referință* folosite ca *input* în procesul de antrenare a algoritmilor de recunoaștere facială. Drept urmare, furnizorul trebuie să asigure soluții de integrare ("*mapperi*" și *proces de achiziție*¹⁰) a unor depozite de date în format PDF, HTML, HTM, XHTML, PPT, PPTX, DOC, DOCX, RTF, XLS, XLSX, CSV, XML, JSON și TXT ("*plain text*" sau valori separate prin delimitatori).

2.19.3.1.2 Seturi de date individuale

În prezent, beneficiarul nu are capacitatea de a anticipa complet diversitatea formatelor și structura seturilor de date ce pot ajunge în posesia utilizatorilor finali. Drept urmare, furnizorul trebuie să asigure soluții de integrare (*proces de încărcare*¹¹) accesibile direct utilizatorului final ca interfețe în cadrul platformei Big Data, cel puțin pentru formatele PDF, HTML, HTM, XHTML, PPT, PPTX, DOC, DOCX, RTF, XLS, XLSX, CSV, XML, JSON și TXT ("*plain text*" sau valori separate prin delimitatori).

2.19.3.2 Arhitectura funcțională aferentă platformei Big Data

Platforma Big Data trebuie să fie constituită pe baza unei arhitecturi segregate pe verticală și pe orizontală la un nivel optim de granularitate, astfel încât să poată anticipa, prin scalabilitate și flexibilitate, eventuale cerințe ulterioare ale beneficiarilor.

¹⁰ vezi capitolele 3.2.2.2.1.1. Mapperi și 3.2.2.2.1.2.1. Procese de achiziție;

¹¹ vezi capitolul 3.2.2.2.1.2.2. Procese de încărcare;

Arhitectura logic-funcțională aferentă platformei Big Data, este prezentată, într-o manieră detaliată, în figura următoare:

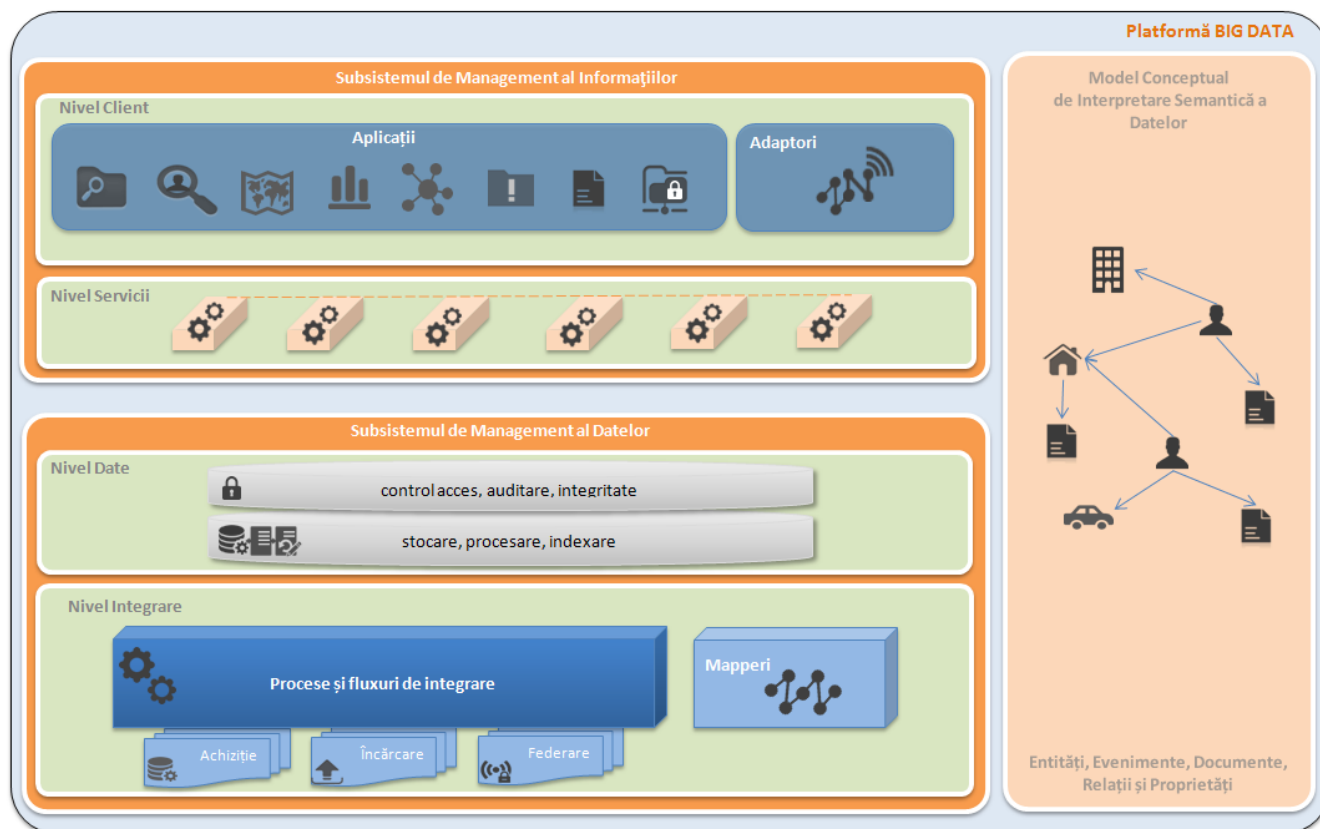


Figura 4: Arhitectura logic-funcțională a platformei Big Data

Raportat la modul de reprezentare a arhitecturii din figura anterioară, admitem faptul că segregarea pe orizontală construiește, în cadrul platformei Big Data, patru niveluri arhitecturale, grupate în două subsisteme interconectate: *subsistemul de management al datelor* și *subsistemul de management al informațiilor*.

Subsistemul de management al datelor grupează următoarele două niveluri arhitecturale:

- *nivelul de integrare* - cuprinde "mapperi", fluxurile și procesele de integrare, ce corelează volumele mari de date existente în depozitele de date comune și seturile de date individuale, sub o formă unică de vizualizare, cu sau fără preluarea acestora în depozitul de date propriu platformei Big Data;
- *nivelul de date* - cuprinde depozitul de date propriu platformei Big Data, definit ca totalitatea formelor fizice și tehnologiilor de stocare, precum și totalitatea tehnologiilor de indexare și procesare.

Subsistemul de management al informațiilor grupează următoarele două niveluri arhitecturale:

- *nivelul servicii* - cuprinde toate serviciile software care, pe baza formei unice de vizualizare a datelor, asigură accesarea depozitului de date propriu platformei Big Data și a depozitelor de date comune prin intermediul unor fluxuri de regăsire federativă;
- *nivelul client* - cuprinde instrumentele grafice ce permit interacțiunea utilizatorilor finali cu platforma Big Data și adaptorii ce permit interacțiunea componentei de acces securizat în condiții de mobilitate, precum și a altor sisteme informatice cu platforma Big Data.

Segregarea pe verticală a nivelului client, construiește funcționalități astfel grupate în blocuri și / sau module funcționale, încât să susțină în mod optim activitatea curentă a instituțiilor publice beneficiare:

- *"Enterprise search"* - trebuie să ofere o gamă diversificată de abordări, precum:
 - *"full text search"* - soluție de căutare unificată, întâlnită preponderent în domeniul motoarelor de căutare, ce permite regăsirea informațiilor utilizând limbajul natural - completată prin mecanisme ce îmbunătățesc modul de definire a criteriilor de regăsire, pentru a reduce rezultatele de tip *"false positive"*, nerelevante în contextul căutării, generate de ambiguitatea limbajului natural;
 - *"query builder"* - soluție de căutare avansată, ce permite definirea grafică, arborescentă a criteriilor de regăsire, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual;
 - *"spatial search"* - soluție de căutare avansată, ce permite regăsirea informațiilor folosind diverse instrumente geometrice precum restrângerea zonei de interes prin definirea grafică a unor forme poligonale pe o hartă;
 - *"face recognition"* - soluție de recunoaștere a persoanei / persoanelor dintr-o imagine digitală;
- *Vizualizarea și rafinarea rezultatului* generat în urma procesului de regăsire:
 - *"guided navigation"* - soluție avansată de rafinare a rezultatelor, întâlnită preponderent în domeniul site-urilor de e-commerce, ce permite explorarea informațiilor clasificate după mai multe dimensiuni, prin aplicarea unor filtre succesive;

- *"drill down"* - soluție ce permite navigarea în adâncime, printr-o parcurgere ierarhică nivel cu nivel a rezultatelor, cu scopul de a obține detalii suplimentare, cu granularitate din ce în ce mai fină;
- *"detail view"* - interfață ce permite vizualizarea tuturor detaliilor asociate fiecărei înregistrări din rezultat, în funcție de tipul de obiect selectat: document, entitate sau eveniment;
- *Analiza avansată a datelor* - trebuie să ofere o gamă diversificată de abordări, precum:
 - *"link analysis"* - soluție de dispunere grafică a obiectelor, proprietăților și relațiilor, sub formă de grafuri compuse din noduri și muchii, astfel încât să permită descoperirea de noi informații și conexiuni ce îmbogățesc valoarea datelor existente;
 - *"spatial analysis"* - soluție de analiză avansată, ce permite dispunerea pe hartă a metadatelor geospațiale aferente obiectelor, proprietăților și relațiilor;
 - *"semantic analytics"* - soluție de analiză avansată ce permite clasificarea multidimensională a datelor și extragerea automată a obiectelor, proprietăților și relațiilor din conținut nestructurat, astfel încât, plecând de la o vedere de ansamblu, printr-o rafinare succesivă a informațiilor folosind forme variate de vizualizare precum histograme de proprietăți și de relații, grupări și agregări, chart-uri, dispunere pe hartă și / sau operații cu mulțimi, să permită micșorarea setului de date supus analizei, până la un nivel de unde se poate începe procesul investigativ;
 - *"behavioral analytics"* - soluție de analiză avansată, ce permite definirea unor comportamente, ca o grupare de filtre complexe construite grafic și / sau programatic, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual sau calculată prin agregări și grupări multiple, pe baza cărora pot fi identificate, vizualizate, analizate și monitorizate obiecte ce se încadrează într-un tipar;
- *"Early warning"* - notificări generate pe baza unui *"watchlist"* compus din entități, sau pe bază de comportamente;
- *"Enrichment"* - soluție de îmbogățire a procesului de analiză, prin achiziția și corelarea, pe baza modelului de date conceptual, a unor seturi de date individuale, precum și prin etichetarea conținutului nestructurat;

- *Spațiu privat și colaborare* - soluție ce permite construirea unui spațiu privat prin gruparea analizei în investigații, salvarea și administrarea rezultatului analizei, a căutărilor și a notificărilor proprii, colaborare, precum și extragerea rezultatului analizei sub formă de rapoarte concise, dar cuprinzătoare.

Blocurile și / sau modulele funcționale, succint prezentate anterior, deși interconectate, trebuie să permită echipei tehnice planificarea secvențială a procesului de dezvoltare și implementare a acestora în cadrul platformei Big Data, în conformitate cu graficul de activități.

2.19.3.2.1 Modelul conceptual de interpretare semantică a datelor

Platforma Big Data trebuie să fie construită plecând de la un model conceptual de interpretare semantică a datelor - *parametru fundamental al sistemului informatic*, funcție de care volumul mare de date existent este corelat într-o formă unică de vizualizare foarte apropiată gândirii umane, care să reprezinte realitatea din punct de vedere semantic cel puțin sub formă de:

- *obiecte* ca, spre exemplu:
 - *entități* - persoană, mașină, telefon, etc;
 - *evenimente* - achiziție, accident, etc.;
 - *documente* - informație cu conținut nestructurat;
- *proprietăți* ca, spre exemplu: culoarea unei mașini, numele unei persoane, data unui eveniment, dimensiunea, formatul sau conținutul unui fișier text, etc.;
- *relațiile* între obiecte ca, spre exemplu: - persoana A este tatăl persoanei B, mașina A a fost implicată în evenimentul B, proprietatea A este menționată în documentul B, etc..

Acest model conceptual de interpretare semantică a datelor sub formă de *obiecte, proprietăți și relații*, trebuie:

- să permită corelarea volumelor mari de date existente în depozitele de date comune și seturile de date individuale, indiferent de forma de reprezentare a acestora: structurate, semi-structurate sau nestructurate;
- să descrie obiectele, proprietățile și relațiile la nivel de instanță, fără necesitatea cunoașterii nivelurilor intermediare de stocare și organizare;
- să permită construirea de "*mapperi*" specializați care să susțină prin fluxuri și procese de integrare, corelarea volumului mare de date existent în depozitele de date comune și seturile de date individuale;

- să susțină nivelul de servicii și nivelul client în procesul de regăsire, analiză și prezentare a datelor;
- să accepte informații multi-valoare și temporale ca, spre exemplu: salariul lunar al unui angajat;
- să permită beneficiarului să realizeze actualizări ulterioare cu minimum de efort prin soluții preponderent grafice care să nu necesite cunoștințe solide de programare.

Modelul conceptual de interpretare semantică a datelor sub formă de *obiecte, proprietăți și relații*, va fi definit de către furnizor în etapa de analiză, de comun acord cu beneficiarul, în funcție de structura și semnificația datelor din depozitelor de date comune și de capacitatea de anticipare a beneficiarului cu privire la posibile structuri și semnificații ale seturile de date ce pot ajunge în posesia utilizatorilor finali. În această etapă, furnizorul trebuie să aibă capacitatea de a analiza depozitele de date comune și de a face propuneri cu privire la definirea modelului conceptual, dar și de a include în această formă unică de vizualizare orice solicitare suplimentară, venită din partea beneficiarului.

În caz de necesitate, în etapa de analiză, furnizorul va solicita detalii suplimentare referitoare la structura și semnificația datelor din depozitelor de date comune, direct de la proprietarii datelor - instituțiile publice furnizoare.

2.19.3.2.2 Subsistemul de management al datelor

Pentru a permite decuplarea completă a modelului de business implementat la nivelul platformei Big Data, de structura fizică și modelul fizic și logic de organizare a volumelor mari de date în depozitele de date comune și seturile de date individuale, soluția tehnică aferentă subsistemului de management al datelor, trebuie să asigure - prin "*mapperii*", fluxuri și procese de integrare - o formă unică de vizualizare a datelor, cu sau fără preluarea acestora în depozitul de date propriu platformei, astfel încât să creeze premisele unei implementări coerente a unui lanț de servicii și instrumente software interconectate, care să susțină utilizatorul final în procesul investigativ.

2.19.3.2.2.1 Nivelul de integrare

Nivelul de integrare cuprinde "*mapperii*", fluxurile și procesele de integrare, ce corelează volumele mari de date existente în depozitele de date comune și seturile de date individuale, sub o formă unică de vizualizare, cu sau fără preluarea acestora în depozitul de date propriu platformei Big Data.

Toți "*mapperii*", procesele și fluxurile de integrare vor fi configurate de către furnizor. Datorită faptului că varietatea depozitelor de date comune este prevăzută să crească pe durata de implementare a proiectului, la solicitarea beneficiarului, furnizorul trebuie să aibă capacitatea de a configura noi "*mapperi*", procese și fluxuri de integrare pentru orice alt format nespecificat în mod explicit în acest document, atât pentru noi depozite de date comune cât și pentru noi seturi de date individuale.

Pentru a evita situațiile în care procesele și fluxurile de integrare limitează, îngreunează sau împiedică interacțiunea utilizatorilor finali, a componentei de acces securizat în condiții de mobilitate sau a altor sisteme informatice cu platforma Big Data, soluția tehnică trebuie să gestioneze diferențiat subsistemul de management al datelor și subsistemul de management al informațiilor.

2.19.3.2.2.1.1 Mapperi

Prin "*mapper*" se înțelege acea unitate funcțională care mapează volumul mare de date din depozitele de date comune și din seturile de date individuale, pe baza modelului conceptual de interpretare semantică a datelor sub formă de *obiecte, proprietăți și relații*. Aceștia au rolul de a:

- ascunde structura fizică și modelul fizic și logic de organizare a datelor în depozitele de date comune și seturile de date individuale, permițând decuplarea completă și implementarea independentă a modelului de business la nivelul platformei Big Data;
- susține fluxurile și procesele de integrare ce corelează volumul mare de date existent sub o formă unică de vizualizare.

Accesul la "*mapperi*" trebuie să poată fi restricționat. La finalul perioadei de implementare a proiectului, beneficiarul trebuie să poată configura noi "*mapperi*" cu minimum de efort, prin soluții preponderent grafice care să nu necesite cunoștințe solide de programare.

2.19.3.2.2.1.2 Procese și fluxuri de integrare

Procesele și fluxurile de integrare trebuie să permită identificarea depozitului de date comun sau a setului de date individual, pentru fiecare informație corelată, astfel încât să asigure definirea unor condiții de acces în funcție de sursa de date integrată. Trebuie să asigure mecanisme de control al calității precum deduplicare sau tokenizare și să nu afecteze performanța sistemelor ce valorifică în prezent depozitele de date comune. Nu trebuie să

implice costuri suplimentare de licențiere pentru instituțiile furnizoare de date și să fie implementate cel puțin sub formă de procese de achiziție și încărcare, respectiv fluxuri de acces federativ, așa cum sunt ele definite în continuare.

2.19.3.2.2.1.2.1 Procese de achiziție

Reprezintă acele procese care, utilizând *"mapperi"* în caz de necesitate, accesează, preiau, transformă, procesează, încarcă și / sau indexează date din depozitele de date comune, în depozitul de date propriu platformei Big Data. Aceste tipuri de procese trebuie să asigure un transfer unidirecțional dinspre depozitele de date comune către depozitul de date propriu platformei Big Data și să asigure o achiziție inițială masivă a tuturor datelor existente, urmată de o achiziție incrementală, astfel încât să susțină funcționalitățile de avertizare și să crească performanța modulelor de regăsire și analiză avansată. Trebuie să utilizeze o versiune anonimată sau criptată a parolei de acces la depozitele de date comune. Totodată trebuie să asigure condiții optime de sincronizare a depozitului de date propriu platformei Big Data cu depozitele de date comune, chiar și în condițiile în care acestea sunt construite prin instrumente de replicare online, în timp real sau periodic (o dată pe zi / săptămână / lună) în loturi incrementale sau integrale, sau prin instrumente offline.

Implementări ale acestui tip de proces pot fi utilizate în vederea corelării datelor din depozitele de date comune sub o formă unică de vizualizare, cu sau fără preluarea acestora în depozitul de date propriu platformei Big Data.

2.19.3.2.2.1.2.2 Procese de încărcare

Reprezintă acele procese care, utilizând *"mapperi"* în caz de necesitate, preiau, transformă, procesează, încarcă și / sau indexează date din seturile de date individuale, în depozitul de date propriu platformei Big Data. *"Mapperii"* aferenți acestor tipuri de procese de achiziție trebuie să poată fi construiți de către utilizator prin intermediul unor interfețe grafice. Seturile de date individuale, astfel încărcate, vor fi accesibile în sistem doar utilizatorilor ce le-au încărcat, oferindu-le acestora posibilitatea de a le partaja în cadrul platformei Big Data.

Implementări ale acestui tip de proces pot fi utilizate în vederea corelării datelor din seturile de date individuale sub o formă unică de vizualizare, cu preluarea acestora în depozitul de date propriu platformei Big Data.

2.19.3.2.2.1.2.3 Fluxuri de acces federativ

Reprezintă acele fluxuri care, utilizând *"mapperi"* în caz de necesitate, permit distribuirea accesului la depozitele de date comune, prin procese de regăsire federativă. Aceste fluxuri, din motive de performanță a platformei Big Data sau pentru a nu afecta performanța sistemelor existente în prezent, pot folosi un *"cache"* local sub formă de depozit propriu platformei Big Data, copie a depozitelor de date comune.

Implementări ale acestui tip de proces vor fi utilizate doar în situația în care furnizorul justifică, argumentează și / sau demonstrează beneficiile aduse de o astfel de abordare în detrimentul proceselor de achiziție și doar la solicitarea sau cu acordul explicit al beneficiarului.

2.19.3.2.2.2 Nivelul de date

Nivelul de date cuprinde depozitul de date propriu platformei Big Data, definit ca totalitatea formelor fizice și tehnologiilor de stocare, precum și totalitatea tehnologiilor de indexare și procesare.

Nu există restricții în ceea ce privește structura fizică și modelul fizic și logic de organizare a datelor în depozitul de date propriu platformei Big Data, atât timp cât acesta este corelat într-o formă unică de vizualizare, descrisă prin intermediul modelului conceptual de interpretare semantică a datelor sub formă de obiecte, proprietăți și relații.

Totuși, acest nivel trebuie să fie dimensionat astfel încât să asigure performanță liniară serviciilor oferite de platforma Big Data, chiar și în condiții de creștere polinomială sau exponențială a volumului de date. În acest sens, platforma Big Data trebuie să utilizeze tehnologii moderne de stocare, indexare și procesare întâlnite în zona Big Data, precum MapReduce și calcul in-memory.

Nivelul de date trebuie să asigure:

- securitatea depozitului de date propriu platformei Big Data, având în vedere cel puțin următoarele aspecte: controlul accesului, auditarea operațiunilor efectuate, respectiv verificarea integrității datelor;
- implementarea unor măsuri logice și fizice ce asigură păstrarea depozitului de date propriu platformei Big Data într-o formă consistentă, chiar și în cazul apariției unui incident logic sau fizic;

- filtrarea volumului de informație existent în depozitul de date propriu platformei Big Data, în funcție de politicile de acces ale utilizatorilor la sursele de date integrate;
- repunerea în funcțiune, după o avarie, a depozitului de date propriu platformei Big Data, păstrând totodată politicile de acces definite în funcție de sursele de date integrate.

2.19.3.2.3 Subsistemul de management al informațiilor

Subsistemul de management al informațiilor asigură un lanț de procese distribuite de-a lungul a două niveluri arhitecturale: *nivel servicii* și *nivel client*, astfel încât, pe baza formei unice de vizualizare a datelor, să permită valorificarea operațională și analitică a volumele mari de date existente în depozitele de date comune și seturile de date individuale, prin *instrumente grafice* (aplicații) ce permit interacțiunea cu utilizatorii finali și prin *adaptorii* ce permit interacțiunea cu componenta de acces securizat în condiții de mobilitate, precum și cu alte sisteme informatice.

2.19.3.2.3.1 Nivelul servicii

Nivelul servicii cuprinde toate serviciile software care, pe baza formei unice de vizualizare a datelor, asigură accesarea depozitului de date propriu platformei Big Data (*în mod direct*) și a depozitelor de date comune (*prin fluxuri de regăsire federativă*).

Acest nivel implementează modelul de business existent la nivelul platformei Big Data și permite decuplarea nivelului client de nivelul de date. Aceste servicii trebuie să ofere performanță liniară la nivelul platformei Big Data, chiar și în condiții de creștere polinomială sau exponențială a volumului de date. În acest sens, trebuie să utilizeze tehnologii moderne de accesare a volumului mare de date, întâlnite în zona BigData, precum MapReduce și calcul in-memory.

Acest nivel trebuie să susțină instrumentele grafice (aplicațiile) și adaptorii ce construiesc nivelul client, oferind cel puțin servicii integrate de regăsire, avertizare, colaborare și monitorizare.

2.19.3.2.3.2 Nivelul client

Nivelul client cuprinde instrumentele grafice (aplicațiile) ce permit interacțiunea utilizatorilor finali cu platforma Big Data și adaptorii ce permit interacțiunea componentei de acces securizat în condiții de mobilitate, precum și a altor sisteme informatice cu platforma Big Data.

Printr-un set de instrumente software avansate de regăsire, vizualizare, analiză, colaborare, avertizare și extragere a rezultatului obținut sub formă de rapoarte concise dar cuprinzătoare, nivelul client trebuie să permită instituțiilor publice beneficiare construirea unor procese ample de explorare, descoperire și investigare a situațiilor generatoare de fenomene de criminalitate organizată și evaziune fiscală la nivel național, precum și a faptelor asociate fenomenului de corupție și de finanțare a terorismului, în vederea diminuării și prevenirii acestora.

2.19.3.2.3.2.1 Interfața cu utilizatorul

Interfața cu utilizatorul reprezintă acea unitate funcțională ce cuprinde instrumente grafice (aplicații) ce permit interacțiunea utilizatorului cu platforma Big Data. Pentru a asigura condiții optime de interoperabilitate, aceste aplicații pot fi grupate în blocuri, module, respectiv componente funcționale organizate în pagini, "*tab-uri*" sau orice alte forme de vizualizare interconectate prin "*link-uri*" și mecanisme de tip "*drag and drop*" sau "*send to*" - fără a se limita la acestea.

Interfața grafică expusă utilizatorului trebuie să fie construită în tehnologie web HTTP[S] și să respecte următoarele standarde:

- *de interacțiune* - să permită interacțiune prin intermediul dispozitivelor periferice ca tastatura (computer keyboard) și tastatura virtuală (virtual keyboard), precum și prin intermediul dispozitivelor periferice de indicare ca: mouse, touchpad și touchscreen; să permită, pentru o experiență de navigare optimă, utilizarea de scurtături (keyboard shortcuts), eventual și prin asociere cu dispozitivele periferice de indicare;
- *de compatibilitate (progressive enhancement & cross browser compatibility)* - să permită redarea corectă și uniformă a interfeței grafice, pe o gamă variată de navigatoare web consacrate - și diverse versiuni ale acestora - ca, spre exemplu: Internet Explorer, Mozilla Firefox, Chrome și Safari;
- *de adaptativitate (responsive user interface & adaptive layout)* - să minimizeze necesitatea utilizării funcțiilor de "*resize*" și "*scroll*" și să creeze o experiență de navigare optimă pe o gamă variată de dispozitive, indiferent de dimensiunea ecranului: de la telefoane până la monitoare; să ofere un feedback oricărei interacțiuni a utilizatorului cu interfața grafică, astfel încât să elimine percepția de *blocare a ecranului*;

- *de tehnologie* - să utilizeze HTML5 ca tehnologie de bază; interfețele de tip *"rich internet application"*¹² sunt acceptate doar cu menținerea preponderent server-side a operațiilor de procesare, mari consumatoare de resurse hardware și/sau software, astfel încât să ofere șanse egale de utilizare tuturor utilizatorilor, indiferent de configurația stației client.

2.19.3.2.3.2.1.1 Enterprise search

"Enterprise search" reprezintă acea componentă a platformei Big Data ce oferă utilizatorului posibilitatea de a interoga întregul volum de date existent - filtrat în funcție de sursele de date accesibile acestuia, printr-o singură operație de regăsire, independentă de structura fizică și modelul fizic și logic de organizare a datelor în depozitul de date propriu platformei Big Data, respectiv în depozitele de date comune și seturile de date individuale. Implementată în mod corespunzător, componenta trebuie să asigure o interfață grafică intuitivă, ce expune mecanisme avansate de definire a criteriilor de regăsire, precum și de vizualizare a rezultatelor în conformitate cu politicile de securitate descrise prin intermediul prezentului caiet de sarcini.

Această componentă trebuie să ofere o gamă diversificată de abordări, astfel încât să poată răspunde celor mai înalte standarde de exigență. Utilizatorul trebuie să se bucure de o experiență variată, construită prin intermediul a cel puțin următoarelor soluții:

- *"full text search"* - soluție de căutare unificată, întâlnită preponderent în domeniul motoarelor de căutare, ce permite regăsirea informațiilor utilizând limbajul natural - completată prin mecanisme ce îmbunătățesc modul de definire a criteriilor de regăsire, pentru a reduce rezultatele de tip *"false positive"*, nerelevante în contextul căutării, generate de ambiguitatea limbajului natural;

- *"spatial search"* - soluție de căutare avansată, ce permite regăsirea informațiilor folosind diverse instrumente geometrice precum restrângerea zonei de interes prin definirea grafică a unor forme poligonale pe o hartă;

- *"query builder"* - soluție de căutare avansată, ce permite definirea grafică, arborescentă a criteriilor de regăsire, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual;

- *"face recognition"* - soluție de recunoaștere a persoanei / persoanelor dintr-o imagine digitală.

¹² HTML / Javascript based – fără să necesite instalări pe stația client;

Indiferent de soluția de căutare utilizată:

- volumul de date supus filtrării trebuie să poată fi restricționat prin selectarea surselor de date¹³ de către utilizator ("*source-restricted search*");

Notă: - orice sursă de date nou adăugată în sistem, trebuie să fie implicit vizibilă utilizatorului, în funcție de drepturile asociate, fără a fi necesare intervenții la nivelul componentei de regăsire;

- rezultatul procesului de regăsire trebuie să poată fi vizualizat în aceeași zonă unică, definită în conformitate cu cerințele descrise în capitolul *Vizualizare și rafinare*.

2.19.3.2.3.2.1.1 Full text search

"*Full text search*" reprezintă o soluție de căutare unificată, întâlnită preponderent în domeniul motoarelor de căutare, ce permite regăsirea informațiilor utilizând limbajul natural, prin scanarea întregului volum de date existent. Pentru a reduce rezultatele de tip "*false positive*", nerelevante în contextul căutării, generate de ambiguitatea limbajului natural, soluția trebuie să fie, în mod obligatoriu, completată prin mecanisme ce îmbunătățesc modul de definire a criteriilor de regăsire, sens în care trebuie să ofere cel puțin următoarele funcționalități:

- introducerea unuia sau mai multor cuvinte cheie într-un câmp unic de căutare;
- regăsirea termenilor introduși prin specificarea numărului maxim de cuvinte intermediare între aceștia, cu sau fără restricționări cu privire la păstrarea ordinii de introducere ("*proximity search*");
- regăsirea exactă a frazei introduse ("*phrase search*"), prin marcarea cuvintelor (utilizarea, spre exemplu, a caracterului "*quote*") ce trebuie să se regăsească obligatoriu, ca formă și ordine, în rezultatele generate;
- independență față de modul de scriere: interpretarea literelor mari și mici ca fiind la fel ("*case insensitive*") și aducerea diacriticelor la forma de bază;
- construirea unor clauze condiționale complexe, prin utilizarea parantezelor și a unor operatori de tip *boolean* precum AND, OR sau NOT ("*boolean queries*"), aplicați între termeni sau grupări de termeni ("*grouping terms*");
- construirea unor clauze condiționale complexe, prin utilizarea unor expresii regulate ("*regular expressions*");

¹³ vor fi vizibile doar acele surse de date accesibile acestuia

- utilizarea unor caractere speciale ("*wildcard search*") ca înlocuitor al unuia (spre exemplu, caracterului "*question mark*") sau mai multor caractere (spre exemplu, caracterului "*asterisk*");

- restricționarea volumului de date supus filtrării, în funcție de sensul pe care cuvintele îl au pentru utilizator; în acest sens, utilizatorul trebuie să aibă posibilitatea selectării obiectelor / proprietăților definite în modelul conceptual ("*field-restricted search*");

Notă: - orice nou obiect / proprietate, rezultat al actualizării modelului conceptual, trebuie să fie implicit vizibil utilizatorului, fără a fi necesare intervenții la nivelul componentei de regăsire;

- specificarea unui interval de valori inclusiv sau exclusiv ("*range search*"), între care să se regăsească valoarea unei proprietăți definite în modelul conceptual: dată calendaristică, proprietate numerică, etc.;

Notă: - spre exemplu, data nașterii unei persoane să se regăsească între două valori specificate;

- configurarea unor mecanisme avansate de asimilare, precum:
 - asimilare fonetică ("*sounds like*") - regăsiri după variante fonetice ale termenilor căutați;
 - asimilare lexicală ("*stemming*") - regăsiri după cuvinte de bază asociate termenilor căutați;
 - asimilare semantică ("*conceptual search*") - regăsiri după sinonime ale termenilor căutați, ținând cont și de polisemia cuvintelor în contextul frazei introduse;

Notă: - platforma Big Data trebuie să permită utilizarea implicită a unei configurații prestabilite de către un administrator. Utilizatorul trebuie să aibă posibilitatea de a actualiza modul de utilizare a mecanismelor de asimilare, inclusiv în ceea ce privește excluderea sau cumularea formelor de asimilare, particularizarea dicționarilor de asimilare, implicit definite, prin îmbogățirea acestora cu variante personale.

- regăsirea cuvintelor introduse folosind variații de scriere ale acestora ("*fuzzy search*");

Notă: - vor fi utilizați algoritmi ce pot cunosc diferența (gradul de similaritate) dintre forma scrisă a două cuvinte ("*edit distance*"), ca, spre exemplu: "*levenshtein distance*"; utilizatorul trebuie să aibă posibilitatea de a specifica gradul de similaritate ca, spre exemplu, valoare cuprinsă între 0 și 1;

- utilizarea unor caractere speciale (ca, spre exemplu, a caracterului "*caret*") pentru a crește relevanța unuia sau mai multor termeni introduși ("*boosting a term*");

- utilizarea unor sugestii de tip "*did you mean*" sau corecții ortografice;

- utilizarea unei funcții de tip "*type-ahead*"; configurarea pragului minim la care să fie afișate sugestii și rezultate, precum și setarea numărului de mostre afișate;

Notă: - după introducerea unui număr minim de caractere (ex. 3-4 caractere), utilizatorul trebuie să primească, pe măsură ce tastează, sugestii de continuare, mostre ale rezultatului, precum și numărul de rezultate grupate în funcție de sursa de date și / sau obiectele / proprietățile definite în modelul conceptual;

- utilizarea în timpul procesului de regăsire a unor cuvinte cheie ("*keywords*") asociate textelor nestructurate automat la indexare, sau manual prin etichetarea conținutului ("*tagging*") de către utilizatori;

- configurarea limbii de execuție a procesului de regăsire, aspect ce prezintă particularități cel puțin în ceea ce privește mecanismele de asimilare, sugestiile de tip "*did you mean*", corecțiile ortografice, "*fuzzy search*" și funcțiile de tip "*type-ahead*";

Notă: - implicit va fi utilizată limba română iar printre opțiunile de selecție disponibile utilizatorului se va regăsi cel puțin limba engleză, fiecare dintre acestea fiind susținută, în mod evident, de existența unor dicționare proprii;

- configurarea modului de funcționare a procesului de regăsire, în situația în care au fost introduși mai mulți termeni:

- oprirea procesului de regăsire, dacă au fost returnate rezultate ce conțin toți termenii introduși;
- continuarea procesului de regăsire, cu toate permutările posibile generate prin eliminarea succesivă a k termeni ($k = 1, p$), până la un pas ce generează rezultate dar nu mai jos de un prag p predefinit;
- continuarea procesului de regăsire până la pragul p , indiferent de faptul că sunt generate rezultate la un pas intermediar;

- configurarea unor criterii de relevanță în funcție de care vor fi ordonate rezultatele; calcularea scorului se va realiza conform unui algoritm care va ține cont de o gamă variată de factori, precum: tipul obiectelor returnate, numărul de termeni regăsiți, frecvența și ordinea apariției, etc.;

- asigurarea persistenței setărilor configurate de către utilizatori, nu doar pe sesiunea curentă ci și între sesiuni;

- lansarea în execuție a procesului de regăsire, atât prin apăsarea unui buton cu o denumire sugestivă cât și prin apăsarea tastei ENTER;

- realizarea unor regăsiri succesive care, prin introducerea unor noi termeni, să filtreze doar setul de rezultate anterior generat.

Pentru *"full text search"*, soluția trebuie să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.1.2 Spatial search

"Spatial search" reprezintă o soluție de căutare avansată, ce permite regăsirea obiectelor care au atașate informații geospațiale, prin utilizarea unor mecanisme de tip *"geocoding"* și *"reverse-geocoding"*.

Poate fi privită ca o extensie a soluției *"full text search"*, completând-o cu mecanisme de restrângere a zonei de interes prin definirea grafică a unor forme poligonale pe o hartă. În acest fel, utilizatorul poate restricționa setul de rezultate, funcție de metadatele geospațiale, la o anumită zonă geografică, folosind diverse instrumente geometrice pentru definirea unor perimetre de proximitate geospațială, fie utilizând un cerc, prin selectarea centrului și a razei pe o hartă, fie utilizând un poligon, prin selectarea unor puncte pe hartă.

În situația în care *"spatial search"* este utilizată ca o formă de căutare independentă de *"full text search"* și nu ca o extensie a acesteia, atunci rezultatul regăsirii va cuprinde obiecte pentru care metadatele geospațiale se încadrează în zona geografică astfel definită (perimetru de proximitate, respectiv mecanisme de *"geocoding"* și *"reverse-geocoding"*), fără a fi aplicată în prealabil nici o altfel de restricție. O astfel de căutare va permite afișarea rezultatelor direct pe hartă.

Pentru *"spatial search"*, soluția trebuie să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.1.3 Query Builder

"Query builder" reprezintă o alternativă pentru *"full text search"*, ce permite definirea grafică, arborescentă a criteriilor de regăsire, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual. Această soluție de căutare avansată trebuie să permită construirea unor clauze condiționale complexe, prin:

- definirea grafică a unor condiții de filtrare de forma *proprietate obiect - operator relațional - valoare*, unde operatorii relaționali sunt dependenți de tipul proprietății (*text, numeric, dată calendaritică, listă de valori, etc.*) și pot fi de forma: *mai mic, mai mic sau egal,*

mai mare, mai mare sau egal, egal - "case sensitive", egal - "case insensitive", conține, între, "is null", etc. și orice negație a acestora;

- definirea grafică a unor condiții de filtrare de forma *proprietate obiect - operator relațional - proprietate obiect*;
- definirea grafică a unor condiții de filtrare de forma *funcție de agregare aplicată unei proprietăți obiect - operator relațional - valoare*, unde funcția de agregare poate fi de forma: *count, min, max, avg, sum, etc.*;
- definirea grafică a unor condiții de filtrare de forma *obiect - relație - obiect*;
- înlănțuirea condițiilor prin intermediul unor operatori de tip *boolean* precum AND, OR sau NOT;
- gruparea condițiilor, utilizând paranteze, sub forma unor clauze imbricate și înlănțuirea grupurilor de condiții prin intermediul operatorilor de tip *boolean*.

Pentru *"query builder"*, soluția trebuie să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.1.4 Vizualizare și rafinare

Zona de *vizualizare și rafinare* trebuie să fie în deplină corelare cu orice soluție de căutare anterioară, astfel încât să permită, indiferent de soluția de căutare aleasă, vizualizarea rezultatelor procesului de regăsire în aceeași zonă unică, definită în conformitate cu cerințele descrise în continuare. În ceea ce privește funcționalitățile interfeței de vizualizare, zona de *vizualizare și rafinare* a rezultatelor trebuie să asigure:

- afișarea rezultatelor sub formă de *"GRID"* și / sau *"LIST"*, în care fiecare înregistrare este reprezentată în mod distinct;
- afișarea paginată a rezultatelor, cu posibilitatea de navigare între pagini și de modificare a numărului de înregistrări pe pagină;
- afișarea valorii numărului total de rezultate generate;
- afișarea evoluției în timp a procesului de regăsire, printr-un feedback procentual sau cantitativ cu privire la volumul de date scanat, respectiv la numărul de înregistrări regăsite;
- afișarea unei estimări aproximative a timpului necesar finalizării procesului de regăsire;
- afișarea graduală a rezultatelor, pe măsură ce acestea au fost regăsite;

- vizibilitatea implicită, textuală și / sau grafică, a unui set de proprietăți sugestive pentru fiecare înregistrare din rezultat;

- afișarea celei mai recente imagini, în situația în care obiectul returnat are asociate imagini (ex: poza entității de tip *persoană*);

- **Caz particular:** - atunci când este utilizată soluția de recunoaștere facială ca formă de regăsire, pentru fiecare identitate returnată va fi afișată o unică înregistrare care, alături de setul de proprietăți sugestive, va cuprinde, în mod obligatoriu, toate pozele proprii ce depășesc "*threshold*"-ul setat de către utilizator, împreună cu scorul de "*matching*".

- afișarea și clasificarea, într-o interfață grafică independentă, a tuturor imaginilor asociate obiectelor returnate, astfel încât să ofere utilizatorului posibilitatea de a explora rezultatele și în funcție de acest tip de informație;

- ordonarea crescătoare și descrescătoare, automată și / sau manuală, simplă și multiplă¹⁴, a rezultatelor în funcție de criterii diverse, printre care trebuie să se regăsească cel puțin:

- sortarea înregistrărilor în funcție de ordinea alfabetică a proprietăților obiectelor returnate;
- sortarea înregistrărilor în funcție de criteriile de relevanță existente (vezi capitolul "*Full text search*");

- **Caz particular:** - atunci când este utilizată soluția de recunoaștere facială ca formă de regăsire, ordinea implicită de afișare a înregistrărilor va fi determinată de sortarea descrescătoare a valorii maxime a scorurilor de "*matching*" aferente pozelor fiecărei identități returnate;

- transmiterea uneia sau mai multor înregistrări către diverse interfețe de analiză avansată precum "*Link analysis*" și "*Spatial analysis*", cu vizualizarea concomitentă a acestora atât în interfețele de analiză cât și în interfața de vizualizare și rafinare;

- exportul rezultatelor în cel puțin două din următoarele formate: PDF, DOC, HTML, XLS și XML;

- adăugarea *entității* într-un "*watchlist*", cu scopul de a notifica utilizatorul în momentul în care se modifică o proprietate / relație sau se produce un eveniment aferent entității, cu posibilitatea de a configura proprietățile / evenimentele / relațiile a căror schimbare produce notificări;

¹⁴ aplicarea cumulativă a unor criterii de ordonare succesive;

- vizualizarea tuturor detaliilor ("*detail view*") asociate fiecărei înregistrări din rezultat, în funcție de tipul de obiect selectat: document, entitate sau eveniment.

Zona de *vizualizare și rafinare* trebuie să asigure și rafinarea rezultatelor într-o manieră unificată, prin intermediul unor mecanisme avansate precum "*guided navigation*" și "*drill down*", astfel încât să permită:

- clasificarea rezultatelor după mai multe dimensiuni și metrici, funcție de care să asigure rafinarea acestora prin aplicarea unor filtre succesive;
- navigarea în adâncime, printr-o parcurgere ierarhică nivel cu nivel a rezultatelor, cu scopul de a obține detalii suplimentare, cu granularitate din ce în ce mai fină.

2.19.3.2.3.2.1.1.4.1 Guided navigation

"*Guided navigation*" reprezintă o metodă de rafinare a rezultatelor, întâlnită preponderent în domeniul site-urilor de e-commerce, care, pentru a reduce rezultatele de tip "*false positive*", nerelevante în contextul căutării, generate de ambiguitatea limbajului natural, permite gruparea acestora ("*clustering*") printr-o clasificare după diverse dimensiuni și metrici, cel puțin în funcție de obiectele, proprietățile și relațiile definite în modelul de date conceptual.

Acestă formă de rafinare a rezultatelor oferă sprijin în cazul căutărilor ce generează mai mult de un singur răspuns, prin posibilitatea aplicării unor filtre succesive ce permit explorarea ghidată a rezultatelor procesului de regăsire. Explorarea ghidată poate fi realizată, spre exemplu, prin utilizarea unei diagrame de frecvență (*histogramă*).

2.19.3.2.3.2.1.1.4.2 Detail view

În funcție de tipul de obiect selectat din zona de vizualizare (document, entitate sau eveniment), soluția trebuie să permită vizualizarea tuturor detaliilor asociate. Deoarece informația aferentă unui document reprezintă preponderent conținut nestructurat, în timp ce informația aferentă unei entități sau eveniment este reprezentată preponderent sub formă de attribute și relații, interfața de vizualizare a detaliilor trebuie tratată independent pentru fiecare din aceste două categorii.

Interfața de vizualizare a detaliilor asociate entităților și evenimentelor trebuie să asigure o vedere de ansamblu a obiectului, sens în care trebuie să asigure:

- vizualizarea tuturor proprietăților, pozelor și relațiilor asociate;
- explorarea în adâncime a relațiilor, prin mecanisme de tip "*drill down*";

- vizualizarea unor metadate precum tipul obiectului, sursa de date și data creării;
- semnalarea faptului că obiectului face parte din *"watchlist"*-ul utilizatorului;
- vizualizarea notificărilor emise de sistem urmare a faptului că obiectul face parte din *"watchlist"*-ul utilizatorului;
- accesarea interfeței ce permite configurarea proprietăților / evenimentelor / relațiilor obiectelor ce fac parte din *"watchlist"*-ul utilizatorului, a căror schimbare declanșează notificări;

Interfața de vizualizare a detaliilor asociate documentelor trebuie să asigure o vedere de ansamblu a obiectului, sens în care trebuie să asigure:

- vizualizarea conținutului documentului / textului nestructurat;
- vizualizarea unor metadate precum sursa de date și data creării;
- etichetarea conținutului documentului, astfel încât să permită structurarea textului nestructurat în conformitate cu cerințele definite în capitolul *Etichetare conținut nestructurat*.

2.19.3.2.3.2.1.2 Analiză avansată

Analiza avansată reprezintă acea componentă a platformei Big Data ce oferă utilizatorului posibilitatea de a analiza întregul volum de date existent - filtrat în funcție de sursele de date accesibile acestuia, utilizând eventual, ca pași intermediari, soluții de regăsire, vizualizare și rafinare. Implementată în mod corespunzător, componenta trebuie să asigure o interfață grafică intuitivă, ce expune mecanisme avansate de transformare a datelor în informații și în cunoștințe, în conformitate cu politicile de securitate descrise prin intermediul prezentului caiet de sarcini.

Această componentă trebuie să ofere o gamă diversificată de abordări, astfel încât să poată răspunde celor mai înalte standarde de exigență. Utilizatorul trebuie să se bucure de o experiență variată, construită prin intermediul a cel puțin următoarelor soluții:

- *"link analysis"* - soluție de dispunere grafică a obiectelor, proprietăților și relațiilor, sub formă de grafuri compuse din noduri și muchii, astfel încât să permită descoperirea de noi informații și conexiuni ce îmbogățesc valoarea datelor existente;
- *"spatial analysis"* - soluție de analiză avansată, ce permite dispunerea pe hartă a metadatelor geospațiale aferente obiectelor, proprietăților și relațiilor;
- *"semantic analytics"* - soluție de analiză avansată ce permite clasificarea multidimensională a datelor și extragerea automată a obiectelor, proprietăților și relațiilor din

conținut nestructurat, astfel încât, plecând de la o vedere de ansamblu, printr-o rafinare succesivă a informațiilor folosind forme variate de vizualizare precum histogramme de proprietăți și de relații, grupări și agregări, chart-uri, dispunere pe hartă și / sau operații cu mulțimi, să permită micșorarea setului de date supus analizei, până la un nivel de unde se poate începe procesul investigativ;

- *"behavioral analytics"* - soluție de analiză avansată, ce permite definirea unor comportamente, ca o grupare de filtre complexe construite grafic și / sau programatic, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual sau calculată prin agregări și grupări multiple, pe baza cărora pot fi identificate, vizualizate, analizate și monitorizate obiecte ce se încadrează într-un tipar.

Soluțiile de analiză avansată trebuie să ofere posibilitatea salvării rezultatelor procesului de analiză sub formă de rapoarte concise dar cuprinzătoare, partajarea rezultatelor, însoțite eventual și de concluzii proprii și interoperabilitate în cadrul platformei Big Data.

2.19.3.2.3.2.1.2.1 Link analysis

"Link analysis" reprezintă o soluție de analiză avansată, ce permite dispunere grafică a obiectelor, proprietăților și relațiilor, sub formă de grafuri compuse din noduri și muchii, astfel încât să permită descoperirea de noi informații și conexiuni ce îmbogățesc valoarea datelor existente. Pentru a asigura explorarea vizuală a legăturilor semantice dintre obiecte, cu scopul de obține răspunsuri la întrebări de tipul *"who is who"*, *"who knows who"*, *"who does what"*, această soluție trebuie să asigure:

- afișarea obiectelor (entități, evenimente și documente), proprietăților și relațiilor, sub o formă vizuală de tip graf;
- funcționalități de tip *"zoom in"* și *"zoom out"*, prin mecanisme de tip *"mouse scroll"*, *"slider"* sau alegerea exactă a valorii de *"zoom"*;
- agățarea nodurilor și re poziționarea acestora în cadrul grafului (*"drag and drop"*);
- contractarea grupurilor de noduri cu aceleași proprietăți, într-un nod unic (*"collapse"*);
- expandarea unui nod contractat;
- fuziunea a două sau mai multor noduri, cu preluarea tuturor proprietăților și relațiilor;
- permită eliminarea din graf a unui nod sau a unui grup de noduri;
- eliminarea unor noduri intermediare, cu păstrarea legăturii dintre nodurile extreme;

- cel puțin următoarele forme de vizualizare a grafului: distanțe egale ("*auto-layout*"), circular, grupat, tabelar, ierarhic, număr de legături / densitatea nodului, timeline;
- afișarea proprietăților unui obiect, sub formă de noduri / etichete în graf;
- etichetarea oricărui nod sau legătură din graf;
- evidențierea nodurilor / legăturilor pentru care valorile proprietăților respectă un filtru introdus de utilizator (prin utilizarea, spre exemplu, a unei palete de culori, dimensiuni și / sau fonturi);
- clasificarea nodurilor și legăturilor sub forma unor histograme de proprietăți și / sau relații;
- filtrarea nodurilor din graf, utilizând histograme de proprietăți și / sau relații;
- adăugarea unor noi obiecte, proprietăți și relații ca noi noduri, respectiv legături în graf;
- vizualizarea temporală a evenimentelor / relațiilor, sub formă de "*timeline*";
- animarea vizualizării de tip "*timeline*", cu funcționalități de stop, start ("*play*"), pauză ("*pause*") și reluare ("*resume*"), ce permite evidențierea evoluției în timp a grafului prin mecanisme de tip "*hide*" - "*show*" și / sau "*fade-in*" - "*fade-out*";
- vizualizări ce permit înțelegerea periodicității și frecvenței apariției evenimentelor / relațiilor;
- păstrarea în graf doar a acelor noduri pentru care există evenimente / relații într-un anumit interval de timp, prin funcționalități de tip restrângere, respectiv glisare pe "*timeline*";
- evidențierea animată a fluxurilor de date sub forma unor grafuri orientate;
- extinderea legăturilor asociate unui nod, pe minim 2 niveluri de adâncime, prin intermediul unei singure operații de regăsire ("*search around*");
- evidențierea drumurilor existente între două noduri selectate de utilizator, relaționate direct sau indirect în graf ("*show path*");
- evidențierea celui mai scurt drum existent între două noduri selectate de utilizator, relaționate direct sau indirect în graf ("*show shortest path*");
- identificarea drumurilor cu o adâncime de maxim 5 muchii, existente între două noduri între care nu există o relaționare în cadrul grafului ("*find path*");
- relaționarea unui nod nou introdus cu graful existent;
- customizarea modului de reprezentare a obiectelor, proprietăților și relațiilor, respectiv etichetelor definite, prin setarea unor pictograme intuitive și prin modificări de culoare, dimensiune și / sau font;

- salvarea grafului în cel puțin două din următoarele formate: JPG, PNG, GIF, PDF, DOC[X], HTML;
- exportul grafului într-un format ce permite importul ulterior;
- construirea unui istoric al actualizărilor, prin mecanisme de versionare ce permit vizualizarea / restaurarea versiunilor grafului, folosind conceptul de *"branching"*;
- vizualizarea tuturor detaliilor (*"detail view"*) asociate unui nod, în funcție de tipul de obiect reprezentat: document, entitate sau eveniment;
- accesarea interfeței de etichetare a conținutului unui document, astfel încât să permită structurarea textului nestructurat în conformitate cu cerințele definite în capitolul *Etichetare conținut nestructurat*; afișarea automată în graf a noilor informații structurate prin mecanismele de etichetare;
- afișarea pe hartă a informațiilor geospațiale asociate obiectelor / relațiilor prezente în graf, eventual prin transmiterea acestora către soluția *"spatial analysis"*;
- transmiterea unui nod selectat către componenta *"enterprise search"* și lansarea automată a procesului de regăsire;
- salvarea și distribuirea rezultatului analizei, însoțit eventual și de concluzii proprii, unui utilizator sau grup de utilizatori, prin utilizarea mecanismelor de salvare / export și / sau prin procese de colaborare;
- adăugarea *entității* într-un *"watchlist"*, cu scopul de a notifica utilizatorul în momentul în care se modifică o proprietate / relație sau se produce un eveniment aferent entității, cu posibilitatea de a configura proprietățile / evenimentele / relațiile a căror schimbare produce notificări;
- accesul la funcționalitățile solicitate, prin intermediul unui meniu contextual.

Pentru *"link analysis"*, soluția trebuie să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.2.2 Spatial analysis

"Spatial analysis" reprezintă o soluție de analiză avansată, ce permite dispunerea pe hartă a metadatelor geospațiale aferente obiectelor, proprietăților și relațiilor, astfel încât să permită descoperirea de noi informații și conexiuni ce îmbogățesc valoarea datelor existente. Această soluție trebuie să asigure:

- afișarea obiectelor, proprietăților și relațiilor, prin localizarea acestora pe hartă;
- hărți de fundal ca, spre exemplu: "*street map*" și "*satellite*";
- harta României cu cel puțin următoarele straturi ("*layer*"):
 - toate județele reprezentate ca poligon, cu indicarea denumirii județului și a codului corespondent, la precizia scării 1:10.000;
 - toate Unitățile Administrativ Teritoriale reprezentate ca poligon, cu indicarea denumirii și a codului SIRUTA, la precizia scării 1:10.000;
 - toate localitățile, ca poligon sau multipart poligon, reprezentând perimetrul construit al localității, cu indicarea denumirii localității și a codului SIRUTA, la precizia scării 1:10.000;
 - drumurile naționale și județene la precizia scării 1:10.000, precum și alte categorii de drumuri, la precizia scării 1:25.000 (ex: drumuri comunale, drumuri de exploatare), reprezentate ca polilinie având următoarele atribute: clasificarea (ex: DN, DJ, DC) și codul (ex: 1A) drumului;
 - arterele, reprezentate ca polilinie, din principalele orașe și localități, având ca atribute județul, localitatea, tipul arterei (ex: strada, bulevard, alee), denumirea arterei, la precizia scării 1:10.000;
 - căile ferate reprezentate ca poliline, la precizia scării 1:10.000, inclusiv zona de depou sau căi ferate industriale;
 - gările reprezentate ca punct, la precizia scării 1:10.000;
 - râurile permanente, la precizia scării 1:10.000, reprezentate ca polilinie cu indicarea denumirii;
 - râurile principale reprezentate ca poligon, la precizia scării 1:10.000;
 - lacurile reprezentate ca poligon și denumirea acestora, la precizia scării 1:10.000;
 - curbele de nivel reprezentate ca polilinie cu indicarea altitudinii la precizia scării 1:50.000;
 - vârfurile importante din Romania reprezentate ca punct, la precizia scării 1:25.000;
 - punctele de interes precum monumente istorice, obiectivele socio-culturale, asistență medicală, primării, resurse hoteliere, benzinării, biserici, centre comerciale, grădinițe, școli, licee, universități, bănci, cimitire, fabrici, secții de

- poliție și jandarmerie, tribunale și judecătoria, oficii poștale, piețe, secții de pompieri, administrații publice, reprezentate ca punct, la precizia scării 1:10.000;
- puncte de frontieră, aeroporturi, porturi maritime / fluviale naționale;
- clădirile, reprezentate ca poligon, cu indicarea adresei (denumirii străzii, numărului administrativ, scară, cod poștal) și tipului clădirii, la precizia scării 1:5.000;
- adresele, reprezentate ca punct, cu indicarea denumirii străzii și numărului administrativ, cod poștal, la precizia scării 1:5.000;
- rețelele de transport în comun, cu indicarea traseului la precizia scării 1:5.000;
- arterele, reprezentate ca polilinie, cu indicarea denumirii străzii și a restricțiilor de circulație (sens unic, interzis la stânga, interzis la dreapta), la precizia scării 1:5.000;
- harta globală cu cel puțin următoarele straturi:
 - granițele tuturor statelor, reprezentate ca poligon, cu indicarea denumirii acestora, la precizia scării 1:100.000;
 - orașele, reprezentate ca punct, cu indicarea denumirii acestora, la precizia scării 1:100.000;
 - localitățile, reprezentate ca punct, cu indicarea denumirii acestora, la precizia scării 1:100.000;
 - împărțirea pe regiuni administrative specifice fiecărei țări, reprezentate ca poligon, la precizia scării 1:100.000;
- furnizarea tuturor denumirilor utilizând diacritice;
- furnizarea straturilor atât în format vectorial, cât și în format raster sub forma de cache;
- importul și utilizarea unor noi straturi;
- importul unor fișiere ale căror formate pot reprezenta date geospațiale, ca spre exemplu: *KML, KMZ, GPX, SHP*;
- funcționalități avansate de navigare pe hartă: *"zoom in"*, *"zoom out"*, *"mouse scroll zoom"*, *"slider zoom"*, *"zoom to area"*, *"double-click zoom"*, *"keyboard navigation"*, *"drag"*, *"rotate"* și busolă;
- funcționalități de tip *"geocoding"* și *"reverse-geocoding"* (translatarea bidirecțională între o adresă / locație și coordonate geospațiale);

- mecanisme de tip *"heatmap"* și / sau *"clustering nearby markers"*, actualizate în același timp cu modificarea scării de reprezentare a hărții;
- vizualizarea, direct pe hartă, a unor informații statistice referitoare la datele clusterizate, sub formă scalară sau grafic sub formă de *"chart"*;
- prezentarea pe aceeași hartă a două sau mai multe seturi de date diferite, prin evidențierea separată a acestora folosind elemente grafice și / sau culori diferite (*"bivariate map"*);
- vizualizarea temporală a evenimentelor / relațiilor, sub formă de *"timeline"*;
- păstrarea pe hartă doar a acelor obiecte pentru care există evenimente într-un anumit interval de timp, prin funcționalități de tip restrângere, respectiv glisare pe *"timeline"*;
- animarea vizualizării de tip *"timeline"*, cu funcționalități de stop, start (*"play"*), pauză (*"pause"*) și reluare (*"resume"*), ce permite evidențierea evoluției în timp a evenimentelor prin mecanisme de tip *"hide"* - *"show"* și / sau *"fade-in"* - *"fade-out"*;
- vizualizări ce permit înțelegerea periodicității și frecvenței apariției evenimentelor;
- localizarea pe hartă a tuturor datelor geospațiale specifice unui obiect (ex.: - domiciliul, reședința);
- vizualizarea obiectelor ce au legătură cu locația sau perimetrul selectat de către utilizator (ex.: - firme care au sediul social / persoane care locuiesc la o anumită adresă);
- calcularea distanței dintre mai multe puncte definite de utilizator;
- vizualizarea sub formă de histogramă a tuturor elementelor reprezentate pe hartă (sau a unui subset selectat de utilizator) și a proprietăților comune ale acestora;
- filtrarea datelor reprezentate pe hartă, prin selectarea unui perimetru definit sub formă de cerc - cu centrul și raza setată de utilizator, sau sub formă de poligon format din mai multe puncte;
- selectarea / eliminarea de pe hartă a unuia sau mai multor obiecte;
- crearea / ștergerea de adnotări (săgeți, text, puncte de interes), ce pot fi atașate unui *"layer"*;
- customizarea detaliilor aferente elementelor grafice specifice fiecărui *"layer"*, prin setarea unor pictograme intuitive și prin modificări de culoare, dimensiune și / sau font;
- selectarea / deselectarea *"layer"-elor*;

- customizarea modului de reprezentare a obiectelor, proprietăților și relațiilor, respectiv etichetelor definite, prin setarea unor pictograme intuitive și prin modificări de culoare, dimensiune și / sau font;
- salvarea hărții împreună cu toate elementele grafice reprezentate pe aceasta, în cel puțin două din următoarele formate: JPG, PNG, GIF, PDF, DOC[X], HTML;
- exportul tuturor elementelor reprezentate pe hartă, într-un format ce permite importul ulterior;
- vizualizarea tuturor detaliilor ("*detail view*") asociate unui obiect reprezentat pe hartă;
- transmiterea unor obiecte reprezentată pe hartă, către soluția "*link analysis*";
- salvarea și distribuirea rezultatului analizei, însoțit eventual și de concluzii proprii, unui utilizator sau grup de utilizatori, prin utilizarea mecanismelor de salvare / export și / sau prin procese de colaborare;
- adăugarea într-un "*watchlist*", a unei *entități* reprezentată pe hartă, cu scopul de a notifica utilizatorul în momentul în care se modifică o proprietate / relație sau se produce un eveniment aferent entității, cu posibilitatea de a configura proprietățile / evenimentele / relațiile a căror schimbare produce notificări;
- accesul la funcționalitățile solicitate, prin intermediul unui meniu contextual.

Pentru "*spatial analysis*", soluția trebuie să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.2.3 Semantic analytics

"*Semantic analytics*" reprezintă o analiză avansată, ce permite clasificarea multidimensională a datelor și extragerea automată a obiectelor, proprietăților și relațiilor din conținut nestructurat, astfel încât, plecând de la o vedere de ansamblu, printr-o rafinare succesivă a informațiilor folosind forme variate de vizualizare precum histograme de proprietăți și de relații, grupări și agregări, chart-uri, dispunere pe hartă și / sau operații cu mulțimi, să permită micșorarea setului de date supus analizei, până la un nivel de unde se poate începe procesul investigativ.

Această formă de analiză, utilă atunci când informațiile disponibile la începutul procesului investigativ nu sunt suficient de precise, punctul de plecare fiind necunoscut sau difuz, raportat la limba română, trebuie să asigure:

- analiza multidimensională a conținutului nestructurat, precum și a obiectelor, proprietăților și relațiilor;
- normalizarea conținutului nestructurat;
- extragerea automată a obiectelor, proprietăților și relațiilor din conținut nestructurat;
- explorarea *"top down"* a datelor, folosind diverse forme de vizualizare / perspective interdependente;
- filtrarea datelor prezentate într-o formă de vizualizare să se propage în mod automat și la nivelul celorlalte forme de vizualizare (*"refresh"*);
- afișarea datelor în diagrame de relație, folosind, spre exemplu, soluția *"link analysis"*;
- dispunerea pe hartă a datelor geospațiale, folosind, spre exemplu, soluția *"spatial analysis"*;
- funcții de vizualizare și raportare similare celor din domeniul aplicațiilor de tip *"business intelligence"*;
- gruparea documentelor în funcție de topic, prin folosirea unor algoritmi avansați de clasificare bazați, spre exemplu, pe dicționare de topic și frecvență de cuvinte;
- sumarizarea conținutului nestructurat;
- clasificarea datelor prin histograme de proprietăți și de relații;
- afișarea și clasificarea informațiilor multimedia, astfel încât să ofere utilizatorului posibilitatea de a explora volumul de date și din această perspectivă.

Pentru *"semantic analytics"*, soluția trebuie să asigure o medie a timpului de răspuns de sub 30 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.2.4 Behavioral analytics

"Behavioral analytics" reprezintă o analiză avansată, ce permite definirea unor comportamente, ca o grupare de filtre complexe construite grafic și / sau programatic, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual sau calculată prin agregări și grupări multiple, pe baza cărora pot fi identificate, vizualizate, analizate și monitorizate obiecte ce se încadrează într-un tipar. Această soluție trebuie să asigure:

- răspunsuri la întrebări de tipul:

- A. care sunt societățile comerciale ai căror acționari sau administratori figurează la mai mult de N societăți comerciale și au cazier judiciar?
 - B. care sunt societățile comerciale înființate între anii AAAA-AAAA, cu numărul mediu de angajați în perioada BBBB-BBBB mai mic decât N și cu rambursări de TVA mai mari de S lei?
 - C. care sunt societățile comerciale cu cifra medie / angajat mai mare decât media + $P\%$ din abaterea medie standard a codului CAEN X ?
 - D. care sunt persoanele fizice al căror venit personal declarat pe perioada AAAA - AAAA și creditele bancare contractate pe perioada BBBB - BBBB este cu $P\%$ mai mic decât numărul de metri pătrați de teren / clădiri * V și auto de valoare minim S lei, dobândite în perioada CCCC - CCCC;
- definirea grafică, arborescentă a întrebărilor sub formă unor condiții de filtrare, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual;
 - definirea programatică a întrebărilor sub formă de *propoziții parametrizate*, în situațiile în care acestea au nivel ridicat de complexitate și nu pot fi definite grafic de utilizator;
 - accesul utilizatorilor la propozițiile parametrizate, în conformitate cu politicile de acces;
 - personalizarea *propozițiilor parametrizate*, prin asocierea de valori pentru fiecare parametru;
 - execuția întrebărilor (*propoziție parametrizată personalizată sau condiție de filtrare grafică*);
 - vizualizarea rezultatului execuției întrebărilor, în conformitate cu cerințele definite în capitolul *Vizualizare și rafinare*, sub formă de listă de entități care respectă condițiile de filtrare;
 - gruparea întrebărilor care oferă ca rezultat același tip de entitate, în *comportamente* ca, spre exemplu:
 1. *comportament 1*: grupează întrebările A, B, C;
 2. *comportament 2*: cuprinde întrebarea D;
 - asocierea unui scor pentru fiecare întrebare din comportament:
 - A. întrebarea A din comportamentul 1 – scor = 3;
 - B. întrebarea B din comportamentul 1 – scor = 2;
 - C. întrebarea C din comportamentul 1 – scor = 5;
 - asocierea unui prag pentru un comportament:

A. *comportament 1* – prag = 5;

- execuția comportamentelor: dacă o entitate face parte din rezultatul unei întrebări atunci va avea asociată o valoare egală cu scorul întrebării, altfel va avea asociată valoarea 0;
- vizualizarea rezultatului execuției comportamentului, în conformitate cu cerințele definite în capitolul *Vizualizare și rafinare*, sub formă de listă de entități pentru care suma valorilor asociate în procesul de execuție (funcție de scorul fiecărei întrebări) depășește pragul definit la nivelul comportamentului;
- salvarea oricărui comportament, cu posibilitatea asocierii unei descrieri;
- programarea unui plan de execuție pentru comportamentele salvate:
 - A. execuție incrementală (la intrarea datelor în sistem), cu scopul de a crește performanța acestui proces de analiză și de a notifica utilizatorul în momentul în care o entitate recent intrată în sistem respectă comportamentul definit;
 - B. execuție temporizată, cu scopul de a determina tendința entităților ce respectă comportamentul și de a transmite notificări atunci când entități existente în sistem intră sub incidența comportamentului;
- vizualizarea tuturor entităților care au corespuns comportamentului de la prima execuție a acestuia, în conformitate cu cerințele definite în capitolul *Vizualizare și rafinare*, cu afișarea grafică a istoricului de scor (inclusiv sub formă de "*chart*") și evidențierea obiectelor aflate pe un trend ascendent;
- execuția unui comportament salvat pentru o entitate selectată de utilizator;
- administrarea comportamentelor salvate.

Pentru "*behavioral analytics*", soluția trebuie să asigure o medie a timpului de răspuns de sub 60 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute.

2.19.3.2.3.2.1.3 Early warning

"*Early warning*" este un instrument ce poate facilita trecerea de la o atitudine reactivă la o atitudine proactivă. Acesta grupează sub aceeași formă de exprimare, notificările pe care platforma Big Data le transmite în mod automat, în situația în care sunt îndeplinite regulile de avertizare definite:

- pe baza unui *"watchlist"* compus din entități adăugate prin mecanisme de tip *"add to watchlist"*, existente la nivelul interfețelor de regăsire, vizualizare și analiză;
- pe baza comportamentelor definite prin intermediul soluției *"Behavioral analytics"*.

Avertizarea pe bază de *"watchlist"*, notifică utilizatorul în momentul în care se modifică o proprietate / relație sau se produce un eveniment aferent oricărei entități existente în *"watchlist"*, respectiv este recunoscută persoana din *imaginile probă* existente în *"watchlist"*.

Notă: - soluția trebuie să permită utilizatorului selectarea proprietăților / evenimentelor / relațiilor a căror schimbare produce notificări; soluția trebuie să permită configurarea aceleiași notificări pentru mai multe entități existente într-un set de date specificat;

Avertizarea pe bază de comportament, notifică utilizatorul în momentul în care o entitate recent intrată în sistem respectă comportamentul sau atunci când entități existente în sistem intră sub incidența comportamentului. Acest tip de notificare, permite alocarea unui anumit procentaj virtual fiecărui criteriu definit în parte, astfel încât, în momentul generării notificării, evidențierea posibilului grad de implicare a entităților în activitățile definite să fie realizată prin afișarea probabilității în procente.

Platforma Big Data trebuie să ofere cel puțin următoarele opțiuni de transmitere a notificărilor:

- sub formă de mesaje la nivelul interfeței grafice, cu evidențiere vizuală și / sau sonoră;
- sub formă de mesaje vizibile direct la nivelul Portalului existent, în cadrul unor componente specializate ("portleți");
- sub formă de e-mail, fără ca mesajul să conțină informații sensibile.

Notificările generate de sistem trebuie să poată fi administrate prin intermediul unei interfețe grafice ce permite stabilirea frecvenței, modificarea parametrilor și anularea acestora.

2.19.3.2.3.2.1.4 Enrichment

"Enrichment" este un termen ce grupează sub aceeași formă de exprimare toate instrumentele ce permit îmbogățirea procesului de analiză, prin achiziția și corelarea, pe baza modelului conceptual de interpretare semantică a datelor sub formă de *obiecte, proprietăți și relații*, a unor seturi de date individuale precum și prin etichetarea conținutului nestructurat.

2.19.3.2.3.2.1.4.1 Adăugare sursă de date individuală

Reprezintă o formă de completare a datelor existente, ce permite utilizatorilor încărcarea grafică a unor seturi de date individuale, în depozitul de date propriu platformei Big Data, fie prin indexarea conținutului nestructurat, fie prin structurarea conținutului semi-structurat pe baza modelului conceptual de interpretare semantică a datelor sub formă de *obiecte, proprietăți și relații*.

Aceste funcționalități vor fi susținute prin intermediul *proceselor de încărcare*, așa cum au fost ele descrise în cadrul documentului, în capitolul *Procese de încărcare*. În cazul datelor semi-structurate, "*mapperii*" ce susțin aceste procese de încărcare trebuie să poată fi construiți direct de către utilizator prin intermediul unor interfețe grafice. Seturile de date individuale, astfel încărcate, vor fi accesibile în sistem doar utilizatorilor ce le-au încărcat, oferindu-le acestora posibilitatea de a le partaja în cadrul platformei Big Data.

Această formă de completare a datelor existente trebuie să asigure:

- încărcarea, extragerea și indexarea conținutului unor fișiere nestructurate, în format PDF, HTML, HTM, XHTML, PPT, PPTX, DOC, DOCX, RTF și TXT;
- încărcarea unor fișiere semi-structurate, în format XLS, XLSX, CSV, XML, JSON și TXT (valori separate prin delimitatori) și structurarea conținutului acestora pe baza modelului conceptual de interpretare semantică a datelor sub formă de *obiecte, proprietăți și relații*, prin intermediul unor interfețe grafice ce permit:
 - identificarea și prezentarea elementelor existente în fișier;
 - maparea asistată ("*wizard*") a elementelor extrase, cu obiectele, proprietățile și relațiile definite în modelul de date conceptual;
 - rularea procesului de încărcare.

2.19.3.2.3.2.1.4.2 Etichetare conținut nestructurat

Reprezintă o formă de îmbogățire a valorii datelor existente, ce permite structurarea conținutului nestructurat indexat în sistem, prin adăugarea unor marcaje de tip legătură, unor părți din document, cu scopul de a crea noi obiecte, proprietăți și / sau relații, respectiv de a actualiza proprietățile / relațiile obiectelor existente.

Obiectele, proprietățile și relațiile astfel extrase pot fi corelate cu datele ce provin din surse structurate și vizualizate / analizate prin intermediul facilităților de analiză descrise la nivelul soluției "*link analysis*". De asemenea, acestea trebuie să fie accesibile doar

utilizatorului ce a realizat etichetarea, oferindu-i și posibilitatea de a le partaja în cadrul platformei Big Data. Pentru toate informațiile extrase, utilizatorul trebuie să poată identifica documentul sursă, aspect ce poate crește gradul de veridicitate prin posibilitatea verificării provenienței datelor.

Această formă de îmbogățire a valorii datelor existente trebuie să asigure:

- instrumente grafice de etichetare precum selecție, meniu contextual și *"drag and drop"*;
- căutarea unui termen în textul documentului și apoi etichetarea aparițiilor;
- anularea unei etichetări anterior realizate;
- selectarea unei porțiuni de text și adăugarea acestuia ca proprietate a unui obiect;
- relaționarea grafică a obiectelor, funcție de conținutul etichetat;
- extragerea și relaționarea automată a obiectelor și proprietăților;
- sugestii de etichetare, funcție de acțiunile anterioare ale utilizatorului.

2.19.3.2.3.2.1.5 Spațiu privat și colaborare

Reprezintă o soluție care oferă utilizatorului facilități de organizare a activității într-un spațiu privat, precum și de partajare a rezultatelor obținute.

În ceea ce privește funcționalitățile aferente spațiului privat, soluția trebuie să asigure:

- gruparea proceselor de analiză în investigații;
- afișarea tuturor datelor aferente unei investigații;
- căutare rapidă a informațiilor existente într-o investigație;
- revizuirea și înțelegerea rapidă și sintetică a unui investigații sau analize în lucru;
- acces rapid tip *"drill down"* la orice informații suplimentare necesare;
- administrarea investigației;
- configurarea modului în care sunt afișate elementele în spațiul privat;
- administrarea surselor de date individuale;
- salvarea și administrarea rezultatului analizei;
- administrarea căutărilor, comportamentelor, *"watchlist"*-ului și a notificărilor proprii utilizatorului;
- extragerea rezultatului analizei sub formă de rapoarte concise, dar cuprinzătoare, pe baza unor template-uri specifice;

- păstrarea unui jurnal pentru monitorizarea fiecărei schimbări în cadrul investigației și documentarea informațiilor referitoare la utilizatorul care a realizat modificarea, data și momentul modificării, valorile vechi și valorile noi;
- păstrarea unui istoric al activității utilizatorului, prin mecanisme de versionare ce permit vizualizarea / restaurarea versiunilor, folosind conceptul de *"branching"*.

Pentru a sprijini lucrul în echipă, soluția trebuie să permită salvarea și distribuirea rezultatului analizei, comportamentelor, *"watchlist"*-ului și / sau a notificărilor, însoțite eventual și de observații / concluzii proprii, unui utilizator sau grup de utilizatori, prin utilizarea mecanismelor de salvare / export și / sau prin procese de colaborare. Suplimentar, platforma Big Data trebuie să ofere și soluții de tip *"instant messaging"*.

2.19.3.2.3.2.2 Interfața cu componenta de acces securizat în condiții de mobilitate, precum și cu alte sisteme informatice

Platforma Big Data trebuie să ofere adaptori standard de comunicare cu componenta de acces securizat în condiții de mobilitate, precum și cu alte sisteme informatice, prin schimb de mesaje în format XML și / sau JSON - fără a se limita la acestea. Adaptorii au rolul de a expune cel puțin serviciile de regăsire și avertizare, implementate la nivelul platformei.

Pentru a permite integrarea produselor / serviciilor informatice care vor fi implementate prin proiectul depus, cu alte sisteme informatice, platforma trebuie să fie capabilă să exporte date în formate standard de interoperabilitate (ex. XML, CSV, JSON - fără a se limita la acestea).

În ceea ce privește Componenta de Acces, platforma Big Data trebuie să susțină prin intermediul acestor adaptori, toate funcționalitățile implementate în aplicațiile accesate de pe dispozitive mobile.

2.20 Servicii de implementare modul Face Recognition - platforma Big Data - (1 serviciu)

"Face recognition" reprezintă o alternativă pentru *"full text search"*, ce permite recunoașterea persoanei / persoanelor dintr-o imagine digitală. Această soluție de căutare avansată trebuie privită ca o parte integrantă a platformei Big Data, ce are ca scop detecția și recunoașterea uneia sau mai multor persoane dintr-o fotografie încărcată de utilizator, numită *image probă*, prin compararea feței / fețelor detectate cu înregistrările existente în sistem,

numite *imagini de referință*, și returnarea informațiilor specifice persoanei / persoanelor recunoscute.

2.20.1 Imagini de referință

Imaginile de referință utilizate în cadrul soluției "*face recognition*" reprezintă un caz particular al datelor salvate în depozitele de date nestructurate. Acest set de imagini va fi folosit ca *input* în procesul de antrenare a algoritmilor de recunoaștere facială. În prezent, există *imagini de referință* alb-negru și color, cu o dimensiune medie de 16KB, ce ocupă cel puțin 950 GB spațiu pe disk în obiecte de tip BLOB distribuite în 6 tabele de-a lungul a 2 scheme din 2 pluggable-uri ORACLE 12c. O persoană poate avea asociate mai multe *imagini de referință*. În aceste imagini, subiectul nu prezintă ocluzii sau variații ale aspectului și expresiei faciale, respectiv ale rotației capului față de poziția frontală. Rezoluția nativă este de minim 200 x 240 pixeli.

Numărul și varietatea depozitelor de date comune este prevăzut să crească în continuare, fapt ce va conduce la creșterea valorilor anterioare și diversificarea formatelor conținutului structurat, semi-structurat și nestructurat - inclusiv în ceea ce privește *imaginile de referință* folosite ca *input* în procesul de antrenare a algoritmilor de recunoaștere facială.

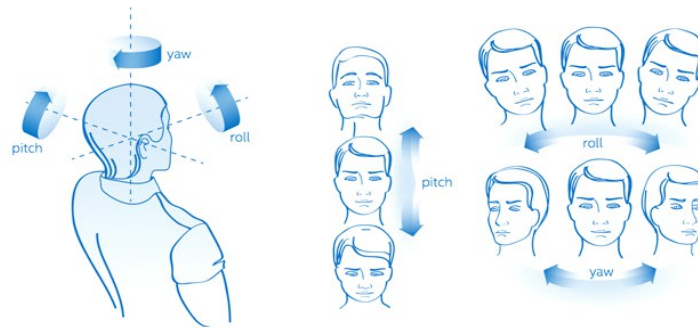
2.20.2 Proces de achiziție

O implementare particulară a procesului de achiziție poate fi utilizată în vederea susținerii soluției "*face recognition*", prin accesarea, procesarea, încărcarea și / sau indexarea *imaginilor de referință* folosite ca *input* pentru procesul de antrenare a algoritmilor de recunoaștere facială. O astfel de implementare trebuie să asigure:

- achiziția *imaginilor de referință*, așa cum au fost ele dimensionate și descrise în secțiunea *Depozite de date comune*;
- o achiziție inițială masivă a tuturor *imaginilor de referință* existente;
- o achiziție incrementală temporizată sau la cerere, a noilor *imagini de referință* consolidate în depozitele de date comune;
- achiziția *imaginilor de referință*, indiferent de sexul și etnia persoanei;
- asocierea fiecărei *imagini de referință* cu persoana aferentă, astfel încât să permită includerea în rezultatul procesului de regăsire a oricăror metadate, definite în modelul conceptual, specifice persoanei / persoanelor recunoscute.

2.20.3 Imagini de probă

Imaginile probă reprezintă acele imagini încărcate de utilizator în momentul utilizării soluției de recunoaștere facială. În figura următoare sunt evidențiate cele trei axe de rotație a capului, informație utilă în contextul în care soluția "*face recognition*" trebuie să accepte *imagini probă* ce prezintă variații ale poziției capului, în raport cu aceste axe.



©IBM **Figura 5. Cele trei axe de rotație a capului**

"yaw" = girație (rotație în jurul axei longitudinale)

"pitch" = tangaj (rotație în jurul axei transversale)

"roll" = ruluu (rotație în jurul axei sagitale)

Din punct de vedere tehnic, soluția "*face recognition*" trebuie să accepte *imagini probă* color sau alb-negru, cu rezoluție nativă de minim 200 x 240 pixeli, codate în cel puțin următoarele formate: JPEG, JPG, PNG, BMP și GIF. Rezultatul efectuării unei regăsiri de tip "*face recognition*", nu trebuie să fie influențat major în situațiile în care *imaginile probă* prezintă următoarele particularități:

- variații de până la ± 45 grade ale girației capului subiectului ("yaw"), față de poziția frontală;
- variații de până la ± 15 grade ale înclinării pe verticală a capului subiectului ("pitch"), față de poziția frontală;
- variații de până la ± 15 grade ale înclinării stânga - dreapta a capului subiectului ("roll"), față de poziția frontală;
- variații ale distanței dintre ochii subiectului, cu acceptarea oricăror valori până la un prag minim de 30 pixeli nativi (ce nu sunt obținuți prin redimensionarea imaginii);
- schimbări minore ale aspectului subiectului, față de *imaginile de referință*, cel puțin în ceea ce privește părul facial, mustața, barba, ochelarii de vedere și ochelarii de soare;

- schimbări minore a expresiei faciale a subiectului, față de *imaginile de referință*;
- ocluzii, datorate schimbării direcției și / sau unghiului sursei de lumină.

2.20.4 Vizualizare și rafinare

Modul de vizualizare și rafinare a rezultatelor returnate în urma unui proces de căutare utilizând soluția "*face recognition*" se va conforma cerințelor formulate în secțiunea 2.19.3.2.3.2.1.1.4 - Vizualizare și rafinare.

2.20.5 Cerințe funcționale

Procesul de recunoaștere facială este un proces în mai multe etape: încărcarea imaginii, detecția feței / fețelor, recunoașterea persoanei / persoanelor și generarea rezultatului. În acest sens, soluția de recunoaștere facială trebuie să asigure:

- încărcarea unor *imagini probă*, așa cum au fost ele definite anterior - în capitolul *Imagini probă*;
- detecția feței / fețelor din *imaginile probă*, indiferent de gama cromatică (ex.: alb-negru, color, filtre de culoare, filtre de lumină) și de sexul persoanei;
- recunoașterea persoanei / persoanelor în funcție de modelul antrenat pe baza *imaginilor de referință*, așa cum au fost ele definite anterior - în capitolul *Depozite de date comune*;
- afișarea rezultatului în aceeași zonă unică utilizată de orice formă de regăsire, definită în conformitate cu cerințele descrise în capitolul *Vizualizare și rafinare*;

În ceea ce privește cerințele funcționale, soluția de recunoaștere facială trebuie să asigure posibilitatea utilizatorului:

- să încarce una sau mai multe *imagini probă* salvate pe mediul de stocare aferent dispozitivului utilizat, cu scopul de a recunoaște persoana / persoanele din imagini ("*upload*" *simplu* sau "*upload*" *multiplu*);
- să seteze / selecteze manual câmpuri / criterii / filtre specifice obiectelor / proprietăților, definite în modelul conceptual ("*field-restricted search*"), câmpurile urmând a fi stabilite în urma procesului de analiză;-
- să selecteze manual fața / fețele ce urmează a fi supuse procesului de recunoaștere facială, în situația în care în imaginea probă au fost detectate mai multe fețe sau soluția nu a detectat nici o față în *imaginea probă* încărcată;

- să selecteze manual filtre pentru minimizarea efectelor produse de variațiile de iluminare și condițiile de captare a *imaginilor probă* (exemple neexhaustive; filtru pentru ajustarea contrastului și tonalității, normalizarea imaginii în raport cu distribuția nivelelor de intensitate a pixelilor, eliminarea anumitor frecvențe);

- să configureze un prag minim de încredere (acuratețe) a algoritmului de recunoaștere facială, pentru ca, în acest fel, în urma procesului de regăsire, în rezultat să fie incluse doar acele persoane pentru care scorul de "*matching*" este peste prag; să adauge *imaginea probă* într-un "*watchlist*", doar în situația în care persoana din imagine nu a fost recunoscută, cu scopul de a fi notificat în momentul în care persoana din imagine este recunoscută, prin compararea acesteia cu noile *imagini de referință* achiziționate.

2.20.6 Cerințe de acuratețe și performanță

Acuratețea procesului de recunoaștere facială va fi măsurată în funcție de numărul de *alarme false* raportat la numărul de regăsiri efectuate (*valoarea FPIR*) și numărul de "*misses*" raportat la numărul de regăsiri efectuate (*valoarea FNIR*), în timp ce performanța procesului de recunoaștere facială va fi măsurată în funcție de timpul de răspuns. În acest sens, vom defini următorul set de termeni:

- *identitatea unei persoane* este reprezentată de totalul *imaginilor de referință* ce corespund acesteia;

- "*misses*" sunt erori generate de soluția de recunoaștere facială, atunci când persoana dintr-o imagine probă, pentru care apriori se cunoaște că are corespondență în setul de *imagini de referință* (are identitate definită în sistem), este asociată în mod incorect cu o *imagine de referință* a unei alte *identități* definită în sistem; asocierea incorectă apare atunci când identitatea căutată nu se află printre identitățile returnate pe primele R poziții;

- "*false negative identification rate*" (*FNIR*) reprezintă numărul de "*misses*" raportat la numărul de regăsiri efectuate.

A. Măsurare "*misses*"

Scenariul 1 - inițial, bazat pe "*ranking*"

Din volumul de date existent, se vor alege 640.000 de identități. Pentru fiecare identitate, raportat la ordinea temporală de achiziție a imaginilor asociate, primele $n - 1$ vor fi utilizate ca și *imagini de referință* iar ultima ca *imagine de probă*. Astfel că, în etapa de

antrenare a algoritmilor de recunoaștere facială vor fi folosite mai mult de 640.000 de *imagini de referință*, iar din cele 640.000 de *imagini de probă*, 10.000 vor fi alese, în mod aleator, ca și *imagini de test*. În urma rulării procesului de recunoaștere facială pentru cele 10.000 de *imagini de test*, valoarea FNIR trebuie să se încadreze în limitele următoare:

- returnarea pe prima poziție a identității căutate în cel puțin 94% din cazuri ($FNIR \leq 0.06$);
- returnarea în primele 10 poziții a identității căutate în cel puțin 95% din cazuri ($FNIR \leq 0.05$);
- returnarea în primele 50 poziții a identității căutate în cel puțin 96% din cazuri ($FNIR \leq 0.04$).

Scenariul 2 - scalabilitate, bazat pe "ranking"

Din volumul de date existent, se vor alege 1.600.000 de identități. Pentru fiecare identitate, raportat la ordinea temporală de achiziție a imaginilor asociate, primele $n - 1$ vor fi utilizate ca și *imagini de referință* iar ultima ca *image de probă*. Astfel că, în etapa de antrenare a algoritmilor de recunoaștere facială vor fi folosite mai mult de 1.600.000 de *imagini de referință*, iar din cele 1.600.000 de *imagini de probă*, 10.000 vor fi alese, în mod aleator, ca și *imagini de test*. În urma rulării procesului de recunoaștere facială pentru cele 10.000 de *imagini de test*, valoarea FNIR trebuie să se încadreze în limitele următoare:

- returnarea pe prima poziție a identității căutate în cel puțin 93% din cazuri ($FNIR \leq 0.07$);
- returnarea în primele 10 poziții a identității căutate în cel puțin 95% din cazuri ($FNIR \leq 0.05$);
- returnarea în primele 50 poziții a identității căutate în cel puțin 96% din cazuri ($FNIR \leq 0.04$).

Scenariul 3 - "in the wild", bazat pe "ranking"

Din volumul de date existent, se vor alege 1.600.000 de identități. Pentru fiecare identitate, raportat la ordinea temporală de achiziție a imaginilor asociate, ultima va fi utilizată ca și *image de referință*. Astfel că, în etapa de antrenare a algoritmilor de recunoaștere facială vor fi folosite 1.600.000 de *imagini de referință*. Ca și *imagini de test*, vor fi folosite 100 de imagini inexistente în sistem, ale unor identități existente în sistem, pe care beneficiarul le

va pune la dispoziție. Aceste imagini de test pot prezenta orice particularitate în limitele descrise în capitolul *Imagini probă*. În urma rulării procesului de recunoaștere facială pentru cele 100 de *imagini de test*, valoarea FNIR trebuie să se încadreze în limitele următoare:

- returnarea pe prima poziție a identității căutate în cel puțin 85% din cazuri (FNIR $\leq$ 0.15).

B. Măsurare performanță

În etapa de antrenare a algoritmilor de recunoaștere facială vor fi folosite 1.000.000 de *imagini de referință* alese în mod aleator. Ca și *imagini de test*, vor fi folosite alte 10.000 de imagini diferite alese în mod aleator din imaginile de referință sau puse la dispoziție de către beneficiar. Soluția trebuie să ofere o medie a timpului de răspuns de sub 10 secunde, în condițiile în care toate cele 10.000 de regăsiri vor fi realizate într-un interval de 60 minute.

Pentru toate scenariile de măsurare a acurateței și a performanței soluției "face recognition", beneficiarul va trebui să asigure instrumente software de testare automată.

2.21 Servicii de implementare sistem monitorizare - (1 serviciu).

Soluția trebuie să ofere facilități pentru monitorizare și auditare a interacțiunii utilizatorilor cu sistemul informatic, precum și administrarea și monitorizarea modului de funcționare a componentelor software, hardware și de comunicații. Toate aceste activități trebuie susținute de politici și proceduri bine definite, a căror aplicabilitate conduce la creșterea calității serviciilor implementate.

Ca parte a infrastructurii generale de management, la nivelul platformei analitice și, în mod independent, la nivelul componentei de acces securizat în condiții de mobilitate, se vor implementa instanțe de colectare și de valorificare a semnalelor generate de senzori, a jurnalelor de operații generate de echipamentele și componentele software ale infrastructurii, precum și a jurnalelor specifice generate de componentele de aplicații.

Acestea vor putea fi configurate (cel puțin) să prezinte o imagine sintetică a stării generale a sistemului, să alerteze în cazul atingerii unor praguri de utilizare și/sau în cazul incidenței unor situații specific identificate, precum și să permită investigarea situațiilor de urgență operațională și a celor asimilabile unui incident de securitate.

2.21.1 Audit

Sistemul informatic trebuie să asigure o jurnalizare completă a evenimentelor, inclusiv activitățile utilizatorilor sau ale administratorilor. În acest sens trebuie să fie jurnalizate activitățile de regăsire și vizualizare a datelor, împreună cu contul de utilizator, ora, data și tipul acțiunii. Prin accesarea jurnalului de audit, administratorii sau utilizatorii speciali desemnați, trebuie să poată verifica informațiile despre tipul interacțiunii utilizatorilor cu sistemul, incluzând acțiuni precum logarea utilizatorilor (cu succes sau fără succes), vizualizarea unui obiect sau a unei înregistrări, respectiv exportul unor informații. Combinând detalii despre istoricul obiectelor, auditul trebuie să furnizeze o imagine completă a modalității de utilizare a sistemului de către beneficiari.

De asemenea sistemul informatic trebuie să asigure o soluție de management al logurilor cu următoarele capabilități:

- facilități de analiză a logurilor, prin existența unor mecanisme de transformare și procesare a logurilor;
- configurarea unor subcategorii de audit, cum ar fi:
 - excepții și trace-uri pentru API;
 - excepții pentru ACL-uri (aplicarea politicilor de securitate);
 - acțiuni de startup/shutdown aferente componentelor sistemului;
 - acțiuni specifice utilizatorilor - toate acțiunile efectuate de către utilizatori în cadrul sistemului vor fi auditate;
- posibilitatea de ignorare a auditului pentru unele acțiuni (în cazul în care acestea ar genera volume foarte mari de date de audit a căror stocare ar determina scăderi de performanță în utilizarea sistemului);
- jurnalizarea operațiilor generale precum login și logout;
- arhitectură scalabilă bazată pe mai multe noduri de procesare a logurilor;
- management centralizat al întregii soluții;
- posibilitatea de extindere a arhitecturii cu noduri suplimentare de procesare de loguri;
- posibilitatea de integrare cu sisteme de tip *"load balancing"* pentru nodurile de procesare;
- suport pentru păstrarea mesajelor de log în arhive cu capacități de *"multi-terabytes"*;

- suport pentru păstrarea mesajelor de log în arhive pentru audit pe perioade mari de timp (mai mari de 3 ani);
- posibilitatea definirii metodei de retenție a mesajelor de log pe bază de număr de mesaje sau intervale de timp;
- posibilitatea de parsare a logurilor primite în mai multe formate: syslog, json/xml, windows - nelimitat la acestea;
- posibilitatea de identificare a câmpurilor în fiecare mesaj de log și indexarea pe baza câmpurilor identificate;
- posibilitatea de definire de reguli de parsare a fiecărui mesaj în parte pe baza tipului de mesaj, formatului de mesaj sau a câmpurilor ce trebuie identificate în mesaj;
- posibilitatea de căutare în arhiva de loguri după orice câmp identificat sau pe bază de expresii regulate în cadrul întregului mesaj;
- posibilitatea de căutare în arhiva de loguri în mod relativ sau în mod absolut față de momentul căutării;
- posibilitatea de a afișa printr-un *"dashboard"* diferite rapoarte generate de căutări în arhiva de loguri pe baza câmpurilor identificate în mesajele de log;

Notă: - soluția de management va cuprinde minim 5 *rapoarte*, urmând ca forma și conținutul acestora să fie stabilit de către beneficiar, de comun acord cu furnizorul, în funcție de structura și semnificația datelor din mesajele de log;

- posibilitatea de a analiza evenimentele pe baza căutarilor folosind unul sau mai multe câmpuri identificate în mesajele de log;
- posibilitatea de a genera statistici pe baza oricărui câmp identificat în cadrul unui mesaj de log;
- posibilitatea de alertare și executare de acțiuni în momentul identificării unor evenimente în cadrul mesajelor de log;
- posibilitatea de rutare de mesaje de log între mai multe sisteme;
- posibilitatea de filtrare a mesajelor de log procesate și/sau modificarea lor în timpul procesării înainte de stocare;
- suport pentru primirea mesajelor de log atât prin TCP cât și prin UDP;
- integrare cu sisteme de tip LDAP pentru autentificarea utilizatorilor;

2.21.2 Administrare și monitorizare

Sistemul informatic trebuie să asigure administratorului accesul la componentele (grafice sau în linie de comandă) de administrare și de monitorizare a sistemului.

Consola de management centralizat pentru monitorizarea stării echipamentelor de rețea trebuie:

- să asigure o imagine de ansamblu a stărilor tuturor componentelor platformei Big Data, a Componentei de Acces, precum și a interacțiunii utilizatorilor cu aplicațiile;
- să asigure un mecanism de alertare bazat pe reguli, ce trebuie să poată fi particularizate ulterior, precum și explicitarea acțiunilor ce trebuiesc realizate la apariția unei alerte;
- să asigure posibilitatea alertării administratorilor prin e-mail sau SMS, fără a se limita la acestea;
- să asigure monitorizarea încărcării serverelor, utilizarea procesoarelor, a memoriei și a spațiului de stocare de pe disk, a numărului de servicii, a numărului de accesări;
- să asigure managementul sistemelor de operare eterogene, a mașinilor fizice sau virtuale astfel încât să poată furniza un suport consistent pentru relația dintre un host de virtualizare și mașinile virtuale găzduite de acesta, precum și pentru relația dintre mai multe host-uri de virtualizare corelate;
- să permită monitorizarea în timp real a echipamentelor de rețea;
- să includă *"plugin"*-uri predefinite pentru cei mai folosiți vendori;
- să permită definirea unor parametri de verificare ce pot identifica starea pentru cel puțin următoarele servicii: *"CPU load"*, *"file systems"*, *"TCP Connections"*, utilizare memorie RAM; HTTP, FTP, DNS, SMTP, NTP;
- să permită definirea de topologii cu echipamentele monitorizate;
- să permită asignarea de tag-uri pentru *"host"*-urile monitorizate; pentru o flexibilitate sporită consola trebuie să ofere posibilitatea adăugării mai multor tag-uri unui *"host"*, grup de *"host"*-uri monitorizate;
- să ofere integrare cu agent necesar monitorizării stațiilor Windows cât și Linux;
- să permită monitorizarea utilizând protocolul SNMP;
- să permită monitorizarea fișierelor de *"logging"* pentru serverele Windows și Linux;
- să permită definirea manuală de reguli și criterii de monitorizare;

- să ofere posibilitatea transmiterii datelor între *"host"* și consola de monitorizare printr-un canal criptat;
 - să ofere un mecanism de *"caching"* pentru verificarea stării dispozitivelor monitorizate și depanare;
 - să ofere un motor de monitorizare predictivă;
 - să asigure posibilitatea de *"backup"* și *"restore"*;
 - să ofere statistici despre performanțele consolei de monitorizare;
 - să asigure posibilitatea generării de rapoarte în funcție de diferite criterii: statusul echipamentelor monitorizate, per servicii, per încărcare CPU - nelimitat la acestea;
 - să ofere un motor de alertare bazat pe condiții logice;
 - să permită definirea de utilizatori cu drepturi diferite: de citire, citire-scriere sau de access doar la diferite configurații ale consolei de management;
 - să ofere un modul de căutare inteligent bazat cel puțin pe: *"IP host"*, grup de *"host"*-uri sau selecție de *"host"*-uri dintr-un grup, servicii (HTTP, SSH - nelimitat la acestea), interval periodic de la ultima schimbare a statusului serviciului, tag-uri, starea aplicației - nelimitat la acestea;
 - să ofere un motor pentru monitorizare distribuită și mai multe console de monitorizare să fie agregate la nivel logic într-o singură consolă de administrare;
 - să ofere un modul inteligent de agregare și monitorizare;
 - să ofere posibilitatea de instalare în mod *"High Availability"*;
- Alertarea administratorilor prin SMS se va realiza prin intermediul unui echipamentului hardware dedicat (*"gateway"* de SMS) ale cărui funcționalități și specificații tehnice sunt descrise în secțiunea 2.14.

2.22 Servicii de integrare cu portalul și access management - (1 serviciu)

2 Accesul utilizatorilor la sistemul SII ANALYTICS se poate face fie de la stații de lucru (de tip desktop), fie de la terminale mobile inteligente (de tip smartphone sau tabletă) prin Componenta de Acces. Pentru utilizatorii care vor accesa platforma Big Data de la stații de lucru, accesul se va face prin instanțele de tip portal existente, iar contextul tehnic de autentificare și autorizare a accesului va fi același.

- 3 Versiunea Portalului din SII Infrastructură este Oracle WebCenter Portal, versiunea 11.1.1.8, a managementului identității este Oracle Identity Management, versiunea 11.1.1.7, respectiv Oracle Acces Manager, versiunea 11.1.2.2 pentru controlul accesului.
- 4 În prezent fiecare utilizator are o identitate electronică unică gestionată în mod centralizat prin intermediul componentei existente de management al identităților electronice, care oferă administratorilor posibilitatea:
- definirii de attribute specifice pentru profilele utilizatorilor;
 - alocării de drepturi de acces pe bază de politici de acces asociate anumitor departamente, poziții sau altor attribute legate de profilul utilizatorului, astfel încât fiecare utilizator să aibă drepturi de acces doar la resursele necesare îndeplinirii sarcinilor de lucru specifice.
- 5 De asemenea, componenta de control al accesului utilizatorilor la Portalul existent și, implicit, la serviciile și datele expuse prin intermediul acestuia, asigură autentificarea (de tip Single Sign On) utilizatorilor prin intermediul certificatelor digitale stocate în dispozitive de tip token, cât și autorizarea utilizatorilor la resurse în conformitate cu drepturile de acces.
- 6 Pentru utilizatorii care vor accesa platforma Big Data prin Componenta de Acces informațiile necesare definirii identității, precum și a atributelor relevante ale acesteia (respectiv, cel puțin, roluri și drepturi de acces), vor fi selectate, filtrate și replicate către instanțele de servicii de management al identității și al politicilor de acces configurate ca parte a Componentei de Acces.
- 7 La nivelul Componentei de Acces, identități reale a utilizatorilor i se vor putea asocia identificatori pseudo-anonimi, pentru a crea unul sau mai multe profiluri de acces online, care vor fi folosite — de către aplicațiile mobile autorizate și de către instanțele centrale de tip server ale subsistemelor Componentei de Acces — pentru autorizarea accesului la resursele online ale sistemului fără a fi necesară, din punct de vedere tehnic, expunerea identității reale a utilizatorilor.
- 8 Corelarea identității convenționale și a celei reale a utilizatorilor se va realiza numai la nivelul subsistemelor offline ale sistemului, pentru autorizarea accesului la date.
- 9 La nivelul subsistemelor online, respectiv la nivelul aplicațiilor mobile autorizate înrolate în sistem și al instanțelor centrale de tip server al Componentei de Acces, se vor utiliza coduri (abstracte, nesugestive) ale funcționalităților specific invocate, ale serviciilor de aplicație, și ale câmpurilor din structurile de date la care se solicită accesul.

10 Politicile de acces la resurse, existente la nivelul surselor de referință ("*authoritative*") de management al identității și al accesului, vor fi translatate pentru operarea — la nivelul Componentei de Acces — cu identificatorii convenționali pseudo-anonimi și cu codurile de lucru.

În acest fel, accesul la resursele tehnice ale subsistemelor online ale Componentei de Acces se va putea face fără invocarea directă a identității reale a utilizatorilor autorizați, iar expunerea în mediu online a cererilor de acces la date nu va permite, chiar în ipoteza compromiterii unor mecanisme tehnice de protecție, decelarea organizării structurilor de date din mediul protejat offline, și nici a logicii care stă la baza politicilor de autorizare a accesului la resurse.

3. Securitatea sistemului

Soluția tehnică de implementare a noului sistem informatic "SII ANALYTICS", trebuie să se bazeze, din punct de vedere al securității, pe un model extrem de configurabil, cu granularitate fină, care să asigure acces corect și complet la date, dar și securitate sporită împotriva accesului neautorizat. Pentru a respecta aceste constrângeri, soluția propusă de furnizor va trebui să se conformeze, în ansamblul său, unui set minim de prevederi generale de securitate, sens în care trebuie:

- să ofere mecanisme de securitate la nivel hardware și software, care să permită protejarea informației atât față de accesul neautorizat intern, cât și față de accesul neautorizat extern, atunci când informația este stocată pe medii magnetice sau când este transportată în rețea;
- să asigure mecanisme de securitate implementate pe mai multe niveluri, care să permită restricționarea accesului la nivel de:
 - echipament de rețea, prin definirea unor rețele logice separate în funcție de necesitățile de securitate ale componentelor sistemului;
 - module funcționale, prin mecanisme avansate de autentificare și autorizare bazate pe roluri și permisiuni;
 - surse de date, conform principiilor "*need to know*" și "*need to share*";
- să permită configurarea politicilor de securitate (roluri și permisiuni / drepturi de acces la resurse) într-un mod uniform și centralizat, astfel încât accesul utilizatorilor să poată fi restricționat din punct de vedere al surselor de date și funcționalităților expuse de noul sistem

informatic (*la ce are acces?*), din punct de vedere al locației¹⁵ (*de unde?*) și din punct de vedere al momentului de timp (*când?*);

- să permită administrarea centralizată a utilizatorilor și a profilurilor asociate acestora;
- să permită navigarea în și între toate modulele funcționale, precum și accesarea tuturor funcțiilor și comenzilor la care utilizatorul este autorizat să dețină acces, menținând persistența sesiunii de lucru, fără a fi necesară deconectarea și reconectarea ca utilizator al aplicației;
- să restricționeze accesul utilizatorului final la date doar prin intermediul interfețelor grafice aferente modulelor funcționale;

3.1 Nivel echipamente de rețea

Sistemul trebuie să permită restricționarea accesului la echipamentele de rețea. Acest lucru implică definirea unor rețele logice separate în funcție de necesitățile de securitate ale componentelor sistemului.

Sistemul va permite auditarea accesului la echipamentele de rețea.

Echipamentele de rețea vor fi de înaltă performanță, care să poată asigura un nivel ridicat de securitate, fiabilitate și scalabilitate sistemului ce va fi implementat.

Echipamentele vor fi amplasate într-o rețea logică separată de cea a utilizatorilor.

Protecția rețelelor logice va fi asigurată prin intermediul echipamentelor de tip firewall. Prin intermediul acestora accesul va fi granularizat până la nivel de IP și port.

3.2 Nivel de date

- trebuie să asigure accesul partajat la resurse, prin restricționarea accesului la nivel de date, conform principiilor *"need to know"* și *"need to share"*, precum și în funcție de depozitul de date comune și seturile de date individuale, prin roluri și privilegii setate la nivelul componenței de management a identității (Oracle Identity Management, versiunea 11.1.1.7);
- trebuie să asigure securitatea surselor de date și a oricărui depozit de date propriu noului sistem informatic, având în vedere cel puțin următoarele aspecte: controlul accesului, auditarea operațiunilor efectuate de utilizatori și verificarea integrității datelor;
- trebuie să asigure măsuri logice și fizice de păstrare a consistenței surselor de date și a oricărui alt depozit de date propriu noului sistem informatic;

¹⁵ cel puțin pentru Platforma Big Data;

- trebuie să mențină într-o stare consistentă, în cazul apariției un incident fizic sau logic, toate informațiile stocate în sursele de date și în orice alt depozit de date propriu noului sistem informatic;
- trebuie să asigure repunerea în funcțiune, după o avarie, a oricărui depozit de date propriu noului sistem informatic, asigurând totodată validarea integrității datelor recuperate cât și a drepturilor utilizatorilor de acces la datele stocate.

3.3 Nivel aplicație

- trebuie să asigure protecția față de accesul neautorizat sau rău intenționat, prin mecanisme care permit autentificarea unică și autorizarea utilizatorilor pe bază de roluri și permisiuni;
- trebuie să asigure accesul partajat la resurse, prin restricționarea accesului la nivel de module funcționale ale noului sistem informatic;
- trebuie să asigure vizibilitatea, prin intermediul modulelor funcționale, doar la datele stocate în sursele de date la care utilizatorul are acces;
- trebuie să permită identificarea, verificarea drepturilor și permisiunilor, supravegherea cererilor de servicii și operațiilor executate de fiecare utilizator;
- trebuie să permită administratorului sistemului să controleze accesul fiecărui utilizator la modulele funcționale ale noului sistem informatic, prin roluri și privilegii setate la nivelul componentei de management a identității (Oracle Identity Management, versiunea 11.1.1.7);
- trebuie să asigure monitorizarea interacțiunii utilizatorului cu interfața grafică, prin intermediul mecanismelor de tip log și audit;
- trebuie să asigure limitarea funcționalităților disponibile unui utilizator, în conformitate cu drepturile asociate.

3.4 Backup și restaurare a datelor

- trebuie să asigure mecanisme de efectuare a copiilor de siguranță prin intermediul unei soluții de back-up care să suporte sistemele de operare și care să se integreze cu modulele funcționale ale noului sistem informatic;
- trebuie să asigure salvarea și restaurarea datelor unice (nemodificate), precum datele sistemului de operare, documentele și datele existente pe serverele și mediile virtuale;

- trebuie să permită efectuarea de salvări complete, incrementale și diferențiale, atât pe benzi magnetice, cât și pe disc, în clar, criptat și/sau comprimat;
- trebuie să asigure restaurarea datelor corupte de viruși, erori software sau erori umane prin posibilitatea de a reveni la o versiune generată la un interval de timp configurabil de către administrator;
- trebuie să permită restaurarea rapidă a datelor în cazul unei defecțiuni temporare sau permanente, hardware sau software.

3.5 Confidențialitatea datelor

Pentru protecția datelor, sursele de referință — respectiv, bazele de date și structurile de tip *"repository"*, pentru date nestructurate, precum și metadatele generate ca urmare a procesării semantice, de către platforma Big Data — vor fi stocate pe termen indefinit numai la nivelul componentelor offline ale sistemului.

La nivelul acestora, accesul în clar la date se va putea face numai prin instanțe de servicii de aplicație, care vor accesa datele direct sau prin intermediul funcționalității native ale sistemelor de gestiune a bazelor de date (SGBD), și va fi în mod riguros autorizat și auditat.

Accesul administrativ, în scopuri de gestiune tehnică a datelor, va putea fi separat de accesul la conținutul de informație obiect, inclusiv prin politici de autorizare explicită și prin mecanisme de protecție criptografică transparentă ce operează independent, în cascadă, la nivelul infrastructurii sistem (cel puțin la nivelul sistemelor de stocare consolidată) și la nivelul serviciilor de aplicație.

La nivelul instanțelor centrale de tip server, din subsistemele online ale Componentei de Acces, datele obiect vor fi primite, de la subsistemele offline, numai pe baza unei cereri autorizate de acces și numai în formă criptată.

Pe terminalele mobile inteligente înrolate în sistem, toate informațiile primite, în răspuns la cererile autorizate de acces, vor fi stocate de către fiecare aplicație mobilă autorizată numai în formă criptată și vor putea fi transferate local, pe terminalul mobil inteligent, numai în formă criptată și numai între aplicațiile mobile autorizate.

Pe toate resursele online, respectiv atât la nivelul terminalelor mobile inteligente, cât și la nivelul instanțelor de servicii din subsistemele centrale ale Componentei de Acces, datele obiect vor putea fi disponibile numai atât timp cât este stric necesar.

După scurgerea termenului de valabilitate a autorizării accesului, precum și în cazul revocării autorizării, datele confidențiale vor fi protejate prin distrugerea imediată a materialului criptografic necesar decriptării, precum și prin ștergerea datelor criptate.

Această politică, în baza căreia scrierea datelor — pe mediile de stocare persistentă ale terminalelor mobile inteligente autorizate și ale echipamentelor ce deservește subsistemele online ale Componentei de acces — se va face numai în formă criptată, va asigura un nivel de suplimentar de protecție împotriva accesului la date (în clar) prin utilizarea neautorizată a unor mijloace tehnice de recuperare (de tip *"forensic"*) a datelor marcate ca șterse, chiar în ipoteza pierderii controlului asupra mediilor de stocare persistentă.

Pentru respectarea caracterului confidențial al datelor, inclusiv prin protejarea identității utilizatorilor autorizați și a contextului în care s-a autorizat accesul la date, instanțele de tip browser și aplicațiile web (HTML5 sau echivalente) vor comunica cu instanțele centrale de servicii ale Componentei de Acces numai prin sesiuni protejate prin tehnici de tip SSL/TLS, sau echivalente.

În același scop, aplicațiile mobile native autorizate care rulează pe terminalele mobile inteligente înrolate în sistem vor comunica cu instanțele centrale de servicii ale Componentei de Acces numai prin mecanisme de tip WS/API care presupun transmiterea informației, inclusiv prin mesaje de tip JSON sau XML, exclusiv în formă criptată.

Prin intermediul mecanismelor native ale suitei EMM, se va asigura că fiecare aplicație mobilă care rulează pe terminalele mobile inteligente înrolate în sistem, care vor comunica cu instanțele centrale de servicii ale Componentei de Acces, vor beneficia în mod transparent de o anvelopă criptografică (*"application level VPN"*) funcțional independentă de aplicație.

Prin intermediul mecanismelor soluției de tip VPN pentru terminale mobile, se va asigura că toate aplicațiile mobile care rulează pe fiecare terminal mobil inteligent înrolat în sistem, care vor comunica cu instanțele centrale de servicii ale Componentei de Acces, vor beneficia în mod transparent de o anvelopă criptografică (*"terminal level VPN"*) administrativ independentă de funcționalitățile native ale sistemului de operare al terminalului mobil inteligent.

4. Servicii de Instruire

Instruirea personalului care va asigura mentenanța soluției, cât și a personalului care va utiliza produsele software implementate va fi realizată de către furnizor, această activitate având un rol esențial în garantarea acceptanței produselor livrate și a întregului proiect.

Cursurile vor fi destinate atât utilizatorilor finali, cât și dezvoltatorilor de aplicații și administratorilor acestui sistem.

Beneficiarul, împreună cu furnizorul proiectului, vor stabili de comun acord datele de început ale cursurilor de instruire pe baza planificării proiectului și disponibilității cursanților, durata acestora, precum și locația de desfășurare, cu mențiunea că persoanelor instruite li se va asigura cazarea, masa și transportul până la locul de desfășurare, în cazul în care locația de desfășurare a acestora este în afara Municipiului București.

Beneficiarul va stabili, la nivel intern, lista participanților la cursurile de instruire și va comunica responsabilului de proiect din partea furnizorului lista de cursanți.

Ofertantul va face dovada capacității acestuia de organizare a cursurilor oferite (spații, materiale, echipamente, etc.), precum și modalitatea de asigurare a instructorilor necesari.

4.1 Desfășurarea instruirii

Instruirea se va desfășura conform planului de instruire stabilit și agreeat contractual.

Pentru instruirea personalului care va asigura mentenanța sistemului, furnizorul va asigura infrastructura hardware, software și suportul de curs. Instruirea personalului se va realiza de către firma/firmele care va/vor câștiga licitația de furnizare a echipamentelor și de implementare a sistemului și conform caietelor de sarcini care vor fi întocmite. Costurile cu locația de desfășurare a cursurilor vor fi în responsabilitatea implementatorului. Instruirea se va face pe baza suportului de curs, livrat de furnizor fiecărui participant. Acest suport de curs poate conține și exemple practice pentru o mai bună înțelegere a modului de funcționare și administrare a sistemului, precum și alte detalii legate de acesta.

Pentru instruirea personalului care va utiliza produsele software implementate, solicitantul finanțării va asigura locația de desfășurare a cursurilor și stații de lucru pentru fiecare cursant. Instruirea se va face pe baza suportului de curs, livrat de furnizor fiecărui participant.

La sfârșitul fiecărei sesiuni de instruire se vor elabora documentele:

- prezență la curs;
- diplomă de participare.

4.2 Cursuri utilizatori finali - (1 pachet)

Pentru instruirea personalului care va utiliza produsele software implementate, resursele materiale destinate instruirii vor fi puse la dispoziție atât de către beneficiar (săli de curs, stații de lucru conectate la infrastructura dezvoltată în cadrul proiectului), cât și de furnizor (suportul de curs).

În vederea instruirii personalului care va utiliza produsele software implementate, furnizorul va asigura instruirea a minim 45 de utilizatori finali / formatori ai sistemului, în minim 3 serii a câte minim 15 zile / serie, cursuri ce vor acoperi toate serviciile furnizate beneficiarilor prin implementarea sistemului informatic.

4.3 Cursuri, concepte și modele teoretice pentru modulele aferente platformei Big Data - (1 pachet).

- pachet de minim 7 cursuri concepte și modele teoretice pentru modulele aferente platformei Big Data, care să conțină cel puțin câte un curs pentru fiecare funcționalitate implementată în cadrul platformei Big Data: **minim 225 zile-om distribuite astfel:**

- minim 2 cursuri de câte 10 zile, pentru un număr total minim de 9 persoane (minim 90 **zile-om**)¹⁶;
- minim 5 cursuri de câte 5 zile, pentru un număr total minim de 27 persoane (minim 135 **zile-om**);

Notă: - pentru întreg pachetul de cursuri, vor fi asigurate cursuri de producător pentru fiecare din funcționalitățile/modulele din cadrul platformei Big Data furnizate.

4.4 Cursuri, concepte și modele teoretice pentru modulul de Face Recognition - (1 buc.)

- curs concepte și modele teoretice pentru modulul de *Face Recognition*: **minim 20 zile-om distribuite astfel:**

¹⁶ 90 zile-om = 10 zile de instruire pentru un total de 9 persoane instruite (distribuite în mod variabil în cadrul a două cursuri)

De ex.

(1 curs x 10 zile x 4 pers)+ (1 curs x 10 zile x 5 pers) = 90 zile-om sau

(1 curs x 10 zile x 6 pers)+ (1 curs x 10 zile x 3 pers) = 90 zile-om

- minim 1 curs de 5 zile, pentru un număr minim de 4 persoane (minim 20 **zile-om**);

Notă: - se va asigura curs de producător pentru modulul de Face Recognition.

4.5 Cursuri administrare, referință, operare și utilizare pentru modulele aferente Big Data - (1 pachet)

- pachet de minim 9 cursuri administrare, referință, operare și utilizare pentru modulele aferente platformei Big Data, care să conțină cel puțin câte un curs pentru fiecare funcționalitate implementată în cadrul platformei Big Data: **minim 234 zile-om distribuite astfel:**

- minim 3 cursuri a câte 3 zile, pentru un număr total minim de 18 persoane (minim 54 **zile-om**);
- minim 6 cursuri a câte 5 zile, pentru un număr total minim de 36 persoane (minim 180 **zile-om**);

4.6 Cursuri administrare, referință, operare și utilizare pentru modulul de Face Recognition - (1 buc.)

- curs administrare, referință, operare și utilizare pentru modulul de *Face Recognition*: **minim 20 zile-om** distribuite astfel:

- minim 1 curs de 5 zile, pentru un număr total minim de 4 persoane (minim 20 **zile-om**);

4.7 Cursuri administrare, referință, operare și utilizare pentru aplicațiile componentei de acces în condiții de mobilitate - (1 buc.)

- curs administrare, referință, operare și utilizare pentru aplicațiile componentei de acces în condiții de mobilitate: **minim 20 zile-om**, distribuite astfel:

- minim 1 curs de 5 zile, pentru un număr total minim de 4 persoane (minim 20 **zile-om**);

4.8 Cursuri administrare, referință, operare și utilizare pentru infrastructura Componentei de Acces în condiții de mobilitate - (1 pachet)

• pachet de minim 13 cursuri administrare, referință, operare și utilizare pentru infrastructura Componentei de Acces în condiții de mobilitate, care să conțină cel puțin următoarele tipuri de cursuri:

- curs transfer cunostințe - Soluție Stocare de Mare Performanță;
- curs transfer cunostințe - Soluție Virtualizare;
- curs transfer cunostințe - Soluție *Diode de Date*;
- curs transfer cunostințe - Soluție de tip WS/API Gateway;
- curs transfer cunostințe - Soluție de asigurare a serviciilor criptografice;
- curs transfer cunostințe - Suita "*Enterprise Mobility Management*" (administrare de baza);
- curs transfer cunostințe - Suita "*Enterprise Mobility Management*" (configurare și dezvoltare);
- curs transfer cunostințe - Suita "*Enterprise Mobility Management*" (administrare de securitate);
- curs transfer cunostințe - Soluție de VPN;
- curs transfer cunostințe - Soluție de protecție anti-intruziune;
- curs transfer cunostințe - Soluție de zonare și de protecție a rețelelor;
- curs transfer cunostințe - Soluție de monitorizare a comunicațiilor;
- curs transfer cunostințe - "*Application Delivery Controller*";

minim 286 zile-om distribuite astfel:

- minim 5 cursuri de câte 3 zile, pentru un număr total minim de 27 persoane (minim 81 **zile-om**);
- minim 7 cursuri de câte 5 zile, pentru un număr total minim de 39 persoane (minim 195 **zile-om**);
- minim 1 curs de 2 zile, pentru un număr minim de 5 persoane (minim 10 **zile-om**).

4.9 Cursuri tehnologii - (1 pachet)

- pachet de minim 10 cursuri tehnologii, care să aparțină următoarelor categorii de cursuri:

- cursuri tehnologii front-end : **minim 59 zile-om, *distribuite astfel***:
 - minim 1 curs de 3 zile, pentru un număr minim de 3 persoane (minim 9 zile-om);
 - minim 1 curs de 4 zile, pentru un număr minim de 5 persoane (minim 20 zile-om);
 - minim 1 curs de 5 zile, pentru un număr minim de 6 persoane (minim 30 zile-om);
- cursuri tehnologii back-end: **minim 135 zile-om *distribuite astfel***:
 - minim 2 cursuri de câte 3 zile, pentru un număr total minim de 6 persoane (minim 18 zile-om);
 - minim 2 cursuri de câte 4 zile, pentru un număr total minim de 8 persoane (minim 32 zile-om);
 - minim 3 cursuri de câte 5 zile, pentru un număr total minim de 17 persoane (minim 85 zile-om);
- cursuri tehnologii native "mobile": **minim 12 zile-om *distribuite astfel***:
 - minim 1 curs de 4 zile, pentru un număr minim de 3 persoane (minim 12 zile-om);

4.10 Cursuri management - (1 pachet)

- pachet de minim 4 cursuri management, care să conțină cel puțin următoarele tipuri de cursuri:

- cursuri de business analysis: **minim 15 zile-om** distribuite astfel:
 - minim 1 curs de 5 zile, pentru un număr minim de 3 persoane (minim 15 **zile-om**);
- cursuri de management servicii IT - ITIL: **minim 15 zile-om** distribuite astfel:
 - minim 1 curs de 5 zile, pentru un număr minim de 3 persoane (minim 15 **zile-om**);
- curs PRINCE Foundation & Practitioner: **minim 20 zile-om** distribuite astfel:

- minim 1 curs de 5 zile, pentru un număr minim de 4 persoane (minim 20 **zile-om**);
- curs Agile PM Foundation & Practitioner: **minim 20 zile-om** distribuite astfel:
 - minim 1 curs de 5 zile, pentru un număr minim de 4 persoane (minim 20 **zile-om**);

5. Instalare echipamente în Centrul de Date

Echipamentele hardware din centrul de date vor fi instalate în maxim 10 rack-uri de 42U, existente la beneficiar. Fiecare rack este echipat cu două PDU-uri cu conecție IEC-320 C13 (36), IEC-320 C19 (6) fiecare dintre ele conectate la câte un circuit electric asigurat de UPS de 220V/32A. Distribuția echipamentelor în rack-uri va fi stabilită împreună cu beneficiarul.

Furnizorul va asigura conecția suplimentară necesară interconectării echipamentelor (patchcord-uri/patchpanel-uri fibră optică, patchcord-uri/patchpanel-uri UTP).

Implementarea sistemului intră în atribuțiile ofertantului și va conține toate componentele, după cum urmează:

- provizionarea tuturor serverelor de procesare, soluției de gestionare a datelor, echipamentelor de comunicații, sistemelor de operare, bazelor de date, a integrării cu rețeaua beneficiarului;
- provizionarea tuturor serviciilor aferente: instalarea și testarea tuturor echipamentelor (incluzând și cablarea acestora) și instalarea și testarea tuturor componentelor software;
- în vederea optimizării procesului de implementare a sistemului pentru bazele de date, furnizorul va efectua următoarele operațiuni:
 - crearea unui plan personalizat de instalare și configurare;
 - verificarea tuturor prerechizitelor înaintea livrării și implementării echipamentelor:
 - locație;
 - necesar de alimentare electrică;
 - necesar de răcire;
 - amplasament;
 - necesar infrastructură rețea;
 - eliminarea ambalajului echipamentelor și verificarea stării acestora;

- instalarea echipamentelor conform cu manualele de instalare ale producătorilor;
- configurarea echipamentelor hardware aferente;
- instalarea și configurarea sistemelor de operare și a unei baze de date de test pentru validare;
- instalarea eventualelor actualizări firmware, sistem de operare, baze de date în cazul în care există probleme de interoperabilitate;
- interconectarea echipamentelor instalate, incluzând configurarea și instalarea cablurilor;
- asigurarea conectivităților LAN cu echipamente de conectare la rețeaua de comunicații de bandă largă;
- efectuarea testelor standard funcționale și de diagnostic folosind instrumentele producătorilor echipamentelor în vederea verificării funcționării optime.

6. Managementul proiectului

- ofertantul va asigura activitatea de management a proiectului, astfel încât să se asigure respectarea graficului de activități conform diagramei Gantt pusă la dispoziție de către beneficiar și anexată caietului de sarcini (**Anexa 2 - Diagrama Gantt**).

- în maxim 21 de zile de la semnarea contractului de furnizare, furnizorul va prezenta beneficiarului, sub formă de livrabile, următoarele documente:

- planul de proiect în concordanță cu diagrama Gantt pusă la dispoziție de către beneficiar;
- metodologia urmată în dezvoltarea, testarea și implementarea cerințelor funcționale;
- managementul riscurilor;
- procedurile de management al schimbărilor.

Pe parcursul implementării proiectului, la fiecare 30 de zile se va preda în format electronic, versiunea actualizată a documentelor mai sus menționate, precum și stadiul de realizare, corelat cu evoluția proiectului.

Furnizorul își va fi îndeplinit obligațiile privind activitatea de managementul proiectului atunci când materialele livrate vor fi analizate și acceptate de către beneficiar. Răspunsul privind acceptarea livrabilelor va fi dat în 5 zile lucrătoare de la primire sau, dacă este cazul, beneficiarul va furniza o listă scrisă a revizuirilor solicitate.

7. Criterii de acceptanță

Acceptanța finală a lotului I se va realiza în baza unui protocol de acceptanță semnat atât de către furnizor cât și de beneficiar la finalizarea livrării și instalării, respectiv configurării tuturor componentelor.

Acceptanța finală a lotului I se va realiza în baza unui Protocol de Acceptanță agreat și semnat atât de către furnizor cât și de către beneficiar la finalizarea lotului I. Protocolul de Acceptanță va fi semnat după ce toate procesele verbale de acceptanță parțială aferente componentelor hardware/software/servicii (1, 2, 4) ce fac obiectul contractului, vor fi semnate.

7.1 Criterii acceptanță Componentă de Acces

Procesul verbal de acceptanță parțială pentru Componenta de Acces, va cuprinde rezultatele testelor funcționale și de performanță. Scenariile de testare vor fi stabilite de comun acord, livrate de către furnizor și agreate de către beneficiar, în scopul verificării îndeplinirii următoarelor criterii de acceptanță ale aplicațiilor mobile instalate în mediul controlat generat de componentele MDM și MAM ale suitei EMM, prin intermediul cărora utilizatorii pot interacționa cu nivelul BUFFER (online), pentru accesul autorizat la datele protejate furnizate de nivelul CORE (offline), și se vor conforma unui set de cerințe de performanță, sens în care trebuie:

- să asigure o medie a timpului de răspuns de sub 10 secunde, în condițiile în care 50 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru modulele "full text search", "spatial search", "link analysis" și "spatial analysis", adaptate pentru accesul de pe terminalele mobile inteligente;
- să asigure o medie a timpului de răspuns de sub 15 secunde, pentru 100 de regăsiri în cadrul modulului "face recognition", adaptat pentru accesul de pe terminalele mobile inteligente;

De asemenea, criteriile de acceptanță ale componentei de acces securizat în condiții de mobilitate sunt legate de încheierea cu succes a celor cinci fluxuri de lucru prezentate în secțiunea 1.19.3.5 - *Fluxuri de date*:

- fluxul de autentificare și autorizare inițială, la nivelul terminalului mobil;
- fluxul de utilizare a aplicațiilor în mediul protejat, pe terminalul mobil;
- fluxul de acces securizat în regim de mobilitate;

- fluxul de comunicare colaborativă securizată în mediul online;
- fluxul de acces la serviciile de aplicație și la resursele de date protejate.

7.2 Criterii de acceptanță - Platforma Big Data

Procesul verbal de acceptanță parțială pentru platforma Big Data, va cuprinde rezultatele testelor funcționale și de performanță. Scenariile de testare vor fi stabilite de comun acord, livrate de către furnizor și agreate de către beneficiar.

- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "full text search";
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "spatial search";
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "query builder";
- să asigure o medie a timpului de răspuns de sub 10 secunde, în condițiile în care se vor efectua 10.000 de regăsiri într-un interval de 60 minute, pentru "face recognition";
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "link analysis";
- să asigure o medie a timpului de răspuns de sub 5 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "spatial analysis";
- să asigure o medie a timpului de răspuns de sub 30 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "semantic analytics";
- să asigure o medie a timpului de răspuns de sub 60 secunde, în condițiile în care 500 de utilizatori concurenți vor efectua regăsiri într-un interval de 60 minute, pentru "behavioral analytics";

- să asigure integrarea cu Portalului web existent¹⁷, administrat de beneficiar, achiziționat și configurat în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea unui punct unic de acces centralizat la instrumentele software grafice furnizate;

- să asigure integrarea cu soluția de control acces existentă¹⁸, administrată de către beneficiar, achiziționată și configurată în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea autentificării unice¹⁹ și autorizării pe bază de roluri și permisiuni;

- să asigure integrarea cu soluția existentă de management al identității²⁰, administrată de către beneficiar, achiziționată și configurată în cadrul proiectului "SII INFRASTRUCTURĂ", pentru asigurarea condițiilor necesare unui management centralizat și reutilizare a utilizatorilor, profilurilor asociate acestora, respectiv organizațiilor existente.

Referitor la modulul de "*face recognition*", soluția trebuie să respecte și cerințele formulate în cadrul secțiunii 2.20.6 - Cerințe de acuratețe și performanță.

7.3 Criterii de acceptanță - Servicii de Instruire

Procesul verbal de acceptanță parțială pentru serviciile de instruire, va cuprinde dovada desfășurării activității de instruire, conform cerințelor formulate în secțiunea 4 - Servicii de Instruire.

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

La sfârșitul fiecărei sesiuni de instruire se vor elabora documentele:

- prezența la curs;
- diplomă de participare.

7.4 Livrabile

Furnizorul va pune la dispoziție, în format electronic, următoarele manuale și documentații:

- manuale de instalare și configurare a echipamentelor și software-ului de bază;

¹⁷ Oracle WebCenter Portal, versiunea 11.1.1.8

¹⁸ Oracle Acces Manager, versiunea 11.1.2.2

¹⁹ Single Sign On

²⁰ Oracle Identity Management, versiunea 11.1.1.7

- manuale de administrare sistem (echipamente hardware și module software ale componentelor/soluțiilor);
- documentația tehnică/funcțională a echipamentelor/componentelor soluțiilor;
- documentația aferentă arhitecturii integrate a sistemului informatic, precum și documentațiile aferente arhitecturilor componentelor sistemului, atât la nivel hardware cât și software și comunicații;
- documentația aferentă procesului de integrare a platformei Big Data cu Portalul existent la beneficiar, inclusiv din punct de vedere al controlului accesului și managementului identității;
- metodologia de configurare a securității la nivelul componentelor sistemului;
- manuale de utilizare aferente aplicațiilor platformei Big Data și ale aplicațiilor adaptate pentru accesul mobil, necesare utilizatorilor finali;
- raportul de identificare a cerințelor funcționale, raportul de analiză complet, planul de implementare și documentația de elaborare a specificațiilor funcționale, elaborate în urma finalizării activității de analiză, atât pentru platforma Big Data, cât și pentru componenta de acces securizat în condiții de mobilitate;
- raport cu rezultatele testelor funcționale și de performanță aferente modulelor platformei Big Data și variantei adaptată pentru mobil în urma finalizării activității de testare funcțională și de performanță.

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

Furnizorul își va fi îndeplinit obligațiile privind activitatea de livrare a documentelor menționate mai sus atunci când materialele livrate vor fi analizate și acceptate de către beneficiar. Răspunsul privind acceptarea livrabilelor va fi dat în 5 zile lucrătoare de la primire sau, dacă este cazul, beneficiarul va furniza o listă scrisă a revizuirilor solicitate.

8. Facilități puse la dispoziția furnizorului

În vederea susținerii procesului de implementare a sistemului informatic “SII ANALYTICS”, beneficiarul va pune la dispoziția echipei de lucru din partea furnizorului, o sala de 40 m², pe care furnizorul o va mobila și dota cu stații de lucru după propriile nevoi.

9. Drepturi de proprietate intelectuală

Toate documentele realizate în cadrul proiectului "SII ANALYTICS - Sistemul Informatic de integrare și valorificare operațională și analitică a volumelor mari de date" sunt proprietatea exclusivă a beneficiarului și nu pot fi utilizate de către furnizor și/sau terți.

Orice rezultate sau drepturi, inclusiv drepturi de autor și/sau orice alte drepturi de proprietate intelectuală și/sau industrială, obținute din implementarea proiectului SII ANALYTICS vor fi proprietatea exclusivă a achizitorului, care le va putea utiliza, publica, cesa ori transfera așa cum va considera de cuviință, fără limitare geografică ori de altă natură, cu excepția situațiilor în care există deja asemenea drepturi de proprietate intelectuală ori industrială.

Suplimentar, codul sursă aferent implementării cerințelor specifice formulate de către Autoritatea Contractantă, va fi deținut în proprietatea intelectuală de către Autoritatea Contractantă.

Dreptul de proprietate asupra tuturor echipamentelor IT&C ce fac obiectul unei tranșe de livrare va trece de la furnizor la achizitor la data semnării procesului verbal de recepție aferent tranșei respective. Dreptul de proprietate asupra aplicației informatice va trece de la furnizor la achizitor la data semnării procesului verbal de recepție finală și punere în funcțiune a sistemului.

10. Garanție și suport tehnic

Pentru componentele hardware și software ale sistemului, din cadrul lotului I, furnizorul va garanta menținerea tuturor funcționalităților prin asigurarea garanției și suportului tehnic, a actualizărilor firmware și software, la un nivel de performanță cel puțin la fel cu cel de la punerea în funcțiune (de la acceptanță) pe toată perioada de viață declarată de acesta. Această perioadă nu poate fi mai mică decât perioada considerată ca referință de achizitor privind exploatarea la un nivel de eficiență de 100% a echipamentelor și produselor software din cadrul lotului, definită în cadrul proiectului. Garanția tehnică va începe de la data semnării protocolului de acceptanță finală a sistemului informatic.

Serviciile de garanție hardware vor include serviciu de tip RMA pentru echipamentele sau componentele defecte, și suport tehnic autorizat 8/5, pe bază de SLA de tip "parts-

replacement onsite", inclusiv înlocuirea și reconfigurarea sistemului pentru reluarea serviciului, și timp de răspuns de tip "Next Business Day" (NBD).

În perioada de garanție și suport tehnic, Furnizorul va asigura analiza tehnică a actualizărilor necesare infrastructurii tehnologice livrate. Această analiză constă în evaluarea separată a aplicațiilor, a instanțelor sau a tehnologiilor folosite în cadrul sistemului și identificarea seturilor de patch-uri care pot îmbunătăți disponibilitatea sau performanța.

Analiza are scopul de a propune o serie de recomandări care adresează:

- Specificarea patch-urilor care necesită aplicare;
- Indicarea patch-urilor cunoscute sau noi versiuni ale aplicațiilor care provin de la alți furnizori;
- Modul de aplicare a patch-urilor;
- Revizuirea documentațiilor aferente;
- Revizuirea instalării, a pașilor de urmat, dacă este cazul.

Această analiză se va realiza o dată pe semestru cu un număr minim de 5 zile alocate pentru fiecare semestru. Rezultatul activităților realizate va fi prezentat sub formă de rapoarte detaliate, incluzând concluzii bazate pe practicile recomandate de către producătorul soluțiilor și documentația corespunzătoare rezultată în urma analizei.

11. Service Level Agreement (SLA) - Mediu de producție și de dezvoltare/testare

După finalizarea implementării proiectului, pe toată perioada de garanție a sistemului, furnizorul va asigura respectarea prevederilor SLA.

Furnizorul va asigura un sistem de ticketing în vederea gestionării incidentelor apărute în exploatarea sistemului.

În funcție de tipul incidentelor, furnizorul va asigura următorii timpi de răspuns și de remediere:

Mediu	Componentă a sistemului	Incident URGENT/CRITIC			Incident MAJOR			Incident MINOR		
		Timp de răspuns	Timp remediere provizorie / temporară	Timp de remediere*	Timp de răspuns	Timp remediere provizorie / temporară	Timp de remediere*	Timp de răspuns	Timp remediere provizorie / temporară	Timp de remediere*
PRODUCȚIE	Hardware	2 ore	N/A	7 zile	8 ore	N/A	7 zile	24 ore	N/A	7 zile
	Software de baza	2 ore	8 ore	24 ore	8 ore	48 ore	5 zile	24 ore	5 zile	7zile
	Aplicații software specifice	2 ore	8 ore	24 ore	8 ore	48 ore	5 zile l	24 ore	5 zile	7zile
DEZVOLTARE/TESTARE	Hardware				8 ore	N/A	5 zile	24 ore	N/A	7 zile
	Software de baza				8 ore	48 ore	5 zile	24 ore	5 zile	7 zile
	Aplicații software specifice				8 ore	48 ore	5 zile	24 ore	5 zile	7 zile

* În cazul în care software-ul de bază, aplicațiile sau tehnologiile folosite necesită corectarea unui bug și/sau construcția unui patch de la producător, timpul de remediere se va modifica cu timpul necesar producătorului să construiască patch-ul și/sau corecteze bug-ul.

Legendă:

- Timp de Răspuns: timpul scurs de la anunțul inițial înregistrat de client prin metodele de comunicare stabilite în procedura de suport tehnic (stabilită de comun acord ulterior semnării contractului de furnizare) și răspunsul primit de la echipa de suport tehnic a furnizorului către client. Răspunsul va conține termenul până la care incidentul va fi remediat, cel puțin printr-o soluție alternativă temporară. Timpul de remediere menționat în tabel se va prelungi cu durata de timp necesară pentru clarificarea incidentului.

- Timp de Remediere: durata de timp de la constatarea de către furnizor a defecțiunii până la implementarea soluției finale.

- Remediere Provizorie/Temporară: o modificare în cadrul procedurilor sau datelor care permite desfășurarea activității utilizatorului, ca soluție care evită temporar manifestarea defectului reclamat.

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

Triajul incidentelor se va face în funcție de gradul de urgență a acestora:

Denumire	Descriere
<i>Urgent</i>	Impact Major asupra funcționării sistemului. Incidentul împiedică desfășurarea activității instituției, care este serios afectată, pierderea funcționalităților devenind critică.
<i>Critic</i>	Impact Semnificativ asupra funcționării sistemului. Incidentul împiedică desfășurarea în condiții normale a activității utilizatorilor. Nu sunt disponibile solutii alternative pentru functionalitatea in cauza, dar activitatea utilizatorilor poate continua, fiind limitata la componentele neafectate ale sistemului.
<i>Major</i>	Impact Mediu asupra functionarii sistemului. Incidentul afectează minor funcționalitățile sistemului. Impactul asupra utilizatorilor reprezintă un inconvenient care se poate rezolva temporar prin soluții alternative ocolitoare, pentru continuarea funcționalităților.
<i>Minor</i>	Impact Minim asupra funcționării sistemului. Incidentul nu afecteaza funcționarea sistemului, putând fi tratată ca pe o eroare minoră care nu împiedică desfășurarea în bune condiții a activității utilizatorilor.

În cazul incidentelor cu nivel de prioritate „Urgent”, furnizorul va asigura asistență 24/7 până când problema va fi rezolvată. Pentru aceasta beneficiarul va furniza o persoană de contact, disponibilă pe perioada remedierii, care să furnizeze informații, să testeze soluții și să aplice soluțiile furnizate.

La sfârșitul fiecărui caz deschis, în sistemul de ticketing, din categoriile „Urgent” și „Critic”, furnizorul va efectua o analiză a cauzelor care au dus la producerea incidentului, iar concluziile vor fi regăsite în sistemul de ticketing.

ANEXĂ ESTIMĂRI

LOT	Denumire	Cantitate	Preț unitar fără TVA	Valoare estimată lei fără TVA	Valoare estimată euro fără TVA
1	Sistem informatic integrat – Platforma BigData				
1.1	Subsistem - Componenta de acces securizat în condiții de mobilitate			25.764.423,13	5.704.637,12
1.1.1	Pachet Smart Card (uSD) și middleware pentru platformele mobile	750	579,16	434.370,00	96.176,16
1.1.2	Echipament de tip Traffic Access Point (TAP) – componenta de acces securizat în condiții de mobilitate	4	68.041,66	272.166,64	60.261,86
1.1.3	Pachet - Soluție de monitorizare a utilizării resurselor de comunicare colaborativă	1	2.245.416,66	2.245.416,66	497.169,57
1.1.4	Pachet - Soluție de monitorizare tehnică a comunicațiilor, la nivel de metadată, prin mecanisme de tip NetFlow	1	1.133.708,33	1.133.708,33	251.020,35
1.1.5	Pachet - Echipamente de tip Switch Ethernet (Tip 1)	6	142.891,66	857.349,96	189.830,39
1.1.6	Pachet - Echipamente de tip Switch Ethernet (Tip 2)	3	86.225,00	258.675,00	57.274,59
1.1.7	Pachet echipamente de tip Next	1	1.792.275,00	1.792.275,00	396.837,08

	Generation IPS				
1.1.8	Pachet complete hardware de tip Dioda de Date	7	430.958,33	3.016.708,31	667.945,33
1.1.9	Pachet echipamente de tip Next Generation Firewall (Tip1)	1	1.473.925,00	1.473.925,00	326.349,53
1.1.10	Pachet echipamente de tip Next Generation Firewall (Tip 2)	1	793.500,00	793.500,00	175.693,03
1.1.11	Pachet echipamente de tip DNS Server/ DNS Firewall	1	567.366,66	567.366,66	125.623,65
1.1.12	Pachet echipamente de tip Application Delivery Controller	1	2.676.700,00	2.676.700,00	592.662,30
1.1.13	Pachet echipamente de tip Secure Web Gateway	1	1.248.166,66	1.248.166,66	276.363,18
1.1.14	Pachet - Echipamente de tip Gateway WS/ API	2	907.012,50	1.814.025,00	401.652,87
1.1.15	Pachet – Soluție de asigurare de servicii criptografice centralizate	3	136.091,66	408.274,98	90.398,32
1.1.16	Componenta de tip server (Tip 1)	12	162.133,33	1.945.599,96	430.785,57
1.1.17	Componenta de tip server (Tip 2)	4	160.979,16	643.916,64	142.572,99
1.1.18	Componenta de tip server (Tip 3)	4	138.412,50	553.650,00	122.586,57
1.1.19	Componenta de tip server (Tip 4)	2	57.837,50	115.675,00	25.612,21
1.1.20	Licențe Suita de tip Enterprise Mobility Management (EMM)	750	1.291,66	968.745,00	214.494,95
1.1.21	Licențe Componenta de tip multi-path VPN pentru terminale mobile	750	612,50	459.375,00	101.712,65
1.1.22	Pachet - Licențe Platforma de virtualizare - componenta de acces securizat în condiții de mobilitate	20	42.537,50	850.750,00	188.369,05
1.1.23	Servicii de instalare și configurare infrastructură componentă acces în	1	1.234.083,33	1.234.083,33	273.244,92

	condiții de mobilitate				
1.2	Subsistem Big Data			85.628.332,73	18.959.421,82
1.2.1	Pachet șasie servere mediu producție– platforma Big Data	1	472.441,66	472.441,66	104.605,81
1.2.2	Pachet șasie servere mediu testare/ dezvoltare– platforma Big Data	1	156.483,33	156.483,33	34.647,80
1.2.3	Servere blade pentru mediul de producție (config. A) – platforma Big Data	16	108.683,33	1.738.933,28	385.026,41
1.2.4	Servere blade pentru mediu testare/ dezvoltare (config. A) – platforma Big Data	4	108.866,66	435.466,64	96.418,97
1.2.5	Servere blade pentru mediul de producție (config. B) – platforma Big Data	8	59.541,66	476.333,28	105.467,47
1.2.6	Servere blade pentru mediu testare/ dezvoltare (config. B) – platforma Big Data	2	59.875,00	119.750,00	26.514,48
1.2.7	Pachet Storage de mare performanță– platforma Big Data	1	12.451.875,00	12.451.875,00	2.757.035,47
1.2.8	Pachet Storage de uz general pentru mediul de producție– platforma Big Data	1	1.746.391,66	1.746.391,66	386.677,81
1.2.9	Pachet Storage de uz general pentru mediul de testare/ dezvoltare– platforma Big Data	1	1.111.191,66	1.111.191,66	246.034,82
1.2.10	Pachet Interconectare privată (top-of-rack) – platforma Big Data	4	459.291,66	1.837.166,64	406.776,78
1.2.11	LAN Fabric– platforma Big Data	2	136.083,33	272.166,66	60.261,86
1.2.12	Pachet platformă de backup– platforma Big Data	1	613.058,33	613.058,33	135.740,49
1.2.13	Pachet licențe - platformă Big Data	1	25.901.025,00	25.901.025,00	5.734.882,87
1.2.14	Pachet licențe sistem monitorizare–	1	1.319.466,66	1.319.466,66	292.150,09

	platforma Big Data				
1.2.15	Pachet licențe modul Face recognition – pentru 3.000.000 de subiecți– platforma Big Data	1	2.279.666,66	2.279.666,66	504.753,05
1.2.16	Licențe Platformă de virtualizare – platforma Big Data	30	42.558,33	1.276.749,90	282.691,94
1.2.17	Licențe Sistem de operare – platforma Big Data	40	4.066,66	162.666,40	36.016,83
1.2.18	Servicii de instalare și configurare infrastructură platformă Big Data	1	961.675,00	961.675,00	212.929,55
1.2.19	Servicii de implementare platformă Big Data	1	28.684.666,66	28.684.666,66	6.351.223,69
1.2.20	Servicii de implementare modul Face Recognition – platforma Big Data	1	1.215.783,33	1.215.783,33	269.193,01
1.2.21	Servicii de implementare sistem monitorizare – platforma Big Data	1	90.766,66	90.766,66	20.097,12
1.2.22	Servicii de integrare cu portalul și acces management – platforma Big Data	1	217.741,66	217.741,66	48.211,33
1.2.23	Servicii de implementare componenta acces în condiții de mobilitate	1	2.086.866,66	2.086.866,66	462.064,17
1.3	Servicii de instruire			2.274.999,98	503.719,77
1.3.1	Pachet cursuri utilizatori finali	1	54.433,33	54.433,33	12.052,37
1.3.2	Pachet cursuri concepute și modele teoretice pentru modulele aferente platformei Big Data	1	814.250,00	814.250,00	180.287,39
1.3.3	Cursuri concepute și modele teoretice pentru modulul de Face Recognition	1	117.941,66	117.941,66	26.114,09
1.3.4	Pachet cursuri administrare, referință, operare, și utilizare pentru modulele aferente Big Data	1	70.766,66	70.766,66	15.668,82

1.3.5	Cursuri administrare, referință, operare și utilizare pentru modulul de Face Recognition	1	9.075,00	9.075,00	2.009,34
1.3.6	Cursuri administrare, referință, operare și utilizare pentru aplicațiile componentei de acces în condiții de mobilitate	1	9.075,00	9.075,00	2.009,34
1.3.7	Pachet - Cursuri administrare, referință, operare și utilizare pentru infrastructura componentei de acces în condiții de mobilitate	1	889.100,00	889.100,00	196.860,34
1.3.8	Pachet cursuri tehnologii	1	238.583,33	238.583,33	52.825,99
1.3.9	Pachet cursuri management	1	71.775,00	71.775,00	15.892,09
TOTAL LOT I				113.667.755,84	25.167.778,71

LOTUL II – Interconectare rețele LAN și SAN

1. SAN Fabric (2 buc.)

Rol și context

- la acest nivel se va asigura creșterea capacității de procesare și a numărului de porturi disponibil pentru interconectarea locală, în rețeaua SAN existentă (aflată în exploatare), a echipamentelor de tip șasiu de servere “blade” cu sistemele de stocare din infrastructura platformei Big Data.

Configurație și dimensionare

2x bucăți de upgrade, integrate hardware/software

- fiecare bucată va include cel puțin 1x componentă de tip cartelă (linecard) de upgrade compatibilă cu echipamentele switch SAN existente, de tip Cisco MDS 9706;
- fiecare cartelă (linecard) de upgrade va dispune de 48 de porturi care suportă echipare 16Gbps FC și va fi echipată cu cel puțin 24 transceivere de tip SFP+, cu transceiver optic de short-range, pentru comunicare FC 8/16Gbps;
- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

2. Interconectare LAN existent (2 pachete)

Rol și context

- la nivelul acestui livrabil se va asigura completarea configurației rețelei locale existentă (aflată în exploatare), pentru a putea prelua conexiunile de uplink de la nivelul mediului de rețea locală LAN (parte a infrastructurii platformei Big Data) și pentru a deservi accesul la sursele de date existente pentru serviciile de aplicație ale componentelor funcționale ale platformei Big Data.

Cerințe funcționale și specificații tehnice

- completarea configurației rețelei existente se va realiza prin două complete de upgrade, integrate hardware/software, care vor asigura nivelul de agregare (spine) în arhitectură de tip Clos (leaf and spine), pentru resurse de acces (leaf) existente, aflate în exploatare;
- fiecare complet de upgrade va respecta următoarele cerințe minime obligatorii:
 - să fie un echipament de tip switch modular redundant, cu cel puțin 4 sloturi pentru module (linecard) de interfață și să suporte module de tip line-card cu porturi de 10Gbps, 40Gbps și 100Gbps;
 - să ofere o arhitectură internă scalabilă de tip "fabric switching" și să aibă instalate module de tip switch-fabric care să ofere o capacitate cumulată de comutare de cel puțin 1.9 Tbps per slot, în ambele direcții;
 - să aibă instalate module de alimentare și ventilație redundante instalate, cu protecție de sursă și linie de alimentare, care să asigure posibilitatea populării tuturor sloturilor din șasiu cu module de interfață;
 - să suporte protocoalele de management uzuale, respectiv cel puțin OpenFlow, Netconf, VXLAN și OpFlex, și să suporte instalarea de module de control echipate cu procesoare multi-core;
 - să poată folosi module (de tip line-card) existente în rețeaua beneficiarului, care dispun, fiecare, de câte 36 porturi 40Gbps Ethernet cu interfață QSFP;
- cele două complete de upgrade vor putea fi administrate, ca un singur echipament logic, prin intermediul protocolului OpFlex (sau echivalent).

Configurație și dimensionare

1 2x pachete de upgrade, integrate hardware/software

- fiecare pachet va include cel puțin 1x componentă de tip șasiu Cisco Nexus 9504, compatibilă cu echipamentele de control existente, de tip Cisco APIC (APIC-CLUSTER-M1), precum și cu linecard-urile existente, de tip Nexus 9500 ACI Spine linecard (N9K-X9736PQ);
- în configurația necesară, fiecare șasiu va fi echipat cel puțin cu 1 modul de tip supervisor, 6 module de tip fabric și 3 surse de alimentare;

- vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN.

3. Criterii de acceptanță

Acceptanța finală a lotului II se va realiza în baza unui protocol de acceptanță semnat atât de către furnizor cât și de beneficiar la finalizarea livrării și instalării, respectiv configurării tuturor componentelor lotului II, care vor include rezultatele unor teste funcționale și de performanță, agreeate de beneficiar cu furnizorul, în scopul verificării îndeplinirii de către echipamentele upgradeate a criteriilor menționate anterior.

De asemenea, furnizorul va pune la dispoziție următoarele livrabile, în mod electronic:

- manual de instalare, configurare pentru componentele lotului II.
- documentația tehnică a componentelor hardware/software.

4. Garanție și suport tehnic

Pentru componentele menționate în secțiunile 1 și 2, din cadrul lotului II, furnizorul va garanta menținerea tuturor funcționalităților prin asigurarea garanției și suportului tehnic, a actualizărilor firmware și software, la un nivel de performanță cel puțin la fel cu cel de la punerea în funcțiune (de la acceptanță) pe toată perioada de viață declarată de acesta. Această perioadă nu poate fi mai mică decât perioada considerată ca referință de achizitor privind exploatarea la un nivel de eficiență de 100% a echipamentelor și produselor software din cadrul lotului, definită în cadrul proiectului. Garanția tehnică va începe de la data semnării procesului verbal de recepție cantitativă și calitativă.

În perioada de garanție și suport tehnic, furnizorul se obligă să asigure constatarea unei defecțiuni cel târziu a doua zi lucrătoare, iar remedierea în cel mult 7 zile lucrătoare de la data reclamării acesteia de către beneficiar.

Serviciile de garanție hardware vor include serviciu de tip RMA pentru echipamentele sau componentele defecte, și suport tehnic autorizat 8/5, inclusiv înlocuirea și reconfigurarea sistemului pentru reluarea serviciului, și timp de răspuns de tip "Next Business Day" (NBD).

ANEXĂ ESTIMĂRI

LOT	Denumire produs	Cant.	Preț unitar fără TVA	Valoare estimată lei fără TVA	Valoare estimată euro fără TVA
2	Interconectare rețele LAN și SAN				
2.1	SAN Fabric	2	226.583,33	453.166,66	100.338,02
2.2	Pachet - Interconectare LAN existent	2	170.108,33	340.216,66	75.329,17
TOTAL LOT II				793.383,32	175.667,19

Anexa 1 - Specificații sesiune demonstrativă

1. Considerații generale

Prezentul document reprezintă o anexă a caietului de sarcini, pusă la dispoziție de către beneficiar cu scopul de a defini și cuantifica subsetul de funcționalități aferente platformei Big Data, extrase dintre cele descrise în caietul de sarcini, din care soluția propusă de ofertant trebuie să cuprindă *"out-of-the-box"* cel puțin **80%**. Pentru referențiere colectivă, această mulțime va fi numită în continuare *"pool" de funcționalități*.

Nivelul procentual până la care soluția propusă de către ofertant cuprinde *"out-of-the-box"* *"pool"-ul de funcționalități*, va fi determinat în mod obiectiv, pentru fiecare ofertă depusă, prin intermediul unei *grile de punctaj* pe care beneficiarul o pune la dispoziția ofertantului prin intermediul prezentului document. *Grila de punctaj* însumează **200** puncte și cuprinde:

- un *scenariu de bază* în cadrul căruia sunt enumerate un set de funcționalități cuantificate *colectiv*, cantitativ cu **100** puncte, respectiv procentual cu **50%** pondere în ansamblul *"pool"-ului*;

Notă: - soluția propusă trebuie să cuprindă *"out-of-the-box"* toate funcționalitățile enumerate în cadrul *scenariului de bază*, lipsa uneia conducând la declararea ofertantului drept *respins*;

- un *scenariu extins* în cadrul căruia sunt enumerate un set de funcționalități cuantificate *colectiv*, cantitativ cu **100** puncte, respectiv procentual cu **50%** pondere în ansamblul *"pool"-ului*, și independent prin intermediul unei valori ce reprezintă numărul de puncte în baza cărora poate fi calculată ponderea fiecăreia în ansamblul *"pool"-ului*;

Notă: - soluția propusă trebuie să cuprindă *"out-of-the-box"* un subset minim de funcționalități - *libertatea de alegere fiind lăsată la îndemâna ofertantului* - ce însumează cantitativ cel puțin **60** puncte, respectiv procentual cel puțin **30%** în ansamblul *"pool"-ului*, orice valoare sub acest prag cantitativ, respectiv procentual, conducând la declararea ofertantului drept *respins*;

Ofertantul are obligativitatea de a pune la dispoziția beneficiarului, ca parte integrantă a ofertei:

- o *grilă de evaluare*, construită plecând de la *grila de punctaj*, prin evidențierea/marcarea funcționalităților implementate *"out-of-the-box"* de către soluția proprie;

- o *înregistrare audio-video*, pe un suport optic, a unei *sesiuni demonstrative*, prin care ofertantul prezintă capabilitățile soluției proprii, aceleași evidențiate în *grila de evaluare*, astfel încât să facă dovada atingerii pragului de **80%** impus;
- o descriere a infrastructurii suport utilizată pentru pregătirea *sesiunii demonstrative înregistrate*;

Ca un pas în cadrul etapei de evaluare, beneficiarul va analiza *grila de evaluare*, mai sus menționată, *înregistrarea sesiunii demonstrative* și concordanța dintre cele două. Dacă beneficiarul constată faptul că ponderea asociată funcționalităților evidențiate/marcate nu atinge pragul de **80%** impus, ofertantul va fi declarat *respins*. După evaluarea ofertelor și stabilirea câștigătorului, acesta va organiza într-o locație proprie, o sesiune demonstrativă cu rol de "*proof of concept*", în care va realiza o prezentare "*live*" a capabilităților soluției proprii, aceleași evidențiate în *grila de evaluare*, respectiv prezentate în *sesiunea demonstrativă înregistrată*, anterior puse la dispoziție, astfel încât să facă dovada atingerii pragului de **80%** impus. Sesiunea demonstrativă "*live*" se va desfășura sub forma unei interacțiuni în care câștigătorul va răspunde oricărei solicitări venită din partea beneficiarului, această sesiune fiind, la rândul său, înregistrată audio-video de către câștigător și predată beneficiarului pe un suport optic. În situația în care sesiunea demonstrativă "*live*" nu acoperă capabilitățile evidențiate în *grila de evaluare*, respectiv prezentate în *sesiunea demonstrativă înregistrată*, câștigătorul va fi declarat *respins*.

Atât *sesiunea demonstrativă înregistrată* cât și *sesiunea demonstrativă "live"* vor fi realizate utilizând o infrastructură echivalentă celei descrise în cadrul caietului de sarcini (mediu virtualizat). Deși domeniul specific datelor utilizate pentru construirea scenariilor de lucru va rămâne la latitudinea ofertantului, acesta va asigura cel puțin următoarele:

- un volum de date construit prin *proces de achiziție* de date structurate, semi-structurate și nestructurate preluate din cel puțin:
 - 2 SGBDR-uri cu producători diferiți (ex. ORACLE, SQL Server), cu minim 20 de tabele, 100 de coloane cu diverse tipuri de date printre care, în mod obligatoriu, numeric, dată, șir de caractere, clob și blob, și care însumează cel puțin 10.000.000 de înregistrări;
 - 10 fișiere XLS ce împreună însumează minim 50 coloane și 10.000 de linii, fișiere din care cel puțin unul să aibă minim 2 foi de calcul;

- 10 fișiere XML care să cuprindă cumulativ minim 10.000 de înregistrări;
- 10 fișiere PDF și 10 fișiere DOC care să conțină cumulativ minim 100 de pagini;
- un volum de date structurate, accesibile prin intermediul unor *fluxuri de acces federativ*, salvate în SGBDR extern platformei Big Data, cu minim 5 tabele, 20 de coloane cu diverse tipuri de date printre care, în mod obligatoriu, numeric, dată, șir de caractere și care însumează cel puțin 10.000 de înregistrări;
- un model conceptual de interpretare semantică a datelor, cu cel puțin 5 entități și 5 evenimente, 30 de proprietăți și 10 relații, extrase din toate tipurile de date prezentate anterior: procese de achiziție și fluxuri de acces federativ;

Câștigătorul are obligativitatea de a implementa aceeași soluție prezentată beneficiarului în cadrul propunerii tehnice, respectiv în *sesiunea demonstrativă* (completată cu diferența de funcționalități descrise în cadrul caietului de sarcini și neabordate în sesiunea "live").

2. Scenariul de bază

Prin intermediul acestui *scenariu de bază* sunt grupate un set de funcționalități cuantificate *colectiv*, cantitativ cu **100** puncte, respectiv procentual cu **50%** pondere în ansamblul "*pool*"-ului de *funcționalități*. Soluția propusă trebuie să cuprindă "*out-of-the-box*" toate funcționalitățile prezente în cadrul acestui capitol, lipsa uneia conducând la declararea ofertantului drept *respins*. Totodată, soluția propusă trebuie să permită ofertantului să evidențieze în *grila de evaluare* și să prezinte în *sesiunea demonstrativă înregistrată*, toate funcționalitățile enumerate în continuare:

Nr. crt	Funcționalitate	Implementată "out-of-the-box" în cadrul soluției oferite
	2.1. Cerințe generale	
1	implementarea mecanismelor de internaționalizare și localizare; <i>Notă:</i> - actualizarea unor mesaje, texte, etichete, date calendaristice, timp, valori numerice sau orice alte aspecte ce țin de cultura locală, prin afișarea acestora în cel puțin două limbi;	
	2.2. Prevederi de securitate	
2	restricționarea accesului la nivel de module funcționale; <i>Notă:</i> - prezentarea unor mecanisme de autentificare și autorizare bazate pe roluri și permisiuni;	
3	restricționarea accesului la nivel de surse de date;	

4	menținerea persistenței sesiunii de lucru; <i>Notă:</i> - navigarea în și între toate modulele funcționale, precum și accesarea tuturor funcțiilor și comenzilor la care utilizatorul este autorizat să dețină acces, fără a fi necesară deconectarea și reconectarea acestuia;	
3.2.2.1. Modelul conceptual de interpretare semantică a datelor		
5	prezentarea modului de definire / configurare a modelului conceptual de interpretare semantică a datelor sub formă de obiecte, proprietăți și relații;	
3.2.2.2.1. Mapperi		
6	prezentarea modului de definire / configurare a unor "mapperi", prin soluții preponderent grafice care să nu necesite cunoștințe solide de programare;	
3.2.2.2.1.2.1. Procese de achiziție		
7	prezentarea "live" a unui proces de achiziție de date structurate;	
8	prezentarea "live" a unui proces de achiziție de date semi-structurate;	
9	prezentarea "live" a unui proces de achiziție de date nestructurate;	
10	prezentarea "live" a unor mecanisme de sincronizare a surselor de date cu depozitul de date propriu platformei Big Data; <i>Notă:</i> - propagarea oricăror modificări de date, de la sursă la destinație;	
3.2.2.2.1.2.3. Fluxuri de acces federativ		
11	prezentarea "live" a unui flux de acces federativ;	
3.2.2.3.2.1. Interfața cu utilizatorul		
12	interfață grafică în tehnologie web, cu acces securizat;	
13	interfață grafică ce respectă standarde de compatibilitate (progressive enhancement & cross browser compatibility); <i>Notă:</i> - redarea corectă și uniformă a interfeței grafice, pe cel puțin două navigatoare web consacrate, printre care să se regăsească în mod obligatoriu Internet Explorer 9+;	
14	interfață grafică ce respectă standarde de adaptativitate (responsive user interface & adaptive layout); <i>Notă:</i> - redarea corectă și uniformă a interfeței grafice pe un dispozitiv de tip desktop / laptop și unul de tip mobil (smartphone sau tabletă);	
3.2.2.3.2.1.1. Enterprise search		
15	restricționarea volumului de date supus filtrării, prin selectarea surselor de date de către utilizator ("source-restricted search");	
3.2.2.3.2.1.1.1. Full text search		
16	introducerea unuia sau mai multor cuvinte cheie într-un câmp unic de căutare;	
17	regăsirea exactă a frazei introduse ("phrase search"), prin marcarea cuvintelor (utilizarea, spre exemplu, a caracterului "quote") ce trebuie să se regăsească obligatoriu, ca formă și ordine, în rezultatele generate;	
18	independență față de modul de scriere: interpretarea literelor mari și mici ca fiind la fel ("case insensitive") și aducerea diacriticelor la forma de bază;	
19	restricționarea volumului de date supus filtrării, în funcție de sensul pe care cuvintele îl au pentru utilizator; în acest sens, utilizatorul trebuie să aibă posibilitatea selectării obiectelor / proprietăților definite în modelul conceptual ("field-restricted search");	
3.2.2.3.2.1.1.2. Spatial search		
20	regăsirea obiectelor care au atașate informații geospațiale, fie prin utilizarea unor mecanisme de tip "geocoding" și "reverse-geocoding", fie folosind direct perechea latitudine-longitudine.	

	3.2.2.3.2.1.1.5. Vizualizare și rafinare	
21	afișarea rezultatelor sub formă de <i>"GRID"</i> și / sau <i>"LIST"</i> , în care fiecare înregistrare este reprezentată în mod distinct;	
22	afișarea paginată a rezultatelor, cu posibilitatea de navigare între pagini și de modificare a numărului de înregistrări pe pagină;	
23	vizibilitatea implicită, textuală și / sau grafică, a unui set de proprietăți sugestive pentru fiecare înregistrare din rezultat;	
24	afișarea celei mai recente imagini, în situația în care obiectul returnat are asociate imagini (ex: poza entității de tip <i>persoană</i>);	
25	ordonarea crescătoare și descrescătoare, automată și / sau manuală, simplă și multiplă a rezultatelor în funcție de criterii diverse, printre care trebuie să se regăsească cel puțin una din următoarele posibilități: – sortarea înregistrărilor în funcție de ordinea alfabetică a proprietăților obiectelor returnate; – sortarea înregistrărilor în funcție de diverse criterii de relevanță;	
26	exportul rezultatelor în cel puțin două din următoarele formate: PDF, DOC, HTML, XLS și XML;	
27	vizualizarea tuturor detaliilor (<i>"detail view"</i>) asociate fiecărei înregistrări din rezultat, în funcție de tipul de obiect selectat: document, entitate sau eveniment;	
28	navigarea în adâncime, printr-o parcurgere ierarhică nivel cu nivel a rezultatelor, cu scopul de a obține detalii suplimentare, cu granularitate din ce în ce mai fină;	
	3.2.2.3.2.1.3.1. Link analysis	
29	afișarea obiectelor (entități, evenimente și documente), proprietăților și relațiilor, sub o formă vizuală de tip graf;	
30	funcționalități de tip <i>"zoom in"</i> și <i>"zoom out"</i> , prin mecanisme de tip <i>"mouse scroll"</i> , <i>"slider"</i> sau alegerea exactă a valorii de <i>"zoom"</i> ;	
31	agățarea nodurilor și re poziționarea acestora în cadrul grafului (<i>"drag and drop"</i>);	
32	eliminarea din graf a unui nod sau a unui grup de noduri;	
33	asigurarea a cel puțin 2 forme de vizualizare a grafului, precum: distanțe egale (<i>"auto-layout"</i>), circular, grupat, tabelar, ierarhic, număr de legături / densitatea nodului, timeline;	
34	salvarea grafului în cel puțin două din următoarele formate: JPG, PNG, GIF, PDF, DOC[X], HTML;	
35	accesul la funcționalitățile solicitate, prin intermediul unui meniu contextual;	
	3.2.2.3.2.1.3.2. Spatial analysis	
36	afișarea obiectelor, proprietăților și relațiilor, prin localizarea acestora pe hartă;	
37	asigurarea unor hărți de fundal ca, spre exemplu: <i>"street map"</i> și <i>"satellite"</i> ;	
38	asigurarea a cel puțin 3 starturi (<i>"layer"</i> -e), precum: state, regiuni administrative, localități, drumuri, rețele de cale ferată, rețele de transport în comun, râuri, curbe de nivel, puncte de interes, clădiri, adrese, etc.;	
39	funcționalități avansate de navigare pe hartă: <i>"zoom in"</i> , <i>"zoom out"</i> , <i>"mouse scroll zoom"</i> , <i>"slider zoom"</i> , <i>"zoom to area"</i> , <i>"double-click zoom"</i> , <i>"keyboard navigation"</i> , <i>"drag"</i> , <i>"rotate"</i> și busolă;	
40	funcționalități de tip <i>"geocoding"</i> și <i>"reverse-geocoding"</i> (translatarea bidirecțională între o adresă / locație și coordonate geospațiale);	
41	mecanisme de tip <i>"heatmap"</i> și / sau <i>"clustering nearby markers"</i> , actualizate în același timp cu modificarea scării de reprezentare a hărții;	
42	salvarea hărții împreună cu toate elementele grafice reprezentate pe aceasta, în cel puțin două din următoarele	

	formate: JPG, PNG, GIF, PDF, DOC[X], HTML;	
43	selectarea / deselectarea " <i>layer</i> "-elor;	
	3.2.2.3.2.1.3.3. Semantic analytics	
44	extragerea automată a obiectelor, proprietăților și relațiilor din conținut nestructurat;	
45	afișarea datelor în diagrame de relație, folosind, spre exemplu, soluția " <i>link analysis</i> ";	
	3.2.2.3.2.1.4. Early warning	
46	construirea unui " <i>watchlist</i> " prin mecanisme de tip " <i>add to watchlist</i> ", existente la nivelul interfețelor de regăsire, vizualizare și analiză	
47	transmiterea notificărilor sub formă de mesaje la nivelul interfeței grafice, cu evidențiere vizuală și / sau sonoră	
	3.2.2.3.2.1.5. Enrichment	
	3.2.2.3.2.1.5.1. Adăugare sursă de date privată	
48	încărcarea grafică, extragerea și indexarea conținutului unor fișiere nestructurate, în format PDF, HTML, HTM, XHTML, PPT, PPTX, DOC, DOCX, RTF și TXT;	
49	încărcarea grafică a unor fișiere semi-structurate, în format XLS, XLSX, CSV, XML, JSON și TXT (valori separate prin delimitatori) și structurarea conținutului acestora pe baza modelului conceptual de interpretare semantică a datelor sub formă de <i>obiecte, proprietăți și relații</i> , prin intermediul unor interfețe grafice ce permit: – identificarea și prezentarea elementelor existente în fișier; – maparea asistată ("<i>wizard</i>") a elementelor extrase, cu obiectele, proprietățile și relațiile definite în modelul de date conceptual; – rularea procesului de încărcare;	
	3.2.2.3.2.1.6. Spațiu privat și colaborare	
50	extragerea rezultatului analizei sub formă de rapoarte concise, dar cuprinzătoare, pe baza unor template-uri specifice;	

Legendă:

- în cadrul *grilei de evaluare*, în coloana **Implementată "out-of-the-box"** în cadrul soluției oferite, vor fi marcate de către ofertant cu simbolul "**x**", doar acele funcționalități implementate "*out-of-the-box*" de către soluția proprie;

Notă: - tabelul trebuie să fie parte integrantă a *grilei de evaluare* din cadrul ofertei depuse;

3. Scenariul extins

Prin intermediul acestui *scenariu extins* sunt grupate un set de funcționalități cuantificate *colectiv*, cantitativ cu **100** puncte, respectiv procentual cu **50%** pondere în ansamblul "*pool*"-ului de funcționalități. Suplimentar, fiecare funcționalitate prezentă în cadrul acestui capitol va fi cuantificată și în mod independent, prin intermediul unei valori ce reprezintă numărul de puncte în baza cărora poate fi calculată ponderea fiecăreia în ansamblul "*pool*"-ului de funcționalități. Soluția propusă trebuie să cuprindă

"out-of-the-box" un subset minim de funcționalități, din cele definite mai jos - *libertatea de alegere fiind lăsată la îndemâna ofertantului* - ce însumează cantitativ cel puțin **60** puncte, respectiv procentual cel puțin **30%** în ansamblul "pool"-ului de funcționalități, orice valoare sub acest prag cantitativ, respectiv procentual, conducând la declararea ofertantului drept *respins*. Soluția propusă trebuie să îi permită ofertantului să evidențieze în *grila de evaluare* și să prezinte în *sesiunea demonstrativă înregistrată*, acel subset minim de funcționalități ce însumează cantitativ cel puțin **60** puncte, respectiv procentual cel puțin **30%** în ansamblul "pool"-ului, funcționalități alese dintre cele enumerate în continuare:

Nr. crt	Funcționalitate	Punctaj	Implementată "out-of-the-box" în cadrul soluției oferite
	2.1. Cerințe generale		
1	evitarea percepției de ecran înghețat; <i>Notă:</i> - furnizarea unui răspuns intermediar imediat, ulterior fiecărei interacțiuni a utilizatorului cu interfața grafică, sub forma unui text sau simbol grafic determinat sau nedeterminat (progress bar, progress wheel);	1	
2	feedback către utilizator, pentru toate interacțiunile finalizate cu eșec; <i>Notă:</i> - emiterea unui mesaj relevant de eroare însoțit de instrucțiuni clare privind modul de continuare;	1	
	3.1.1. Cerințe funcționale aferente platformei Big Data		
3	Identificarea / vizualizarea sursei de date aferentă fiecărei informații accesibilă utilizatorului final la nivelul platformei Big Data, indiferent de forma de prezentare a acestora în cadrul soluțiilor de regăsire, vizualizare și / sau analiză;	2	
	3.2.2.3.2.1.1. Enterprise search		
	3.2.2.3.2.1.1.1. Full text search		
4	regăsirea termenilor introduși prin specificarea numărului maxim de cuvinte intermediare între aceștia, cu sau fără restricționari cu privire la păstrarea ordinii de introducere (" <i>proximity search</i> ");	2	
5	construirea unor clauze condiționale complexe, prin utilizarea parantezelor și a unor operatori de tip <i>boolean</i> precum AND, OR sau NOT (" <i>boolean queries</i> "), aplicați între termeni sau grupări de termeni (" <i>grouping terms</i> ");	1	
6	utilizarea unor caractere speciale (" <i>wildcard search</i> ") ca înlocuitor al unuia (spre exemplu, caracterului " <i>question mark</i> ") sau mai multor caractere (spre exemplu, caracterului " <i>asterisk</i> ");	2	
7	specificarea unui interval de valori inclusiv sau exclusiv (" <i>range search</i> "), între care să se regăsească valoarea unei proprietăți definită în modelul conceptual: dată calendaristică, proprietate numerică, etc.;	2	
8	mecanisme de asimilare fonetică (" <i>sounds like</i> ") - regăsiri după variante fonetice ale termenilor căutați;	2	
9	mecanisme de asimilare semantică (" <i>conceptual search</i> ") - regăsiri după sinonime ale termenilor căutați, ținând cont și de polisemia cuvintelor în contextul frazei introduse;	2	
10	regăsirea cuvintelor introduse folosind variații de scriere ale acestora (" <i>fuzzy search</i> ");	3	

11	utilizarea unor sugestii de tip <i>"did you mean"</i> sau corecții ortografice;	2	
12	utilizarea unei funcții de tip <i>"type-ahead"</i> ;	2	
13	utilizarea în timpul procesului de regăsire a unor cuvinte cheie (<i>"keywords"</i>) asociate textelor nestructurate automat la indexare, sau manual prin etichetarea conținutului (<i>"tagging"</i>) de către utilizatori;	2	
14	realizarea unor regăsiri succesive care, prin introducerea unor noi termeni, să filtreze doar setul de rezultate anterior generat;	1	
3.2.2.3.2.1.1.2. Spatial search			
15	extinderea soluției <i>"full text search"</i> , prin restricționarea setul de rezultate, funcție de metadatele geospațiale, la o anumită zonă geografică, folosind diverse instrumente geometrice pentru definirea unor perimetre de proximitate geospațială, fie utilizând un cerc, prin selectarea centrului și a razei pe o hartă, fie utilizând un poligon, prin selectarea unor puncte pe hartă.	3	
3.2.2.3.2.1.1.3. Query Builder			
16	definirea grafică a unor condiții de filtrare de forma <i>proprietate obiect - operator relațional - valoare</i> , unde operatorii relaționali sunt dependenți de tipul proprietății (<i>text, numeric, dată calendaritică, listă de valori, etc.</i>) și pot fi de forma: <i>mai mic, mai mic sau egal, mai mare, mai mare sau egal, egal - "case sensitive", egal - "case insensitive", conține, între, "is null", etc. și orice negație a acestora</i> ;	3	
17	definirea grafică a unor condiții de filtrare de forma <i>obiect - relație - obiect</i> ;	2	
18	înlănțuirea condițiilor prin intermediul unor operatori de tip <i>boolean</i> precum AND, OR sau NOT;	1	
19	gruparea condițiilor, utilizând paranteze, sub forma unor clauze imbricate și înlănțuirea grupurilor de condiții prin intermediul operatorilor de tip <i>boolean</i>	2	
3.2.2.3.2.1.1.5. Vizualizare și rafinare			
20	afișarea evoluției în timp a procesului de regăsire, printr-un feedback procentual sau cantitativ cu privire la volumul de date scanat, respectiv la numărul de înregistrări regăsite;	2	
21	transmiterea uneia sau mai multor înregistrări către diverse interfețe de analiză avansată precum <i>"Link analysis"</i> și <i>"Spatial analysis"</i> , cu vizualizarea concomitentă a acestora atât în interfețele de analiză cât și în interfața de vizualizare și rafinare;	3	
22	clasificarea rezultatelor după mai multe dimensiuni și metrici, funcție de care să asigure rafinarea acestora prin aplicarea unor filtre succesive;	2	
3.2.2.3.2.1.3.1. Link analysis			
23	afișarea proprietăților unui obiect, sub formă de noduri / etichete în graf;	1	
24	etichetarea oricărui nod sau legătură din graf;	1	
25	evidențierea nodurilor / legăturilor pentru care valorile proprietăților respectă un filtru introdus de utilizator (prin utilizarea, spre exemplu, a unei palete de culori, dimensiuni și / sau fonturi);	1	
26	vizualizarea temporală a evenimentelor / relațiilor, sub formă de <i>"timeline"</i> ;	2	
27	animarea vizualizării de tip <i>"timeline"</i> , cu funcționalități de stop, start (<i>"play"</i>), pauză (<i>"pause"</i>) și reluare (<i>"resume"</i>), ce permite evidențierea evoluției în timp a grafului prin mecanisme de tip <i>"hide" - "show"</i> și / sau <i>"fade-in" - "fade-out"</i> ;	3	
28	păstrarea în graf doar a acelor noduri pentru care există evenimente / relații într-un anumit interval de timp, prin funcționalități de tip restrângere, respectiv glisare pe <i>"timeline"</i> ;	2	

29	extinderea legăturilor asociate unui nod, pe minim 2 niveluri de adâncime, prin intermediul unei singure operații de regăsire (" <i>search around</i> ");	3	
30	evidențierea drumurilor existente între două noduri selectate de utilizator, relaționate direct sau indirect în graf (" <i>show path</i> ");	2	
31	evidențierea celui mai scurt drum existent între două noduri selectate de utilizator, relaționate direct sau indirect în graf (" <i>show shortest path</i> ");	1	
32	relaționarea unui nod nou introdus cu graful existent;	1	
33	customizarea modului de reprezentare a obiectelor, proprietăților și relațiilor, respectiv etichetelor definite, prin setarea unor pictograme intuitive și prin modificări de culoare, dimensiune și / sau font;	1	
34	exportul grafului într-un format ce permite importul ulterior;	1	
35	vizualizarea tuturor detaliilor (" <i>detail view</i> ") asociate unui nod, în funcție de tipul de obiect reprezentat: document, entitate sau eveniment;	1	
36	afișarea pe hartă a informațiilor geospațiale asociate obiectelor / relațiilor prezente în graf, eventual prin transmiterea acestora către soluția " <i>spatial analysis</i> ";	2	
3.2.2.3.2.1.3.2. Spatial analysis			
37	importul și utilizarea unor noi straturi;	1	
38	importul unor fișiere ale căror formate pot reprezenta date geospațiale, ca spre exemplu: <i>KML</i> , <i>KMZ</i> , <i>GPX</i> , <i>SHP</i> ;	1	
39	localizarea pe hartă a tuturor datelor geospațiale specifice unui obiect (ex.: - domiciliul, reședința);	2	
40	vizualizarea obiectelor ce au legătură cu locația sau perimetrul selectat de către utilizator (ex.: - firme care au sediul social / persoane care locuiesc la o anumită adresă);	2	
41	selectarea / eliminarea de pe hartă a unuia sau mai multor obiecte;	1	
42	customizarea modului de reprezentare a obiectelor, proprietăților și relațiilor, respectiv etichetelor definite, prin setarea unor pictograme intuitive și prin modificări de culoare, dimensiune și / sau font;	1	
43	vizualizarea tuturor detaliilor (" <i>detail view</i> ") asociate unui obiect reprezentat pe hartă;	1	
44	accesul la funcționalitățile solicitate, prin intermediul unui meniu contextual;	1	
45	selectarea / deselectarea " <i>layer</i> "-elor;	1	
3.2.2.3.2.1.3.3. Semantic analytics			
46	explorarea " <i>top down</i> " a datelor, folosind diverse forme de vizualizare / perspective interdependente;	1	
47	filtrarea datelor prezentate într-o formă de vizualizare să se propage în mod automat și la nivelul celorlalte forme de vizualizare (" <i>refresh</i> ");	2	
48	dispunerea pe hartă a datelor geospațiale, folosind, spre exemplu, soluția " <i>spatial analysis</i> ";	3	
49	funcții de vizualizare și raportare similare celor din domeniul aplicațiilor de tip " <i>business intelligence</i> ";	1	
50	gruparea documentelor în funcție de topic, prin folosirea unor algoritmi avansați de clasificare bazați, spre exemplu, pe dicționare de topic și frecvență de cuvinte;	1	
51	sumarizarea conținutului nestructurat;	3	
3.2.2.3.2.1.3.5. Behavioral analytics			
52	definirea grafică, arborescentă a întrebărilor sub formă unor condiții de filtrare, folosind orice obiect, proprietate sau relație definită în modelul de date conceptual; <i>sau</i>	3	

	definirea programatică a întrebărilor sub formă de <i>propoziții parametrizate</i> , în situațiile în care acestea au nivel ridicat de complexitate și nu pot fi definite grafic de utilizator;		
53	execuția întrebărilor (<i>propoziție parametrizată personalizată sau condiție de filtrare grafică</i>);	1	
54	vizualizarea rezultatului execuției întrebărilor, în conformitate cu cerințele definite în capitolul <i>Vizualizare și rafinare</i> , sub formă de listă de entități care respectă condițiile de filtrare;1	1	
	3.2.2.3.2.1.4. Early warning		
55	transmiterea notificărilor sub formă de e-mail, fără ca mesajul să conțină informații sensibile;	1	
	3.2.2.3.2.1.5. Enrichment		
	3.2.2.3.2.1.5.2. Etichetare conținut nestructurat		
56	adăugarea unor marcaje de tip legătură, unor părți din document, cu scopul de a crea noi obiecte, proprietăți și / sau relații, respectiv de a actualiza proprietățile / relațiile obiectelor existente	3	
	3.2.2.3.2.1.6. Spațiu privat și colaborare		
57	gruparea proceselor de analiză în investigații;	1	
58	afișarea tuturor datelor aferente unei investigații;	1	
59	configurarea modului în care sunt afișate elementele în spațiul privat;	1	
60	salvarea și distribuirea rezultatului analizei, <i>"watchlist"</i> -ului și / sau a notificărilor, însoțite eventual și de observații / concluzii proprii, unui utilizator sau grup de utilizatori, prin utilizarea mecanismelor de salvare / export și / sau prin procese de colaborare;	1	

Legendă:

- În cadrul *grilei de evaluare*, în coloana **Implementată "out-of-the-box"** în cadrul soluției oferite, vor fi marcate de către ofertant cu simbolul **"x"**, doar acele funcționalități implementate *"out-of-the-box"* de către soluția proprie;

Notă: - tabelul trebuie să fie parte integrantă a *grilei de evaluare* din cadrul ofertei depuse;

Anexa 2 - Diagrama Gantt

Activitate	2016			2017												2018					
	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15	L16	L17	L18	L19	L20	L21
	10	11	12	01	02	03	04	05	06	07	08	09	10	11	12	01	02	03	04	05	06
A3 Implementare infrastructura (hardware și licențe)																					
A3.1 Implementare infrastructura platforma Big Data - mediul de dezvoltare-testare																					
A3.1.1 Livrare si receptie echipamente si licențe																					
A3.1.2 Analiza si proiectare																					
A3.1.3 Implementare de baza																					
A3.1.4 Configurare si documentare																					
A3.1.5 Testare si punere in functiune																					
A3.2 Implementare infrastructura platforma Big Data - mediul de productie																					
A3.2.1 Livrare si receptie echipamente si licențe																					
A3.2.2 Analiza si proiectare																					
A3.2.3 Implementare de baza																					
A3.2.4 Configurare, integrare cu infrastructura componentei de acces mobil si documentare																					
A3.2.5 Testare si punere in functiune																					
A3.3 Implementare infrastructura componentă de acces securizat in conditii de mobilitate																					
A3.3.1 Livrare si receptie echipamente si licențe																					
A3.3.2 Analiza si proiectare																					
A3.3.3 Implementare de baza																					
A3.3.4 Configurare, integrare cu infrastructura existenta si documentare																					
A3.3.5 Testare si punere in functiune																					
A3.3.6 Acceptanta																					
A3.4 Interconectarea LAN și SAN cu rețeaua existentă																					
A3.4.1 Livrare, receptie si instalare echipamente																					
A3.4.2 Configurare echipamente																					
A3.4.3 Acceptanta interconectare																					
A4 Analiză funcțională																					
A4.1 Analiză funcțională platforma Big Data																					
A4.1.1 Identificarea și analiza cerintelor functionale																					
A4.1.2 Elaborarea planului de implementare																					
A4.1.3 Elaborarea specificatiilor functionale																					
A4.2 Analiză funcțională componentă de acces securizat in conditii de mobilitate																					
A4.2.1 Identificarea și analiza cerintelor functionale																					
A4.2.2 Elaborarea planului de implementare																					
A4.2.3 Elaborarea specificatiilor functionale																					
A5 Implementare si dezvoltare software																					
A5.1 Implementare si dezvoltare software platforma Big Data (3 etape)																					
A5.1.1 Implementare si dezvoltare software modul Face recognition - Etapa I																					
A5.1.1.1 Configurare localizare																					
A5.1.1.2 Dezvoltare și adaptare funcționalități																					
A5.1.1.3 Integrare cu modulul de control acces, management identitati si Portal existente																					
A5.1.2 Implementare si dezvoltare software - Etapa II																					
- modul Enterprise Search																					
- integrare modul Face Recognition cu modul Enterprise Search																					
- modul Link Analysis																					
- modul Semantic Analysis																					
A5.1.2.1 Configurare localizare																					

A5.1.2.2 Dezvoltare și adaptare funcționalități																						
A5.1.2.3 Integrare cu modulul de control acces, management identitati si Portal existente																						
A5.1.3 Implementare si dezvoltare software - Etapa III - modul Spatial Analysis - modul spatiu privat si colaborare - modul Behavior Analytics - modul Early Warning - modul Enrichment																						
A5.1.3.1 Configurare localizare																						
A5.1.3.2 Dezvoltare și adaptare funcționalități																						
A5.1.3.3 Integrare cu modulul de control acces, management identitati si Portal existente																						
A5.2 Implementare si dezvoltare software componentă de acces securizat in conditii de mobilitate (Mobilitate)																						
A5.2.1 Configurare localizare																						
A5.2.2 Dezvoltare și adaptare funcționalități																						
A6 Testare funcțională și de performanță																						
A6.1 Testare funcțională și de performanță aplicații mobile punctuale																						
A6.1.1 Planificare testare																						
A6.1.2 Desfasurarea activitatii de testare functionala																						
A6.1.3 Desfasurarea activitatii de testare de performanta																						
A6.2 Testare funcțională și de performanță module din platforma Big Data implementate in Etapa I																						
A6.2.1 Planificare testare																						
A6.2.2 Desfasurarea activitatii de testare functionala																						
A6.2.3 Desfasurarea activitatii de testare de performanta																						
A6.3 Testare funcțională și de performanță module din platforma Big Data implementate in Etapa II , inclusiv versiunea adaptata pentru accesul mobil																						
A6.3.1 Planificare testare																						
A6.3.2 Desfasurarea activitatii de testare functionala																						
A6.3.3 Desfasurarea activitatii de testare de performanta																						
A6.4 Testare funcțională și de performanță module din platforma Big Data implementate in Etapa III , inclusiv versiunea adaptata pentru accesul mobil																						
A6.4.1 Planificare testare																						
A6.4.2 Desfasurarea activitatii de testare functionala																						
A6.4.3 Desfasurarea activitatii de testare de performanta																						
A7 Intrarea in productie																						
A7.1 Intrarea in productie Module Platforma Big Data Etapa I																						
A7.1.1 Asigurarea cadrului tehnic și procedural pentru accesul beneficiarilor interni și externi																						
A7.1.2 Intrare in PREPRODUCTIE și Remediere disfuncționalități																						
A7.1.3 Preluarea securității																						
A7.1.4 Intrare in PRODUCTIE																						
A7.2 Intrarea in productie Module Platforma Big Data Etapa II																						
A7.2.1 Asigurarea cadrului tehnic și procedural pentru accesul beneficiarilor interni și externi																						
A7.2.2 Intrare in PREPRODUCTIE și Remediere disfuncționalități																						
A7.2.3 Preluarea securității																						
A7.2.4 Intrare in PRODUCTIE																						
A7.3 Intrarea intregului sistem în producție și acceptanta finala																						
A7.3.1 Asigurarea cadrului tehnic și procedural pentru accesul beneficiarilor interni și externi																						
A7.3.2 Intrare in PREPRODUCTIE și Remediere disfuncționalități																						
A7.3.3 Preluarea securității																						
A7.3.4 Intrare in PRODUCTIE																						

A7.3.5 Acceptanța																					
A11 Instruire																					
A11.1 Instruire personal care va utiliza produsele software implementate																					
A11.2 Instruire personal care va asigura mentenanța soluției																					
A11.3 Acceptanta instruire																					