AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Nr PSCID: 58/14.12.2020

Aprobat,
PREȘEDINTE
Ioan-Sabin SĂRMAȘ

Semnat/aprobat
în numele Președintelui Autoritati pentru Digitalizarea Romaniei
Vicepresedinte Octavian OPREA
Decizia nr. 297/12.05.2020

CAIET DE SARCINI

pentru

SERVICII DE DEZVOLTARE ȘI IMPLEMENTARE A SOLUȚIEI INFORMATICE, INCLUSIV FURNIZAREA DE ECHIPAMENTE ȘI SOFTWARE DE BAZĂ

în cadrul proiectului

„Platforma Software Centralizata pentru Identificare Digitala" („PSCID")

AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI
Str. Italiana, nr. 22, sector 2, Bucuresti
Tel.: 021.303.29.91; Fax: 021.305.28.99

1. INFORMAȚII GENERALE. OBIECTIVELE PROIECTULUI

1.1. *INFORMAȚII GENERALE*

Autoritatea Contractantă este **Autoritatea pentru Digitalizarea Romaniei** (denumita în continuare și ADR).

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

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

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

Prezentul caiet de sarcini cuprinde regulile de bază care trebuie respectate astfel încât potențialii ofertanți să elaboreze propunerea tehnică corespunzător cu necesitățile autorității contractante.

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

Fără a aduce atingere altor prevederi legale sau dispozițiilor legale privind liberul acces la informațiile de interes public ori ale altor acte normative care reglementează activitatea autorității contractante, autoritatea contractantă are obligația de a nu dezvălui informațiile din propunerea tehnică, elementele din propunerea financiară și/sau fundamentări/justificări de preț/cost transmise de operatorii economici indicate și dovedite de aceștia ca fiind confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Caracterul confidential se aplică doar asupra datelor/informațiilor indicate și dovedite ca fiind date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală.
Operatorii economici vor indica și dovedi în cuprinsul ofertei care informații din propunerea tehnică, elemente din propunerea financiară și/sau fundamentări/justificări de preț/cost sunt confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Informațiile indicate de operatorii economici din propunerea tehnică, elemente din propunerea financiară și/sau fundamentări/justificări de preț/cost ca fiind confidențiale trebuie să fie însoțite de dovada care le conferă caracterul de

confidenţialitate, dovadă ce devine anexă la ofertă.

1.2. *OBIECTIV GENERAL*

Într-un mod generic, o ***identitate electronică*** este *un mijloc pentru entitati ce se manifesta in spatiul electronic, de a se identifica pe cale electronică şi pe baza informaţiilor disponibile (identitate, rol, drept de acces etc) să obţină astfel acces la informatii sau servicii furnizate prin mijloace electronice. Identitatea permite unei entităţi să se distingă de orice altă entitate.*
O altă definiţie a identităţii electronice, aplicabila in sensul prezentului document persoanelor fizice, ar putea fi: *reprezentarea electronică a unei entităţi din lumea reală. Termenul este folosit pentru a înţelege echivalentul online al unei fiinţe umane, care participă în tranzacţiile electronice în numele persoanei în cauză.*

Managementul identităţilor electronice reprezinta un set complet de instrumente şi procese pentru gestionarea identităţilor electronice pentru toate entităţile care sunt afiliate şi care au nevoie de acces la resurse informatice. Managementul identităţilor electronice include, de asemenea, capabilităţi de gestionare a intrărilor non-persoană în registrul de identităţi.
Sistemul de management al identităţilor electronice nu este in mod neaparat o aplicaţie monolitică, ci mai degrabă o serie de sarcini îndeplinite de către mai multe componente software şi tehnologii. Proprietarii de resurse au posibilitatea de a defini şi pune în aplicare criteriile, pe baza datelor de identitate, care vor fi folosite pentru a acorda şi revoca accesul la resurse. Astfel, sistemul de management electronic al identitatii poate fi privit sau realizat ca o aplicatie distribuita sau centralizata care sa gestioneze identitatile si maparile dintre acestea si rolurile pe care o persoana, folosind o identitate electronica, le are in diferite medii sau sisteme informationale.

Scopul acestui proiect constă în implementarea *Platformei Software Centralizata pentru Identificare Digitala (PSCID)* care sa asigure poarta de acces si primul punct de securizare a serviciilor electronice de eGuvernare. Prin implementarea PSCID se asigura instrumente si modalitati mai puternice si sigure de identificare si autentificare electronica pentru accesarea si utilizarea servicilor electronice publice si de gestionare unitara si centralizata a identitatilor electronice ale cetatenilor, credentialelor acestora si provizionarea identitatilor in sistemele tinta care ofera servicii electronice.

Obiectivul general al proiectului consta in imbunatatirea si automatizarea modalitatii de acces a serviciilor electronice guvernamentale de catre cetateni si asigurarea identitatii electronice unice ale fiecarui cetatean care utilizeaza servicii electronice de eGuvernare.

1.3. *OBIECTIVE SPECIFICE*

Obiectivele specifice ale proiectului sunt:

- Constituirea **Registrului Electronic National de Identitati Electronice** in cadrul caruia se vor regasi Identitatile Electronice ale tuturor consumatorilor de servicii electronice de eGuvernare;
- Interconectarea cu portalul de acces unitar si securizat la serviciile electronice de eGuvernare si inrolarea cetatenilor la serviciile dorite;
- Interconectarea cu Catalogul Serviciilor Electronice de eGuvernare la care cetatenii se vor inrola prin intermediul PSCID;

- Cresterea gradului de utilizare a serviciilor de eGuvernare printr-o modalitate consecventa si simplificata de autentificare si accesare (inclusiv SSO – Single Sign ON);
- Inrolarea in cadrul PSCID a sistemelor si serviciilor electronice de eGuvernare din Romania;
- Inrolarea in cadrul PSCID a furnizorilor de identitate (publici si privati) existenti;
- Interconectarea PSCID cu nodul eIDAS national;
- Reducerea riscului in utilizarea serviciilor de eGuvernare si diminuarea posibilitatii si impactului de furt de identitate.

1.4. *CADRUL LEGAL*

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

Nr. crt.	Document
1	Strategia Europa 2020, o strategie pentru crestere inteligenta, ecologica si favorabila incluziunii, Cadrul Strategic Comun 2014-2020
2	Strategia europeana privind Piata Unica Digitala
3	Strategia Nationala privind Agenda Digitala pentru Romania (SNADR) 2020
4	Planul National pentru Dezvoltarea Infrastructurii NGN 2014 – 2020
5	Strategia Nationala pentru Competitivitate (SNC) 2015-2020
6	Strategia de Securitate Cibernetica a Romaniei
7	Planul National de Reforma
8	Strategia Nationala Anticoruptie 2016-2020
9	Strategia sectoriala in domeniul culturii si patrimoniului national pentru perioada 2014-2020
10	Strategia Nationala de Dezvoltare Rurala a Romaniei 2014-2020
11	Strategia pentru Consolidarea Administratiei Publice (SCAP) 2014-2020
12	Strategia privind mai buna reglementare 2014-2020
13	Analiza nevoilor si obiectivelor de simplificare si rationalizare a procedurilor administrative pentru cetateni – MDRAPFE
14	Strategia pentru imbunatatirea sistemului de elaborare, coordonare si planificare a politicilor publice la nivelul administratiei publice centrale
15	Programe Operationale 2014-2020
16	R (UE) nr. 1303/2013 de stabilire a unor dispozitii comune privind Fondul european de dezvoltare regionala, Fondul social european, Fondul de coeziune, Fondul european agricol pentru dezvoltare rurala si Fondul european pentru pescuit si afaceri maritime, precum si de stabilire a unor dispozitii generale privind Fondul european de dezvoltare regionala, Fondul social european, Fondul de coeziune si Fondul european pentru pescuit si afaceri maritime si de abrogare a R (CE) nr. 1083/2006 al Consiliului
17	Regulamentul (UE) nr. 1301/2013 privind Fondul european de dezvoltare regionala si dispozitiile specifice aplicabile obiectivului referitor la investitiile pentru crestere economica si locuri de munca si de abrogare a Regulamentului (CE) nr. 1080/2006
18	Regulamentul (UE) nr. 910/2014 al Parlamentului European si al Consiliului din 23 iulie

Nr. crt.	Document
	2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna si de abrogare a Directivei 1999/93/CE, cu deciziile si regulamentele derivate
19	Ordonanța de urgență nr. 68/2019 privind stabilirea unor măsuri la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative si Hotărârea Guvernului nr. 89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României
20	Legea nr. 365/2002 privind comertul electronic, republicata, cu modificarile si completarile ulterioare
21	Hotararea Guvernului nr. 1308 din 20 noiembrie 2002 privind aprobarea Normelor metodologice pentru aplicarea Legii nr. 365/2002 privind comertul electronic
22	Legea nr. 455/2001 privind semnatura electronica
23	Hotararea Guvernului nr. 1259/2001 pentru aprobarea Normei tehnice si metodologice pentru aplicarea Legii nr. 455/2001 privind semnatura electronica, actualizata
24	Legea nr. 451/2004 privind marca temporala
25	Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice
26	Regulamentul nr. 679 / 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date, cu modificarile si completarile ulterioare
27	Hotararea Guvernului nr. 775/2005 pentru aprobarea Regulamentului privind procedurile de elaborare, monitorizare si evaluare a politicilor publice la nivel central
28	Ordonanta de urgenta a Guvernului nr. 111/2011 privind comunicatiile electronice, actualizata
29	Legea nr. 98/2016 privind achizitiile publice
30	HG nr. 395/2016 pentru aprobarea Normelor Metodologice de aplicare a prevederilor referitoare la atribuirea Contractului de achizitie publica /acordului-cadru din Legea nr. 98/2016 privind achizitiile publice

1.5. *VALOAREA SI DURATA CONTRACTULUI*

Valoarea contractului

Valoarea totală a achiziției este de **78.400.000,00** lei fără TVA, respectiv **93.296.000,00** lei cu TVA.

Durata de implementare a contractului

Durata de implementare a contractului este de **27 de luni**.

Activitățile aflate în responsabilitatea Prestatorului sunt prevăzute a se desfășura conform graficului de implementare a proiectului, anexa la prezentul Caiet de sarcini.

În cazul în care perioada de derulare a procedurii de achiziție publică impune modificarea termenelor de desfășurare a activităților și subactivităților, ofertantul declarat câștigător va actualiza graficul de implementare cu acordul Beneficiarului și va constitui anexă la contract.

2. CERINTE PRIVIND SOLUTIA TEHNICA

2.1. *CERINȚE GENERALE*

Pentru a putea realiza un management eficient al identitatilor electronice trebuie sa fie identificate in primul rand serviciile de eGuvernare electronice actuale, consumatorii acestora si modalitatile de identificare si autentificare a utilizatorilor (credentialele).
Astfel prin intermediul proiectului se va realiza inerconectarea cu **Portalul PCUe** si cu **Catalogul Serviciilor Electronice de eGuvernare** care vor face obiectul managementului la nivel national al Identitatilor Electronice. Pentru fiecare serviciu electronic identificat se va identifica si modalitatea actuala de autentificare in vederea accesarii acestuia.
La consultarea Catalogului Serviciilor Electronice de eGuvernare se vor identifica serviciile electronice de eGuvernare care vor intra in scopul proiectului PSCID si a modalitatilor de autentificare:

- ce servicii electronice sunt oferite catre cetateni;
- modalitatea de autentificare si tipurile de credentiale utilizate;
- furnizorul de identitate.

Pentru fiecare serviciu electronic in parte se vor identifica tipurilor de credentiale utilizate in prezent de catre toti actorii:

- Cetateni: utilizatori/parole, certificat digital calificat, etc.;
- Institutii publice: utilizatori/parole, certificate digitale necalificate, certificate digitale calificate, etc.

PSCID va asigura toate aspectele mentionate anterior si in plus isi propune sa implementeze si instrumente de detectare a posibilelor furturi de identitate.

Referitor la credentialele utilizate pentru accesarea serviciilor prin intermediul PSCID vor fi asigurate:

- **instrumente de emitere, gestionare si de personalizare a credentialelor de tip parole;**
- **instrumente de emitere si gestionare tokenuri virtuale (software) de tip one-time-password (OTP);**
- **suportul pentru integrarea cu credentialele de tip certificate digitale emise de terti:**
  - **calificate emise de furnizori autorizati;**
  - **necalificate emise de institutiile statului;**

Validare identitate la distanță

Validarea identității la distanță va fi un serviciu care introduce **autentificarea cu doi factori si care va fi folosit la inregistrarea cetatenilor in PSCID.**
Criteriile de bază pentru alegerea soluție au fost:

- autentificare puternică
- uşurința de utilizare
- impactul tehnic şi organizatoric

Au fost identificate următoarele avantaje pentru examinarea la distanță:

- Uşor de utilizat de către utilizator: dacă utilizatorul întâmpină dificultăţi în timpul verificării la distanţă poate anula procesul.
- Procesare directă: posibilitatea de a verifica identitatea utilizatorului într-o manieră complet automatizată fără interferenţe umane. Mai mult automatizarea înseamnă timpi de verificare mai scurţi şi îmbunătăţeşte experienţa utilizatorului. De asemenea, oferă mai multă eficienţă şi mai puţine erori (de exemplu, din cauza erorilor de introducere a textului atunci când se introduc informaţii personale).
- Rata suficientă de penetrare: cât mai mulţi potenţiali utilizatori ţintă trebuie să poată trece printr-un proces de examinare de la distanţă. Este posibil ca anumite grupuri de utilizatori să nu poată executa procesul de examinare la distanţă deoarece nu dispun de anumite funcţionalităţi necesare pentru verificarea de la distanţă. Pentru acestia se vor pune la dispozitie instrumente de inregistrare in portal.
- Nivel suficient de asigurare a autentificării: rezultatul verificării de la distanţă trebuie să ofere o suficientă asigurare în privinţa identităţii utilizatorului (care la rândul său va oferi un nivel de autentificare mai ridicat de asigurare). Serviciul va funcţiona minim la nivelurile 2 şi 3 ale ISO29158, în funcţie de mijloacele de autentificare (aceste niveluri corespund nivelurilor eIDAS Scăzut şi Substanţial).
- Controlabilitate / audibilitate: capacitatea de a controla procesul de examinare de la distanţă astfel încât să fie pus în aplicare de către toate instituţiile într-o manieră fără echivoc, inclusiv capacitatea de a controla procesul în scopuri de responsabilitate.

Soluţii identificate in alte state membre

In cadrul unor studii de fezabilitate la nivel european a fost creată următoarea listă de soluţii de verificare la distanţă:

- fizic la ghiseu;
- video chat;
- transmiterea unei fotografii a documentului de identitate prin intermediul unui telefon mobil şi a unei aplicaţii specifice;
- aplicaţie mobilă cu tehnologie NFC pentru citirea cipului documentului de identitate;
- Identitate derivată de la autentificare puternică de către solutii bazate pe carduri bancare (exemplu Olanda iDIN, Idensys sau iDEAL)
- Identitate derivată de la autentificare puternică prin soluţii naţionale eID prin eIDAS;
- reutilizarea birourilor de înregistrare existente în alte organizaţii precum municipalităţi, bănci, Camera de Comerţ, Autorităţi de Certificare sau alte instituţii de învăţământ şi cercetare;
- Verificarea comunitară, verificare realizată de alţi utilizatori.

Concluzia a fost: Soluţiile de verificare bazate pe aplicaţii mobile trebuie să fie preferate, deoarece acestea facilitează cel mai bine toate cazurile de utilizare.

Procesul de verificare la distanţă (autentificare) in PSCID

Procesele de înregistrare şi verificare pentru a stabili identitatea utilizatorului şi a lega această identitate cu acreditările de autentificare vor fi implementate după cum urmează:

A. Procesul de înregistrare în sistem de autoservire

1. Utilizatorul se conecteaza la Registrul Electronic National al Identitatilor Electronice (RENIE) din cadrul PSCID (de tip „utilizator nou")

2. RENIE solicită utilizatorului să-şi scaneze documentul de identitate, sa faca o fotografie cu fata sa (echivalenta cu cea din document - de tip live selfie) si sa completeze toate datele necesare contului sau (ex: adresa de mail, telefon etc)
3. RENIE verifică identitatea utilizatorului (in sistemele MAI) si compară faţa utilizatorului cu imaginea din documentul de identitate.
4. In situatia identificarii pozitive RENIE creaza identitatea electronica si activează tokenul (software) din portalul de administrare PSCID, adică se stabileşte legatura între identitatea verificată a utilizatorului şi identitatea sa electronica. Utilizatorul poate folosi acum tokenul ca fiind un al doilea factor de autentificare (OTP) in procesul de autentificare.

B. Procesul de verificare

1. In situatia in care utilizatorul are conturi de utilizator la instituţii federalizate care ofera servicii de eguvernare (ex.: ANAF, ONRC etc) sau detine certificate electronice (calificate sau necalificate emise de MAI) acesta va completa toate datele necesare pentru operatiunile de tip SSO (Single Sign On). PSCID va verifica toate aceste credentiale si metodele de autentificare la furnizorii de identitate si furnizorii de servicii.
2. Utilizatorul selectează un tip de autentificare (OTP sau certificat electronic) pentru a se înregistra şi va face o autentificare cu el pentru a dovedi că deţine credentialele necesare.

Niveluri de asigurare a identiatii

Există mai multe standarde internaţionale pentru asigurarea identităţii, cum ar fi NIST (SUA), eIDAS (Europa) şi ISO29158. Cele patru niveluri de asigurare a identităţii folosite în mod obişnuit sunt:

- LoA 1 - Puţin sau deloc încredere în identitatea afirmată;
- LoA 2 - Putina încredere în identitatea afirmată;
- LoA 3 - Înaltă încredere în identitatea afirmată;
- LoA 4 - Încredere foarte mare în identitatea afirmată.

Diferitele specificaţii elaborează înţelesul acestor etichete prin specificarea cerinţelor privind identificarea şi înregistrarea utilizatorilor, gestionarea autenticităţii token-ului, autentificarea şi securitatea operaţională.

În ceea ce priveşte alinierea la cadrul european eIDAS, PSCID, pentru nivelurile de asigurare a autentificării, va asigura minim nivelurile Substantial (= LoA 3) şi Ridicat (= LoA 4)

Pentru realizarea acestei cerinţe se vor avea in vedere cerintele eIDAS:

- "Au fost luate măsuri pentru a minimiza riscul ca identitatea persoanei să nu fie identitatea revendicată, luând în considerare, de exemplu, riscul unor documente pierdute, furate, suspendate, revocate sau expirate" - PSCID va verifica dacă documentul de identitate a fost raportat ca fiind pierdut sau furat.
- "Există un sistem eficient de management al securităţii informaţiilor pentru gestionarea şi controlul riscurilor de securitate a informaţiilor. Sistemul de management al securităţii informaţiilor respectă standarde sau principii dovedite pentru gestionarea şi controlul riscurilor de securitate a informaţiei" - PSCID va implementa un sistem care sa respecte aceste cerinte.

2.1.1. Alinierea la eIDAS

Acest capitol mapează caracteristicile propuse pentru PSCID bazat pe profilul SAML la cerințele eIDAS ale cărui niveluri de asigurare sunt definite în Decizia de punere în aplicare a Regulamentului (UE) 2015/1502 În conformitate cu articolul 8 alineatul (3) din Regulamentul eIDAS (UE) 910/2014.
În acest scop, a fost luată în considerare fiecare cerință a Regulamentului de punere în aplicare şi a fost explicat modul în care schema de identitate îndeplineşte cerințele minime privind gradul SUBSTANTIAL de asigurare.

Legislație

SEN

- Hotarare nr. 862 din 22 iulie 2009 privind modificarea si completarea Hotararii Guvernului nr. 1.085/2003 pentru aplicarea unor prevederi ale Legii nr. 161/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei, referitoare la implementarea Sistemului Electronic National
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informatiile de interes public
- Legea nr. 161 din 19 aprilie 2003 privind unele masuri pentru asigurarea transparentei în exercitarea demnităților publice
- Normele metodologice din 7 februarie 2002 de aplicare a Legii nr. 544/2001 privind liberul acces la informațiile de interes public

SEAP

- Legea 98/2016 privind achizitiile publice
- Legea 99/2016 privind achizitiile sectoriale
- Legea 100/2016 privind concesiunile de lucrari si concesiunile de servicii
- Legea 101/2016 privind remediile si caile de atac in materie de atribuire a contractelor de achizitie publica, a contractelor sectoriale si a contractelor de concesiune de lucrari si concesiune de servicii, precum si pentru organizarea si functionarea Consiliului National de Solutionare a Contestatiilor
- HG 394/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului sectorial/acordului-cadru din Legea nr. 99/2016 privind achizitiile sectoriale
- HG 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achizitie publica/acordului-cadru din Legea nr. 98/2016 privind achizitiile publice
- OG 114/2011 privind atribuirea anumitor contracte de achizitii publice in domeniile apararii si securitatii

PCUe

- Hotararea nr 922/2010 privind organizarea si functionarea Punctului de contact unic electronic
- Hotararea nr 542/2003 pentru aprobarea Normelor de utilizare a sistemului electronic de colectare a datelor statistice si aprobare a listei cercetarilor statistice incluse in sistemul electronic
- Hotararea nr 1308/2002 privind aprobarea Normelor metodologice pentru aplicarea Legii nr 365/2002 privind comertul electronic

- Legea nr 68/2010 pentru aprobarea Ordonantei de urgenta a Guvernului nr 49/2009 privind libertatea de stabilire a prestatorilor de servicii si libertatea de a furniza servicii in Romania
- Legea nr 365/2002 privind comertul electronic
- Legea nr 455/2001 privind semnatura electronica
- Legea nr 544/2001 privind liberul acces la informatiile de interes public
- Ordonanta de urgenta nr 49/2009 privind libertatea de stabilire a prestatorilor de servicii si libertatea de a furniza servicii in Romania
- Ordonanta de urgenta nr.41/2016 privind stabilirea unor masuri de simplificare la nivelul administratiei publice centrale si pentru modificarea si completarea unor acte normative
- Ordonanta de urgenta nr.100/2016 pentru modificarea si completarea Legii nr.100/2016 pentru modificarea si completarea Legii nr.350/2001 privind amenajarea teritoriului si urbanismul, precum si a Legii nr.50/1991 privind autorizarea executarii lucrarilor de constructii

SNEP

- Hotararea nr 1235/2010 privind aprobarea realizarii Sistemului national electronic de plata online a taxelor si impozitelor utilizand cardul bancar
- Ordinul 95/2011 pentru aprobarea Normelor metodologice privind Sistemul national electronic de plata online a taxelor si impozitelor utilizand cardul bancar
- Ordinul nr 173/2011 pentru aprobarea Normelor tehnice privind Sistemul national electronic de plata online a taxelor si impozitelor utilizand cardul bancar
- Hotararea nr 1070/2013 pentru modificarea si completarea Hotararii Guvernului nr 1235/2010 privind aprobarea realizarii Sistemului national electronic de plata online a taxelor si impozitelor utilizand cardul bancar

LEGISLATIE EUROPEANA

- Directiva 2003-98-ec privind reutilizarea informatiilor din sectorul public
- Directiva 2006-123-ec privind serviciile în cadrul pietei interne
- REGULAMENTUL (CE) NR. 1177/2009 R al comisiei europene din 30 noiembrie 2009 de modificare a Directivelor 2004/17/CE, 2004/18/CE si 2009/81/CE ale Parlamentului European si ale Consiliului in ceea ce priveste pragurile de aplicare a acestora in cazul procedurilor de atribuire a contractelor de achizitii
- DIRECTIVA 2007/66/CE A PARLAMENTULUI EUROPEAN SI A CONSILIULUI
- de modificare a Directivelor 89/665/CEE si 92/13/CEE ale Consiliului in ceea ce priveste ameliorarea eficacitatii cailor de atac in materie de atribuire a contractelor de achizitii publice - REGULAMENTUL (CE) NR. 213/2008 al comisiei europene din 28 noiembrie 2007 de modificare a Regulamentului (CE)nr.2195/2002 al Parlamentului European si al Consiliului privind Vocabularul comun privind achizitiile publice(CPV) si al Directivelor 2004/17/CE si 2004/18/CE ale Parlamentului European si ale Consiliului in ceea ce priveste procedurile de achizitii publice,in ceea ce priveste revizuirea CPV
- REGULAMENTUL (CE) NR. 213/2008 al comisiei europene din 28 noiembrie 2007 de modificare a Regulamentului (CE)nr.2195/2002 al Parlamentului European si al Consiliului privind Vocabularul comun privind achizitiile publice(CPV) si al Directivelor 2004/17/CE si 2004/18/CE ale Parlamentului European si ale Consiliului in ceea ce priveste procedurile de achizitii publice,in ceea ce priveste revizuirea CPV
- REGULAMENTUL (CE) NR. 1564/2005 al comisiei europene din 7 septembrie 2005 de stabilire a formularelor standard pentru publicarea anunturilor in cadrul procedurilor de

atribuire a contractelor de achizitii publice in conformitate cu Directivele 2004/17/CE si 2004/18/CE ale Parlamentului European si Consiliului

- Regulamentul (CE) nr. 2195/2002 al Parlamentului European si al Consiliului din 5 noiembrie 2002 privind Vocabularul comun privind achizitiile publice (CPV)
- Regulamentul (CE) NR. 2151/2003 al Comisiei din 16 decembrie 2003 de modificare a Regulamentului (CE) nr. 2195/2002 al Parlamentului European si al Consiliului privind Vocabularul comun privind achizitiile publice (CPV)
- DIRECTIVA 2004/17/CE A PARLAMENTULUI EUROPEAN SI A CONSILIULUI
- din 31 martie 2004 de modificare de coordonare a procedurilor de atribuire a contractelor de achizitii in sectoarele apei, energiei, transporturilor si serviciilor postale.
- DIRECTIVA 2004/18/CE A PARLAMENTULUI EUROPEAN SI A CONSILIULUI
- din 31 martie 2004 de modificare privind coordonarea procedurilor de atribuire a contractelor de achizitii publice de lucrari, de bunuri si de servicii.
- Directiva 1999/93/CE a Parlamentului European si a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnaturile electronice
- Directiva 2000/31/CE a Parlamentului European si a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societatii informationale, in special ale comertului electronic, pe piata interna (directiva privind comertul electronic)
- REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUIdin 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE
- REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/1501 AL COMISIEI din 8 septembrie 2015 privind cadrul de interoperabilitate prevăzut la articolul 12 alineatul (8) din Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă
- REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/1502 AL COMISIEI din 8 septembrie 2015 de stabilire a unor specificaţii şi proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare electronică în temeiul articolului 8 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă

Terminologie

- **„sursă sigură”** înseamnă orice sursă, indiferent de formă, în privinţa căreia se poate avea încredere că furnizează date, informaţii şi/sau dovezi exacte care pot fi utilizate pentru dovedirea identităţii;
- **„factor de autentificare”** înseamnă un factor în privinţa căruia s-a confirmat că are legătură cu o persoană şi care se încadrează în una dintre următoarele categorii:
  - „factor de autentificare bazat pe posesie” înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze că se află în posesia acestuia;
  - „factor de autentificare bazat pe cunoştinţe” înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze cunoaşterea informaţiei în cauză;
  - „factor de autentificare inerent” înseamnă un factor de autentificare care se bazează pe o caracteristică fizică a unei persoane fizice şi în cazul căruia subiectul trebuie să demonstreze că prezintă respectiva caracteristică fizică;

- **„autentificare dinamică”** înseamnă un proces electronic care utilizează criptografia sau alte tehnici pentru a oferi un mijloc de a crea, la cerere, o dovadă electronică a faptului că subiectul controlează datele de identificare sau se află în posesia acestora, dovadă care se modifică la fiecare autentificare a subiectului în sistemul care verifică identitatea subiectului;
- **„sistem de management al securității informațiilor”** înseamnă un set de procese și proceduri menite să gestioneze la niveluri acceptabile riscurile legate de securitatea informațiilor.
- În continuare, acest document folosește și următorii termeni:
  - Card de servicii de sănătate - card național de sanatate emis de CNAS;
  - Furnizori de identitate;
  - CEI: carte de identitate electronică.

2.1.1.1. Corespondență cu nivelurile de asigurare eIDAS

2.1.1.1.1. Înscrierea

Cererea și înregistrarea
Cerintele Regulamentului eIDAS vor fi marcate pe fond gri
Scăzut, Substanțial și Ridicat

1. Asigurarea faptului că solicitantul este la curent cu termenii și condițiile legate de utilizarea mijloacelor de identificare electronica.

Site-ul PSCID va furniza toată documentația pe care utilizatorul trebuie să o înțeleagă pentru a activa identitatea digitală.
Se va crea o sectiune "Documentație" va conține următoarea documentație:
Ghid de operare:

- Ghidul utilizatorului
- Instrucțiuni pentru utilizarea identității digitale
- Termeni și condiții generale
- Formularul de solicitare
- Termeni și condiții pentru un serviciu public
- Soluții de autentificare
- Formularul de revocare.

În plus, în timpul procesului de înregistrare, înainte de a utiliza "formularul de solicitare", utilizatorul trebuie să-și confirme decizia de a obține o identitate digitală și să declare că a citit "Termeni și condiții generale" prin bifarea unei căsuțe.

2. Asigurarea faptului că solicitantul are cunoștință de măsurile de prevedere recomandate în materie de securitate a mijloacelor de identificare electronică

Înainte de a solicita identitatea digitală, utilizatorul va putea consulta și descărca informațiile publicate de ADR pentru fiecare furnizor de identitate la adresa http://www.adr.ro.
Instrucțiunile vor enumera acțiunile pe care utilizatorul trebuie să le respecte:

- Să nu comunice unei terțe părți în nici un fel acreditările de acces, păstrându-le cu maximă atenție, pe întreaga perioadă de valabilitate a Identității Digitale;
- Să ia toate precauțiile și contramăsurile pentru a reduce / atenua / elimina riscurile de furt / duplicare / interceptare;
- Să respecte cu maximă atenție utilizarea, stocarea și protecția identității digitale, a dispozitivului și a codului de activare asociat;
- Să ia toate măsurile posibile pentru a împiedica utilizarea propriilor identități digitale de către terți;

- Să protejeze secretul acreditării prin necomunicarea sau dezvăluirea către terți a codurilor personale;
- Să nu transmită identitatea digitală unor terțe părți

3. Colectarea datelor de identitate relevante necesare pentru dovedirea și verificarea identității.
La etapa de înregistrare, toate datele necesare pentru verificarea identității sunt colectate:
Numele și prenumele, sex, data și locul nașterii, CNP, un document de identitate valabil, numărul de telefon mobil, adresa de e-mail.

Dovedirea și verificarea identității (persoană fizică)

SCĂZUT

1. Se poate presupune că persoana este în posesia unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică și care reprezintă identitatea pretinsă..
2. Se poate presupune că dovezile sunt autentice sau că ele există în conformitate cu o sursă sigură, iar dovezile par să fie valabile.
3. Se știe dintr-o sursă sigură că identitatea pretinsă există și se poate presupune că persoana care pretinde a avea identitatea respectivă corespunde acelei identități.

SUBSTANTIAL

Trebuie să fie îndeplinite cerințele aferente nivelului scăzut, plus una dintre alternativele enumerate la punctele 1-4:

1. 1. S-a verificat că persoana este în posesia unor dovezi care sunt recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică și care reprezintă identitatea pretinsă; și

dovezile au fost verificate pentru a se stabili că sunt autentice sau se știe, în conformitate cu o sursă sigură, că ele există și că se referă la o persoană reală; și

au fost luate măsuri pentru a reduce la minimum riscul ca identitatea persoanei să nu fie cea pretinsă, luând în considerare, de exemplu, riscul utilizării unor dovezi pierdute, furate, suspendate, revocate sau expirate;

sau;

2. Un document de identitate este prezentat în cadrul unui proces de înregistrare în statul membru în care a fost eliberat documentul, iar acesta pare să se refere la persoana care îl prezintă;

ȘI

au fost luate măsuri pentru a reduce la minimum riscul ca identitatea persoanei să nu fie cea pretinsă, luând în considerare, de exemplu, riscul utilizării unor documente pierdute, furate, suspendate, revocate sau expirate; sau;

Sau 3. În cazul în care procedurile utilizate anterior de către o entitate publică sau privată în același stat membru în alt scop decât emiterea de mijloace de identificare electronică oferă o asigurare echivalentă cu cele prevăzute în secțiunea 2.1.2 pentru nivelul de asigurare substanțial, atunci entitatea responsabilă cu înregistrarea nu trebuie să repete aceste proceduri anterioare, cu condiția ca respectiva asigurare echivalentă să fie confirmată de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului (1) sau de un organism echivalent; sau

Sau 4. În cazul în care sunt emise mijloace de identificare electronică pe baza unui mijloc de identificare electronică notificat valabil având nivelul de asigurare substanțial sau ridicat și luând

în considerare riscurile unei modificări ale datelor de identificare personală în cauză, nu este necesar să se repete procedurile de dovedire și de verificare a identității. În cazul în care mijlocul de identificare electronică servind drept bază nu a fost notificat, nivelul de asigurare substanțial sau ridicat trebuie confirmat de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent.

RIDICAT

Să fie îndeplinite cerințele de la punctul 1 sau 2:

1.Trebuie să fie îndeplinite cerințele aferente nivelului substanțial, plus una dintre alternativele enumerate la literele a-c:

A. În cazul în care s-a verificat că persoana este în posesia unor dovezi de identificare fotografice sau biometrice recunoscute de către statul membru în care s-a depus cererea vizând mijlocul de identificare electronică, iar elementele respective reprezintă identitatea pretinsă, atunci dovezile sunt verificate pentru a se stabili dacă sunt valabile în conformitate cu o sursă sigură;

PSCID se va incadra in categoria RIDICAT.

Metodele de identificare prin vizualizare directă sunt următoarele:

V-1

Identificare la distanță: în cazul în care solicitantul utilizează identificarea vizuală la distanță, documentul trebuie prezentat în timpul procesului de înregistrare audio / video și sunt adoptate toate contramăsurile următoare:

- Se verifică identitatea solicitantului şi verifică documentele de identitate.
- La sfârşitul procedurii, dacă există încredere în identitatea solicitantului se semnează digital raportul de identificare si se atribuie persoanei identitatea digitala

Utilizatorul trebuie să furnizeze un document de identitate valabil: numai documentele de identitate recunoscute legal sunt acceptate în timpul „identificării la distanță " (carte de identitate).

Prin document de identitate se înţelege cartea de identitate, cartea electronică de identitate, cartea de identitate provizorie şi buletinul de identitate, aflate în termen de valabilitate. Actul de identitate face dovada identităţii, a cetăţeniei române, a adresei de domiciliu şi, după caz, a adresei de reşedinţă.

În condiţiile Legii nr. 248/2005 privind regimul liberei circulaţii a cetăţenilor români în străinătate, cu modificările şi completările ulterioare, cartea de identitate şi cartea electronică de identitate constituie document de călătorie în statele membre ale Uniunii Europene.

Este utilizată o sursă autoritară pentru verificare: SNIEP consultată pentru a verifica existența și valabilitatea datelor furnizate de către Utilizator.

Prin interogarea bazei de date a MAI, PSCID este foarte sigur că Codul Numeric Personal există și că este atribuit în mod unic.

și

prin intermediul unei comparații între una sau mai multe caracteristici fizice ale solicitantului și o sursă sigură se constată că persoana în cauză are identitatea pretinsă;

Se verifică veridicitatea fotografiei documentului de identitate, prin intermediul caracteristicilor obiective a căror autenticitate este verificată utilizând sursele autoritare.

În plus, actul de identitate expirat nu este acceptat. În orice caz, PSCID în timpul fazei de identificare și al controalelor de tip back office, verifică data de expirare a actului de identitate.

În plus, baza de date a Ministerului de Interne este utilizată pentru a verifica dacă documentul nu este pierdut sau furat.

Sau

B. În cazul în care procedurile utilizate anterior de către o entitate publică sau privată în același stat membru în alt scop decât emiterea de mijloace de identificare electronică oferă o asigurare

echivalentă cu cele prevăzute în secțiunea 2.1.2 pentru nivelul de asigurare ridicat, atunci entitatea responsabilă cu înregistrarea nu trebuie să repete aceste proceduri anterioare, cu condiția ca respectiva asigurare echivalentă să fie confirmată de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent;
și
se iau măsuri pentru a demonstra că rezultatele procedurilor anterioare rămân valabile; sau
Identități anterioare deținute de administrația publică sau de către operatori privați (furnizorii de semnaturi calificate de ex), de-a lungul timpului, în scopul de a identifica clienți / angajați pentru a furniza servicii, pot fi reutilizate în scopul de a obține identitatea In cadrul PSCID.
ADR va implementea o procedură specifică prin care își rezervă dreptul de a efectua verificări la structurile utilizate pentru eliberarea identităților anterioare implementării sistemului și va solicita solicitarea organismelor de evaluare a conformității (CAB) un raport de evaluare a conformității (CAR) a sistemelor de verificare a identității în ceea ce privește cerințele tehnice definite prin Regulamentul de punere în aplicare (UE) 2015/1502.
Sau
C. În cazul în care sunt emise mijloace de identificare electronică pe baza unui mijloc de identificare electronică notificat valabil având nivelul de asigurare ridicat și luând în considerare riscurile unei modificări ale datelor de identificare ale persoanei în cauză, nu este necesar să se repete procedurile de dovedire și de verificare a identității. În cazul în care mijlocul de identificare electronică servind drept bază nu a fost notificat, nivelul de asigurare ridicat trebuie confirmat de un organism de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 sau de un organism echivalent
și
se iau măsuri pentru a demonstra că rezultatele acestei proceduri anterioare de emitere a unui mijloc de identificare electronică notificate rămân valabile.

V-2
Semnătura electronică calificată: un certificat electronic calificat este emis de un QTSP emis prin controlul unui act de identitate recunoscut de legislația națională; Pentru a obține identitatea digitală in PSCID, solicitantul semnează formularul de solicitare a identității digitale împreună cu codul său de verificare. Datele solicitantului sunt comparate cu datele din identitatea certificatului electronic calificat.
ADR prin organismul de evaluare a conformității menționat la articolul 2 alineatul (13) din Regulamentul (CE) nr. 765/2008 confirmă echivalentul nivelului ridicat de garanție de două ori, o evaluare pentru IDP (identitate electronica), si o alta pentru statutul de QTSP.

2.1.1.1.2. Gestionarea mijloacelor de identificare electronică

Caracteristicile și concepția mijloacelor de identificare electronică
SCĂZUT

1. Mijlocul de identificare electronică utilizează cel puțin un factor de autentificare.
Mijloacele de autentificare electronică utilizează un factor de autentificare (pereche de acreditări de nume de utilizator și de parolă). Politica de securitate a parolei PSCID va fi certificat ISO27001: 2013, realizat conform descrierii de mai jos.
2. Mijlocul de identificare electronică este conceput în așa fel încât emitentul să ia măsuri rezonabile pentru a se asigura că este utilizat numai sub controlul sau în posesia persoanei căreia îi aparține.

Factorul de autentificare (parola) este ales de către Utilizator care este conştient de păstrarea lui strict confidenţială. Resetarea parolei este posibilă numai prin cunoaşterea răspunsului la întrebările de securitate.
Parola trebuie modificată cel puţin o dată la trei luni şi trebuie să aibă cel puţin 8 caractere, să conţină cel puţin un număr mare, un litere mici, un număr şi un caracter special.
Fiecare utilizare este înregistrată şi pusă la dispoziţia solicitantului printr-o cerere specifică

SUBSTANTIAL

1. Mijlocul de identificare electronică utilizează cel puţin doi factori de autentificare din categorii diferite.

Mijloacele de identificare electronică utilizează o autentificare cu doi factori: primul factor de autentificare este parola; al doilea factor de autentificare este o parolă unică (OTP) randomizată (OTP) trimisă utilizatorului prin: APP mobil, e-mail. În acest fel, se respectă paradigma „Ceva ce ştiţi" (Something You Know - SYK) şi ceva „Ce aţi avut" (Something You Have - SYH).

2. Mijlocul de identificare electronică este conceput în aşa fel încât să se poată **presupune** că este utilizat numai sub controlul sau în posesia persoanei căreia îi aparţine.

Cel de-al doilea factor de autentificare este utilizat în mod rezonabil de titular:

- deoarece aplicaţia APP mobilă este instalată pe dispozitivul aflat în posesia sa, printr-o procedură de înregistrare a dispozitivului (de exemplu, codul de securitate prin email şi codul de securitate setat pentru deblocarea prin APP);
- pentru parola OTP - o singură dată prin email.

RIDICAT

Nivelul substanţial, plus:

1. Mijlocul de identificare electronică este protejat împotriva copierii şi a manipulării frauduloase, precum şi împotriva atacatorilor cu potenţial ridicat de atac.

Nivelul de securitate PSICID L3 (echivalent cu LoA4 din ISO-IEC 29115) va utiliza un sistem de autentificare bazat pe certificatele digitale (doar pentru cetatenii care poseda certificate digitale) şi respectă cerinţele privind cheile private de pe dispozitive pentru crearea unei semnături electronice în conformitate cu Regulamentul Nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind serviciile de identificare electronică şi servicii de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93 / CE.
Certificarea acestor dispozitive garantează, printre altele, că nu se pot duplica (cheia privată nu este exportabilă) şi nici nu a fost manipulată (în caz de încercare de manipulare, dispozitivul devine inutilizabil).

2. Mijlocul de identificare electronică este conceput astfel încât să poată fi protejat în mod fiabil de către persoana căreia îi aparţine împotriva utilizării de către alte persoane .

Certificatul utilizat pentru autentificarea PSCID este stocat în HSM în deplină conformitate cu procedurile şi mecanismele dispozitivului de certificare. Cheia privată este stocată în smartcard sau HSM şi nu poate fi nici extrasă, nici clonată şi fără să se utilizeze cheia pentru a o debloca.
În cazul serverului HSM, este necesară pentru deblocarea certificatului realizarea unei autentificări cu nume de utilizator, parolă şi OTP. Prin urmare, dispozitivul nu poate fi utilizat de la terţi în cazul în care aceştia intră în posesia acestuia.

Emiterea, livrarea şi activarea

SCĂZUT

După emitere, mijlocul de identificare electronică este livrat prin intermediul unui mecanism graţie căruia să se poate presupune că acesta ajunge numai la persoana căreia îi este destinat.

NA

SUBSTANTIAL

După emitere, mijlocul de identificare electronică este livrat prin intermediul unui mecanism grație căruia să se poate presupune că acesta ajunge numai în posesia persoanei căreia îi aparține.

NA

RIDICAT

În cadrul procesului de activare se verifică dacă mijlocul de identificare electronică a ajuns numai în posesia persoanei căreia îi aparține.

Mijloacele de identificare electronică sunt livrate și activate după procesul de înregistrare și identificare la un nivel înalt și numai în posesia persoanei căreia îi aparțin.

Parola nu este transmisă solicitantului, deoarece acesta este aleasă și înregistrată de solicitant în timpul procesului de înregistrare și identificare.

OTP este trimis folosind mijloacele înregistrate de Utilizator în timpul procesului de înrolare și confirmat în timpul procesului de identificare.

LoA4 este realizat utilizând un sistem de autentificare cu doi factori bazați pe certificate digitale și criterii de utilizare a cheilor private pe dispozitive care îndeplinesc cerințele din anexa II la Regulamentul 910/2014 (a se vedea punctul RIDICAT).

Este posibilă asocierea cu identității proprietarului cu dispozitive existente, cum ar fi CEI și certificate calificate QSCD emise de aceeași furnizori de identitate care acționează și ca furnizori de servicii de încredere calificat.

Pentru a asocia dispozitivul și pentru a-l pune sub controlul proprietarului identității, proprietarul identității trebuie să efectueze procedura de asociere.

Solicitantul trebuie să se conecteze la panoul Self-service al PSCID, prin intermediul căruia poate administra identitatea PSCID. În timpul autentificării, sistemul solicită solicitantului să utilizeze un certificat cu cea mai mare valoare a nivelul de asigurare EIDAS disponibilă. Odată terminată logarea, solicitantul începe procesul de activare a dispozitivelor. În cazul semnăturii la distanță: solicitantului i se solicită să semneze o cerere de autentificare către serverul HSM cu acreditări de la distanță (nume de utilizator, parolă și OTP). Dacă codul CNP se potrivește cu utilizatorul, procedura continuă cu următorul pas.

Sistemul reiterează "Certificatul de stare online a certificatelor" (OSCP) și "Liste de revocare a certificatelor" (CRL) pentru verificările valabilității certificatului utilizat. Dacă codul CNP al certificatului se potrivește cu utilizatorul, procedura continuă cu următorul pas.

Suspendarea, revocarea și reactivarea

SCĂZUT, SUBSTANTIAL, ȘI RIDICAT

1. Este posibil ca un mijloc de identificare electronică să fie suspendat și/sau revocat în timp util și în mod eficace.

Suspendarea:

Suspendarea unei identități digitale implică dezactivarea temporară a acesteia. O identitate digitală suspendată poate fi reactivată sau revocată.

- Suspendarea de către Utilizator: utilizatorul poate solicita suspendarea imediată a Identității Digitale dacă consideră că a fost compromisă. La primirea cererii de suspendare, Furnizorul de Identitate suspendă Identitatea digitală pentru o perioadă (maximum treizeci de zile), furnizând informații specifice Utilizatorului.

În termen de treizeci de zile, utilizatorul trebuie să transmită furnizorului de identitate o copie a cererii către autoritatea publică responsabilă pe baza aceloraşi fapte pe care se bazează cererea de suspendare (ex. furt).

În cazul în care nu se primesc cele descrise în în termenii de mai sus, furnizorul de identitate (Identity Provider) restabileşte identitatea digitală.

- Suspendarea de către furnizorul de identitate: la data expirării actului de identitate, Furnizorul de Identitate va suspenda în mod autonom identitatea digitală şi va avertizeaza utilizatorul utilizând datele de contact (e-mail sau număr de telefon mobil).

Revocarea:

- Revocarea de către utilizator: solicitarea utilizatorului în orice moment, fără a fi nevoie de motivaţie privind revocarea identităţii digitale. Pentru a revoca identitatea digitală, utilizatorul trebuie să se conecteze la site-ul furnizorului de identitate folosind autentificarea cu două factori.
- Revocarea de către Furnizorul de Identitate: Furnizorul de Identitate va revoca în mod automat Identitatea Digitală a Utilizatorului, în următoarele cazuri:
  - În cazul inactivităţii identităţii digitale pentru mai mult de 24 de luni
  - În cazul decesului Utilizatorului;
  - În cazul expirării contractului.

2. Existența unor măsuri luate în scopul prevenirii suspendării, a revocării şi/sau a reactivării neautorizate

Pentru a suspenda sau revoca identitatea digitală, utilizatorul trebuie să se conecteze la PSCID cu o autentificare cu doi factori.

Suspendarea sau revocarea pot fi solicitate şi prin poşta electronică certificată aparţinând utilizatorului sau cu un document semnat cu o semnătură electronică calificată trimisă la adresa de e-mail certificată a furnizorului de identitate indicat pe site-ul ADR.

Pentru procedura de reactivare, a se vedea punctul 3.

3. Reactivarea are loc numai în cazul în care cerinţele în materie de asigurare stabilite înainte de suspendare sau revocare continuă să fie îndeplinite.

Statutul de revocare este ireversibil şi nu este posibilă reactivarea unei identităţi după revocarea acesteia.

Dacă utilizatorul suspendă în mod autonom identitatea, atunci se va reactiva automat în cel mult 30 de zile.

După această perioadă, identitatea este reactivată automat, cu excepţia cazului în care a fost revocată între timp.

Atunci când documentul de identitate care este furnizat în timpul procesului de înregistrare expiră, suspendarea se efectuează în mod automat de către furnizorul de identitate, iar utilizatorul este informat despre suspendare printr-un mesaj de e-mail trimis la verificarea prin e-mail în timpul procesului de înregistrare; Mesajul raportează motivele suspendării şi clarifică necesitatea actualizării datelor documentului. Până când utilizatorul nu trimite datele unui alt document valid, identitatea rămâne suspendată.

Reînnoirea şi înlocuirea

SCĂZUT ŞI SUBSTANTIAL Având în vedere riscurile unei modificări ale datelor de identificare personală, reînnoirea sau înlocuirea trebuie să îndeplinească aceleaşi cerinţe de asigurare ca dovedirea şi verificarea identităţii iniţiale sau să se bazeze pe un mijloc de identificare electronică valabil cu un nivel de asigurare identic sau superior.

RIDICAT

NIVEL SCĂZUT, PLUS:

În cazul în care reînnoirea sau înlocuirea se bazează pe un mijloc de identificare electronică, datele de identitate sunt verificate prin raportare la o sursă sigură.
La expirarea termenului de valabilitate a identității digitale, utilizatorul realizează o solicitare nouă.

2.1.1.1.3. Autentificarea

Această secțiune se concentrează pe amenințări asociate cu utilizarea mecanismului de autentificare și enumeră cerințele pentru fiecare nivel de asigurare. În această secțiune controalele trebuie să fie interpretate în așa fel încât să fie proporționale cu riscurile aferente nivelului în cauză.

Mecanismul de autentificare.
SCĂZUT

1. Eliberarea datelor de identificare personală este precedată de verificarea fiabilă a mijlocului de identificare electronică și a valabilității acestuia..
2. În cazul în care datele de identificare personală sunt stocate ca parte a mecanismului de autentificare, informațiile respective sunt securizate împotriva pierderii și a compromiterii, inclusiv prin analizarea lor offline.
3. În cadrul mecanismului de autentificare se pun în aplicare controale de securitate pentru verificarea mijloacelor de identificare electronică, astfel încât să fie foarte puțin probabil ca activități cum ar fi ghicirea, interceptarea, reproducerea sau manipularea comunicațiilor de către un atacator cu potențial de atac scăzut consolidat să poată submina mecanismele de autentificare.

PSCID oferă un singur nume de utilizator și o singură parolă aleasă de utilizator.
Toate comunicările dintre sistemul de utilizatorului și sistemul de autentificare vor fi criptate: ultimul protocol HTTPS stabil (de exemplu TLS 1.2).
În conformitate cu specificațiile SAML, interacțiunile, solicitările și răspunsurile sunt semnate digital și conțin o marcă de timp care nu poate fi modificată din cauza prezenței semnăturii SAML. Adresele URL sunt, de asemenea, scrise în metadate și nu sunt schimbate în mesaje de autentificare pentru a preveni atacurile de tip phishing.
Acreditările sunt stocate criptate (rezultatul funcției SHA-512 hashed). Accesul la citire / scriere către Serverul Directory (LDAP) este posibil numai din rețeaua internă cu acreditări de administrator.
Parolele fac obiectul unei politici de securitate după cum se specifică mai jos:

- Lungimea minimă a parolei este de 8 caractere.
- De asemenea, parola:
  - TREBUIE să conțină cel puțin un caracter alfabetic și unul numeric.
  - NU conține mai mult de două caractere identice consecutive.
  - TREBUIE să nu fie similar cu parola anterioară.
  - NU trebuie să conțină ID-ul de utilizator ca parte a parolei.
  - NU TREBUIE să fie atribuită persoanei sau datelor personale ale familiei sale.
  - TREBUIE să nu poată fi atribuită mărcilor comerciale sau denumirilor produselor.
  - TREBUIE să includă cel puțin un caracter special (#, $,%, etc.).

Parolele trebuie să fie schimbate cel puțin o dată la 180 de zile de către deținător și vor fi blocate după 5 încercări greșite.

O sesiune globală de autentificare de până la 30 de minute va fi stabilită la finalizarea autentificării tip LoA2. Autentificarea nouă către alt furnizor de servicii nu prelungeşte durata de viaţă a autentificării anterioare.
Solicitarea de logout închide sesiunea de autentificare LoA2 şi toate sesiunile individuale legate de sesiunea unică (logout unic).
Următoarea secţiune descrie modul în care vor fi implementate controalele necesare pentru a asigura conformitatea cu standardul ISO / IEC 29115 în timpul autentificării pentru sistemul de autentificare de bază (LoA2):

- Parolă puternică: utilizarea parolelor securizate este cerută de sistemul de gestionare a informaţiilor, atât în faza de creare, cât şi în faza de management;
- Verificarea confidenţialităţii credenţialelor: mecanismele de blocare şi expirare a parolei sunt aplicate conform definiţiei de mai sus, cu până la 5 încercări pentru fiecare solicitare de autentificare.
- Verificarea contului implicit: Nu sunt furnizate în aplicaţie parole sau nume de cont implicite. Utilizatorul este împiedicat să utilizeze parole care conţin date personale neconfidenţiale sau cuvinte utilizate în mod obişnuit.
- Analiza Audit: În jurnalul de aplicaţii şi în jurnalul de audit şi precum şi acordurile privind nivelul serviciilor (SLA) metrici, încercările reuşite şi nereuşite de autentificare sunt logate, permiţând aplicaţiei să ofere rapoarte care dezvăluie incercările de ghicire a parolei.
- Hash parola cu control : parolele sunt stocate sub forma unei funcţii de tip hash;
- Detectarea phishing-ului din controlul mesajelor;
- Controlul parolei: parola utilizatorului este trimisă pentru stocarea în LDAP numai atunci când se realizează acreditarea;
- Controlul autentificării criptate: toate comunicaţiile dintre Sistemul de utilizator şi cel de autentificare sunt realizate prin ultimul protocol HTTPS stabil (de exemplu TLS 1.2) şi apoi criptat;
- Controlul timestamp: interacţiunile, cererile şi răspunsurile SAML conţin o marcă de timp care nu este modificată din cauza prezenţei semnăturii obiectului SAML. Fiecare logare a sistemului de autentificare are un marcaj ce indică timpul sistemului de operare, care este controlat de protocolul NTP la sistemul de sincronizare intern al centrului de date al furnizorului de identitate IdP;
- Controlul sesiunilor criptate: toate interacţiunile dintre utilizator şi furnizorul de identitate apar pe canalul criptat HTTPS;
- Corectarea deficienţelor TCPIP: Toate comunicările dintre Sistemul de utilizator şi de autentificare sunt realizate prin intermediul serverului HTTP, actualizat şi configurat la zi pentru a atenua slăbiciunile cunoscute ale protocolului menţionat;
- Controlul codului semnăturii digitale: interacţiunile, cererile şi răspunsurile SAML sunt semnate digital, verificate la fiecare tranzacţie în conformitate cu specificaţia SAML.

SUBSTANTIAL

1. Nivelul scăzut, plus:
2. Eliberarea datelor de identificare personală este precedată de verificarea fiabilă a mijlocului de identificare electronică şi a valabilităţii acestuia printr-o autentificare dinamică.
3. În cadrul mecanismului de autentificare se pun în aplicare controale de securitate pentru verificarea mijloacelor de identificare electronică, astfel încât să fie foarte puţin probabil ca activităţi cum ar fi ghicirea, interceptarea, reproducerea sau manipularea comunicaţiilor de către un atacator cu potenţial de atac moderat să poată submina mecanismele de autentificare.

Nivelul de asigurare LoA3 realizează în mai multe moduri echivalente, la alegerea utilizatorului:

V-1

Nume de utilizator / parolă şi Parolă unică (OTP), printr-o aplicaţie disponibilă pentru dispozitivele iOS, Android. OTP are o valabilitate limitată în timp. Activarea aplicaţiei este subordonată autentificării LoA2 şi verificării dispozitivului cu un OTP prin email. Utilizarea aplicaţiei implică deblocarea utilizatorului introducând un cod PIN, cunoscut numai de utilizator, folosit pentru criptare.

V-2

Nume de utilizator / parolă şi parolă unică (OTP), generate şi afişate prin solutie software.
Fiecare OTP are valabilitate limitată în timp şi nu poate fi refolosit. OTP este utilizat pentru un singur acces şi există un număr maxim de încercări de a încerca accesul.

RIDICAT

Nivelul substanţial, plus:
În cadrul mecanismului de autentificare se pun în aplicare controale de securitate pentru verificarea mijloacelor de identificare electronică, astfel încât să fie foarte puţin probabil ca activităţi cum ar fi ghicirea, interceptarea, reproducerea sau manipularea comunicaţiilor de către un atacator cu potenţial de atac ridicat să poată submina mecanismele de autentificare.

LoA4 se realizează utilizând o autentificare cu două factori şi chei (RSA 2048) stocate pe un dispozitiv care îndeplineşte cerinţele stabilite în anexa II a Regulamentului eIDAS. SCD poate fi o cartelă inteligentă sau un token deţinut de utilizator sau un HSM gestionat de Furnizorul de Identitate Partener (care este acreditat de ADR). Este generat un certificat X.509 care conţine cheia publică.
Sistemul de autentificare pentru această categorie se bazează pe utilizarea sistemelor criptografice cu certificate digitale.

2.2. *PREVEDERI DE SECURITATE*

Tinant cont ca PSCID va reprezenta principalul punct de acces catre serviciile de eGuvernare, precum si faptul ca va gestiona date cu caracter personal, vor trebui respectate urmatoarele principii:

- **Confidenţialitate** - asigurarea protecţiei datelor împotriva acceselor neautorizate.
- **Integritate** - asigurarea protecţiei, exactitatii şi completitudinii datelor atat la nivelul modalitatii de stocare si gestionare a acestora, dar şi pentru asigurarea impotriva manipulării frauduloase a datelor/informatiilor din cadrul PSCID
- **Disponibilitate** - sistemul trebuie să asigure un proces de disponibilitate prin asigurarea redundanţei tuturor componentelor sistemului pentru a asigura utilizatorii de eventualele defecţiuni care pot surveni în timpul funcţionării precum si pentru asigurarea pastrarii coerentei si necoruperii datelor
- **Autenticitatea** - asigurarea autenticitatii partilor care participa la tranzactii
- **Ne-repudierea** - sistemul trebuie sa asigure un mecanism de prevenire a fraudelor prin care se dovedeste ca un utilizator a executat o anumita actiune.

Platforma va implementa o serie intreaga de solutii si instrumente de securitate printre care enumeram:

- Componenta de stocare centralizata a identitatilor electronice si profilelor de utilizatori

- Componenta de control al accesului si functionalitati de Single sign-On
- Asigurare posibilitatilor de autentificare folosind doi factori de tipul carduri electronice cu certificate digitale, OTP, etc.
- Posibilitatea de criptare a datelor in trafic si in modul de stocare in baza de date
- Auditarea activitatilor realizate in sistem si solicitarile de acces la serviciile de eGuvernare expuse prin intermediul platformei

3. DESCRIEREA TEHNICĂ A PROIECTULUI

3.1. *CERINȚELE FUNCȚIONALE ALE SISTEMULUI*

Principalele functionalitati care vor fi asigurate de Sistem de management al identității electronice și accesului pentru cetățenii care interacționează cu serviciile electronice puse la dispozitie de PSCID:

a) Furnizarea de servicii de management al identitatii referitoare la utilizatori, cum ar fi autentificare, federalizare și self-service utilizatori;
b) Sistemele institutiilor publice care ofera servicii electronice vor accesa infrastructura comuna PSCID pentru a sustine partajarea identitatilor, credentialelor, provizionarea, autorizarea, și servicii de audit;
c) Integrarea cu portalul unic a serviciilor electronice disponibile care se regasesc in *Catalogul Serviciilor Electronice de eGuvernare* catre cetateni cu care se va interconecta PSCID;
d) Crearea si mentinerea identitatilor electronice;
e) Stabilirea tipurilor de credentiale si eliberarea credentialelor de acces;
f) Provizionarea conturilor de utilizatori in sistemele tinta;
g) Definirea privilegiilor si serviciilor care vor fi gestionate de PSCID;
h) Stabilirea modalitatilor de autentificare;
i) Autorizare si acces la serviciile expuse prin intermediul PSCID;
j) Acces la sistemele de eguvernare prin mecanisme de tip SSO;
k) Auditarea activitatilor de accesare a serviciilor electronice si instrumente de Analiza si Raportare pe baza datelor referitoare la accesul serviciilor si utilizarea platformei;
l) Criptarea datelor sensibile atat la nivelul bazelor de date cat si in trafic;
m) Integrarea cu Cardul Electronic de Identitate, la momentul aparitiei acestuia;
n) Integrarea cu alti furnizori de identitate existenti;
o) Integrarea cu SNIEP in vederea validarii atributelor identitatii;
p) Expunerea de servicii catre terte sisteme in vederea integrarii cu furnizorii privati de servicii (ex: banci).

Printre principalele functionalitati oferite de platforma evidentiem:

a) Identificare

- **Constituirea Registrului Electronic National de Identitati Electronice** in cadrul caruia se vor regasi Identitatile Electronice ale tuturor consumatorilor de servicii electronice de eGuvernare;
- Pentru fiecare cetatean trebuie sa existe o modalitate de regasire a identitatilor electronice din sistemele tinta ale furnizorilor de servicii de eGuvernare;
- Consolidarea tuturor identitatilor electronice ale cetatenilor regasite in serviciile electronice existente.

b) Self-Service:

Pagina de auto-service pentru consumatorii de servicii electronice ar trebui sa asigure:

- Inregistrarea in PSCID a cetateanului;
- Solicitarea accesului la Serviciilor Electronice care vor fi expuse catre cetatean;
- Renuntarea la utilizarea serviciilor electronice oferite de PSCID;
- Schimbarea credentialelor de acces la serviciile electronice.

Aplicație de tip mobile pentru platformele IOS si Android care va trebui să asigure:

- Înregistrarea în PSCID a consumatorilor prin scanarea cartii de indetitate si preluarea informațiilor din MRZ (Machine Readable Zone) cu ajutorul camerei telefonului mobil;
- Verificarea în cadrul aplicației a identității consumatorilor prin compararea pozei acestora din cartea de identitate scanată cu un macanism de face comparison cu funcționalitate de "detectarea vieții";
- Schimbarea credențialelor de acces la serviciile electronice.

c) ***Provizionare:***
- Provizionarea identitatilor electronice ale consumatorilor in cadrul sistemelor tinta care furnizeaza servicii electronice;
- Provizionarea drepturilor de acces corespunzatoare serviciilor solicitate;
- Sincronizarea modificarilor asupra identitatilor electronice in sistemele tinta.

d) ***Autentificare:***
- Autentificarea consumatorilor la PSCID si federalizat la serviciile de eGuvernare
- Implementarea unei modalitati de autentificare bazata pe utilizator si parola combinata cu autentificare de tip ridicat cu token-uri software
- Autentificare de tip ridicat pe baza de smart card si certificate digitale necalificate emise de institutiile statului
- Autentificare de tip ridicat pe baza de smart card si certificate digitale calificate
- Autentificare pe baza de dispozitive/terminale mobile

e) ***Federalizare:***
- Partajarea informatiilor aferente identitatilor electronice cu furnizorii de servicii
- Asigurarea accesului federalizat la serviciile de eGuvernare utilizand solutiile deja implementate de furnizorii de servicii

f) ***Auditare si Raportare:***
- Colectarea informatiilor de auditare corespunzatoare ciclului de viata al identitatilor digitale, conturilor de utilizatori, credentialelor emise si a privilegiilor gestionate prin intermediul platformei
- Generarea de situatii statistice si de rapoarte cu privire la nivelul de utilizare al serviciilor electronice de eGuvernare prin intermediul acestei platforme.
- Rapoarte cu posibile incidente de securitate identificate

3.2. *ARHITECTURA FUNCȚIONALĂ A SISTEMULUI*

In momentul actual in cadrul fiecarui furnizor de servicii electronice de eGuvernare exista implementate diverse modalitati de definire a identitatilor digitale ale consumatorilor serviciilor, conturi de acces cu privilegii corespunzatoare solicitarilor si credentiale de acces la serviciile electronice.

Fiecare institutie publica care are un sistem ce ofera servicii electronice gestioneaza local utilizatorii si conturile de acces ale acestora la serviciile oferite.

Totodata gestioneaza si cel putin urmatoarele:
- Identitati electronice;
- Credentiale;
- Servicii de autentificare;
- Servicii de autorizare;
- Aplicatii si servicii electronice oferite;

- O solutie de management al identitatilor electronice sau de stocare a atributelor corespunzatoare conturilor de utilizatori, privilegiilor si credentialelor;
- Servicii de integrare cu furnizori de certificate digitale (emise de autoritati de certificare ale altor structuri guvernamentale sau de catre furnizori de certificate digitale calificate);

In arhitectura de mai jos se evidentiaza complexitatea utilizarii unei arhitecturi distribuite si neintegrate privind identitatile digitale ale consumatorilor in cadrul **sistemelor existente** care ofera servicii de eGuvernare.

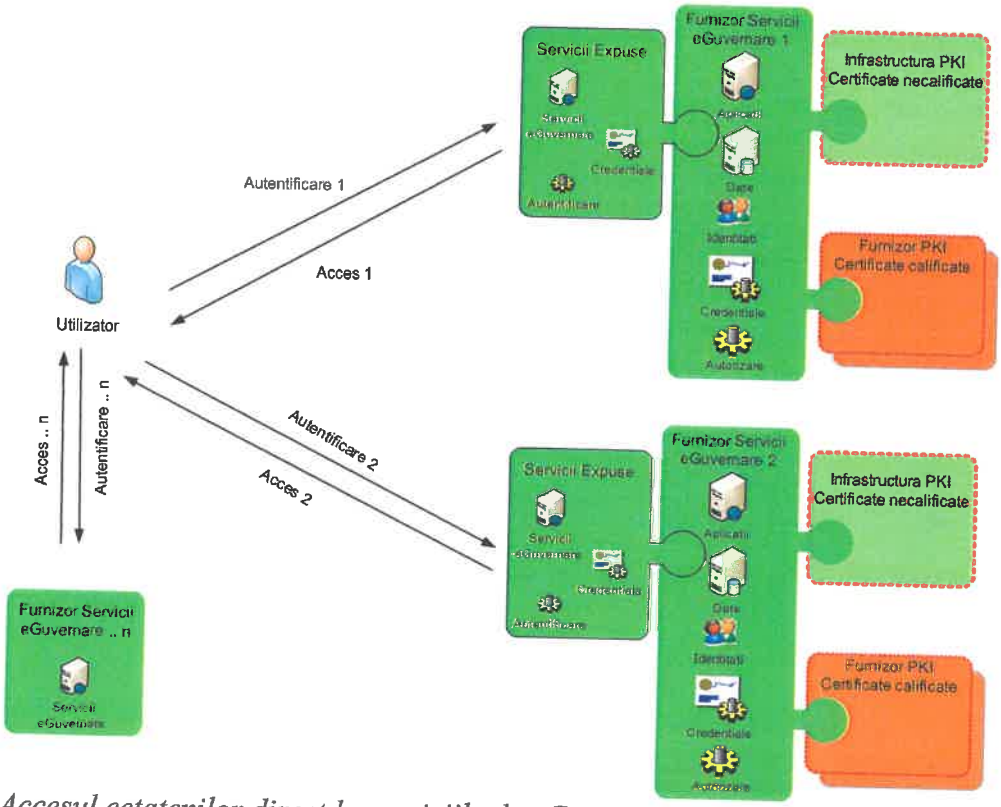


Fig. 1. Accesul cetatenilor direct la serviciile de eGuvernare expuse de furnizorii de servicii

Obiectivul PSCID este acela ca utilizatorii sa poata utiliza un singur credential sau maxim doua credentiale de tipuri diferite (certificat digital si user-parola pentru sistemele cu tehnologii invechite) în sistemele ţintă pentru a realiza o interacţiune simplificata cu serviciile electronice oferite de mai multe institutii publice.

Mai jos este prezentata arhitectura în care un utilizator este autentificat in PSCID în scopul de a accesa serviciile de eGuvernare utilizand un credential si mai departe ii este asigurat accesul la serviciile electronice oferite de institutiile publice. Infrastructura comuna PSCID permite accesul la mai multe institutii publice pe baza accesului federalizat si al relatiei de incredere stabilita intre furnizorii de servicii, furnizorul de identitate digitala si furnizorii de credentiale autorizati si de incredere .

Un alt aspect important intr-o astfel de arhitectura este acela ca in situatia in care furnizorul de servicii electronice utilizeaza credentialele emise de un tert (furnizor de certificate digitale calificate sau furnizor de certificate digitale necalificate emise de institutie publica de incredere) atunci trebuie realizata o integrare intre fiecare furnizor de servicii si furnizorii de credentiale in parte.

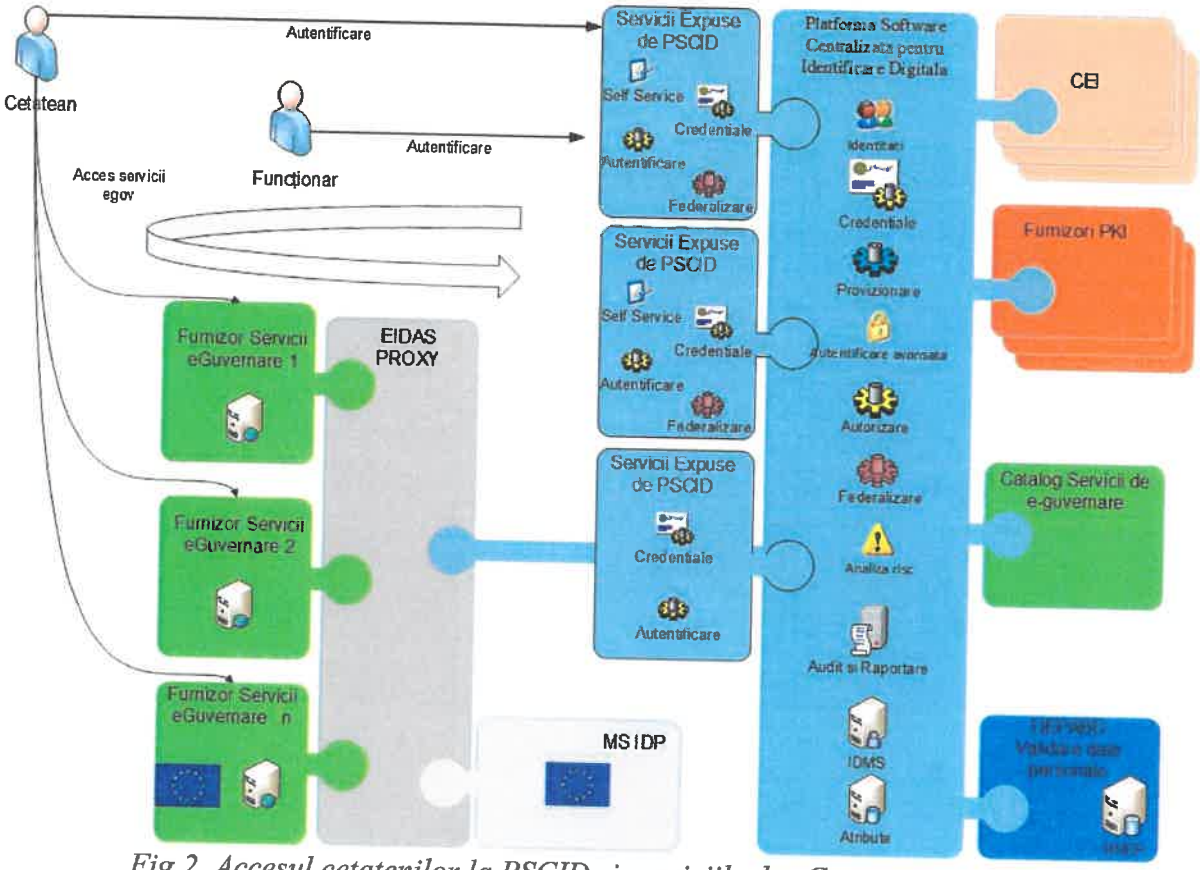


Fig.2. Accesul cetatenilor la PSCID si serviciile de eGuvernare expuse

3.2.1. Componentele arhitecturii functionale ale PSCID

Pentru asigurarea obiectivelor PSCID in cadrul platformei vor fi incluse mai multe componente si submodule impartite pe urmatoarele categorii:

- *Nivel de prezentare* – portalul şi aplicația mobile pentru platformele IOS şi Android de inregistrare a cetatenilor si de inrolare a serviciilor de eGuvernare expuse de furnizorii de servicii electronice
- *Nivel de aplicatii* – componentele de securitate pentru gestionarea identitatilor electronice, stocarea acestora in mod centralizat si de provizionare catre sistemele tinta ale furnizorilor de servicii, platforma de aplicatii si solutia de analiza si raportare
- *Nivelul de date* – componentele de stocare a datelor gestionate in cadrul platformei si de auditare a activitatilor realizate in cadrul sistemului
- *Nivel de suport* – componentele de administrare, monitorizare, backup, help desk si suport ale integului system
- *Securitate* – componentele de securizare a datelor la nivelul bazelor de date (criptare, firewall de date), auditare
- *Infrastructura hardware si de comunicatii* – infrastructura de servere, echipamente de stocare si comunicatii necesare rularii platformei

Principalele componente functionale de securitate si de suport ale platformei sunt:

- Componenta de **portal** prin intermediul careia se expun catre cetateni serviciile PSCID
- O solutie de **management al identitatilor electronice** care va asigura procesele:

- Creare si mentenanta identitatilor digitale, inclusiv prin intermediul aplicației mobile
- Provizionarea conturilor de utilizatori in sistemele care expun serviciile de eGuvernare
- Provizionarea drepturilor de acces ale utilizatorilor in sistemele care expun serviciile de eGuvernare
- Self-service - asigurarea proceselor de:
  - solicitare directa a accesului la servciile electronice expuse prin PSCID
  - resetare credentiale de acces
- Auditarea si raportarea informatiilor corespunzatoare proceselor executate in cadrul solutiei

- O solutie de **management al acceselor** care va asigura procesele:
  - Definirea privilegiilor si serviciilor care vor fi gestionate de PSCID
  - Validarea credentialelor (inclusiv certificatelor digitale prin solutii de tip OCSP/CRL)
  - Autorizare si acces la serviciile electronice
- O solutie de **stocare centralizata a profilelor de utilizatori** aferente identitatilor digitale **(atribute, roluri, grupuri, etc.)** care va asigura stocarea centralizata a tutror informatiilor corespunzatoare conturilor de utilizatori, a credentialelor utilizate si a permisiunilor acordate la rolurile mapate pe privilegiile definite in cadrul sistemelor tinta
- O solutie de **autentificare securizata** care sa permita utilizarea de credentiale de tipul dispozitive de autentificare virtuale (token/software de tip onetime password, etc) si instrumente de anti-malware si anti-phishing prin care utilizatorul certifica ca serviciul utilizat este autentic (prin personalizare) si se asigura securitatea autentificarii impotriva atacurilor
- O componenta de **analiza si raportare** a informatiilor de identitate digitala gestionate in cadrul PSCID.
- O componenta de gestiune a informatiilor de **auditare** legate de definire identitati, provizionarea acestora si acordare de drepturi identitatilor digitale gestionate in cadrul PSCID.
- Sistem de **gestiune a bazelor de date** in cadrul careia se vor stoca toate instantele bazelor de date aferente modulelor functionale si portalului;
- **Solutii de securitate** impotriva accesului neautorizat sau incercari de fortare a accesului la datele aferente identitatilor electronice.
- Componentele suport ale sistemului de **administrare, monitorizare, asigurarea procedurilor de salvare** a datelor si aplicatiilor platformei si componentele **de help desk** si **suport**.

3.2.2. Arhitectura tehnică

Din punct de vedere tehnic arhitectura PSCID va fi constituita din solutii redundante in toate subcomponentele sistemului cu cate doua noduri alocate fiecarei componente in parte astfel:

- Solutie cu asigurarea disponibilitatii si balansarea incarcarii (cluster activ-activ) pentru toate componentele functionale ale sistemului:
  - servere web si poarta securizare servicii electronice
  - portal
  - analiza si raportare
  - managementul identitatilor electronice
  - managementul acceselor
  - stocare centralizata a profilelor de utilizatori aferente identitatilor digitale (LDAP)
  - Sistem de gestiune a bazelor de date in cadrul careia se vor stoca toate instantele bazelor de date aferente modulelor functionale si portalului;
- Solutie cu asigurarea disponibilitatii de tip failover (cluster activ-pasiv) pentru componentele de securitate si suport:
  - auditare
  - firewall de baze de date
  - administrare si monitorizare
  - salvare (backup)

Pentru asigurarea functionarii in bune conditii a performantei PSCID vor fi asigurate următoarele medii:

a) **Mediul de producţie** - asigura funcţionarea în producţie a PSCID si reprezinta mediul care va fi utilizat in mod direct de catre cetateni si institutiile publice pentru definirea identitatilor electronice si furnizarea serviciilor electronice expuse prin intermediul platformei;

b) **Mediul de dezvoltare** si **testare** – asigura mediul pe care vor fi dezvoltate si apoi testate toate componentele dezvoltate ale sistemului intr-un mod integrat, inainte ca acestea sa fie trecute in productie.

Ambele medii vor avea aceeasi arhitectura tehnica din punct de vedere al numarului de noduri si modalitatea de asigurare a disponibilitatii si scalabilitatii sistemului, diferenta fiind doar de dimensionare a acestor medii.
Mediul de productie va fi dimensionat fara limitarea din punct de vedere al licentierii pe infrastructura hardware minima solicitata, iar acolo unde diferite solutii au alta metrica sau modalitate de licentiere, infrastructura software va trebui sa asigure:

- **un minim de 10.000.000 de utilizatori inregistrati;**
- **pentru a mentine nivelul de performanta si concurenta ridicat, sistemul trebuie sa mentina request-urile de autentificare intr-o coada de asteptare;**
- **consumul request-urilor de autentificare se va face in functie de capacitatea maxima a sistemelor terte cu care se va integra;**
- **pentru minim de 500 utilizatori concurenti sistemul trebuie sa asigure un timp de confirmare al solicitarii de autentificare de maxim 100 ms. Autentificarea efectiva se va face in functie de capacitate si nivelul de performanta al sistemului tert;**
- **pentru un numar de utilizatori concurenti mai mare de 500 de utilizatori si mai mic de 2.000 de utilizatori sistemul trebuie sa asigure un timp de confirmare al solicitarii**

de autentificare de maxim 200 ms; Autentificarea efectiva se va face in functie de capacitate si nivelul de performanta al sistemului tert;

- **pentru un numar de utilizatori concurenti mai mare de 2.000 de utilizatori si mai mic de 10.000 de utilizatori sistemul trebuie sa asigure un timp de confirmare al solicitarii de autentificare de maxim 1 secunda; Autentificarea efectiva se va face in functie de capacitate si nivelul de performanta al sistemului tert;**
- **pentru un numar de utilizatori concurenti mai mare de 10.000 sistemul trebuie sa afiseze un mesaj utilizatorului prin care sa fie informat asupra nivelului ridicat de utilizare a sistemului, iar timpul de confirmare al solicitarii de autentificare va fi ridicat.**

Mediul de dezvoltare si testare va fi dimensionat pentru asigurarea unui numar minim de 50 de utilizatori.

Tinand cont de sensibilitatea datelor si nivelului de securitate solicitat in cadrul proiectului cat si de asigurarea de catre producatori a suportului tehnic pentru toate componentele functionale, de securitate si suport ale platformei, furnizorul este solicitat să ofere versiunea comercială (COTS) pentru tot software-ul standard. Pentru software-ul standard furnizat va trebui sa fie asigurat minim 3 ani de suport oferit de catre producatorul acestuia.
Componente functionale (portal, aplicaţie mobile, management identitatilor si controlul accesului, LDAP, BI) si soluţiile de securitate (audit, firewall, PKI), vor avea asigurate servicii furnizate de producător (pentru a asigura implementarea cu succes a proiectului care este unul de interes national si pentru a asigura o arhitectura care permite integrarea cu alte sisteme şi servicii electronice naţionale).
Pentru a reduce complexitatea arhitecturii, precum şi costurile administrative şi operaţionale, platforma de aplicatii propusa trebuie să fie pe deplin integrata la nivelul componentelor de management a fluxurilor si proceselor de emitere, aplicaţii software personalizate pentru acest sistem.
Sistemul informatic central va fi proiectat astfel încat să funcţioneze în regim de înaltă performanţă şi disponibilitate şi va fi separat pe trei niveluri, conform celor mai bune practici în domeniu: stocarea datelor, prelucrare şi prezentare.

3.3. *MANAGEMENTUL UTILIZATORILOR ŞI ACCESUL LA SISTEM*

Prezentul proiect reprezinta implementarea la nivel national a modalitatii de definire a identitatilor electronice ale cetatenilor si modalitatii de definire a accesului acestora la sistemele si serviciile electronice de eGuvernare.
In cadrul serviciilor de eGuvernare oferite in prezent de diferite institutii publice exista implementate mai multe modalitati si solutii de asigurare a accesului la serviciile electronice care sunt strans legate de sistemele informatice ce ofera aceste servicii. De regula un sistem este configurat sa permita utilizarea unui singur tip de credential, iar credentialele cele mai des utilizate sunt cele de tipul *nume utilizator/parola*.
Prin intermediul PSCID se vor asigura pe langa autentificare bazata pe credentiale de tipul ID-uri de utilizatori/parole si suportul pentru credentiale de tip certificate digitale stocate pe token-uri/smartcard-uri hardware si o solutie de *autentificare securizata* care sa permita:

- utilizarea de credentiale de tipul dispozitive de autentificare virtuale (token/software de tip onetime password, etc)

- instrumente de protejare impotriva anti-malware si anti-phishing prin care utilizatorul certifica ca serviciul utilizat este autentic, prin personalizarea paginii de autentificare de pe server, asigurandu-se astfel securitatea autentificarii impotriva atacurilor de tip furt de identitate

Asigurarea managementului utilizatorilor reprezinta una dintre functionalitatile oferite de aceasta platforma de securitate si asigura in principal:

- identificarea în mod unic a fiecarui cetatean in sistem prin crearea unei identitati electronice unice in cadrul sistemului si definirea de conturi unice si personalizate de acces;
- accesul utilizatorilor la PSCID se va realiza doar prin autentificarea utilizatorilor. Vor exista informatii de interes public publicate in portal care nu vor necesita autentificare, dar utilizarea oricarui serviciu oferit prin portal va fi asigurat doar dupa selectarea modalitatii de autentificare si prezentarea credentialelor de acces;
- gestionarea centralizata si unitara a accesului utilizatorilor in sistem prin asigurarea autorizarii utilizatorilor la PSCID si componentele si modulele functionale ale acesteia conform cu drepturilor de acces definite.

Asigurarea accesului la sistem se va realiza diferentiat pe diferitele tipuri de utilizatori (cetateni, operatori, administratori, sau reprezentanti ai institutiilor care expun prin PSCID servicii electronice), astfel ca PSCID va:

- expune cerinţele de securitate ale serviciilor electronice expuse prin portal;
- solicita utilizatorilor să se identifice unic si sa se autentifice înainte de a utiliza orice functionalitate oferita de sistem fie prin certificate calificate fie prin user-parola si OTP;
- avea capabilităţi de criptare a datelor atat in trafic cat si la stocarea acestora atat in baza de date cat si pe disc;
- asigura Single-Sign On pentru accesul la serviciile oferite de PSCID dupa autentificarea utilizatorilor;
- avea capabilitatea de loga operaţiile si tranzacţiile realizate de fiecare utilizator autentificat în cadrul componentei de audit;
- avea capabilitatea de a înregistra evenimente definite de securitate şi definirea de tipuri de alerte catre administratorii de securitate.

Pentru asigurarea autorizarii si asigurarii accesului vor fi definite o serie de fluxuri si procese prin intermediul carora se va asigura accesul la serviciile electronice si datele corespunzatoare acestora. Aceste procese sunt strict legate si depind de procesele de creare a identitatii digitale, de definire a credentialelor si de provizionare a conturilor de utilizatori pentru a putea asigura autorizarea si accesul acestora. Procesul de accesare a serviciilor utilizeaza identitatile si credentialele deja create in procesele mentionate anterior.
Pentru asigurarea accesului cetatenilor este foarte important ca institutiile publice sa adopte modelul identitatilor federalizate, sa accepte credentialele emise de alte institutii ale statului pentru accesarea prin intermediul PSCID. Scopul final pentru consumatorii serviciilor electronice este acela de a avea acces la aceste servicii utilizand un numar limitat de credentiale de autentificare si reutilizarea credentialelor existente si emise de alt furnizor de identitati. Pe termen mediu este de asteptat ca utilizatorii serviciilor din sectorul privat (G2B) sa utilizeze doar certificate digitale calificate emise de funizori acreditati.

Atingerea obiectivelor PSCID necesita unele schimbari la nivelul arhitecturilor curente:

- **Implementarea sistemului de control al accesului centralizat in PSCID** - O modalitate flexibila si gestionata centralizat in cadrul PSCID este necesara pentru a stratifica atributele si permisiunile, si maparea acestora pe mecanismele de autentificare pentru a putea lua decizii asupra accesarii tuturor serviciilor electronice.
- **Adoptarea modelului Federalizat** – va fi necesar stabilirea unor acorduri privind tehnologiile, formatele, versiunile si mecanismele de supraveghere pentru asigurarea increderii si transferului de identitati si credentiale in afara granitelor unei institutii guvernamentale. Stabilirea Furnizorilor de Identitati de incredere si de mecanisme similare va permite furnizorilor de servicii sa ia decizii privind accesul pe baza nivelului de incredere definit.

3.4. *SECURITATEA SISTEMULUI*

Datorita sensibilitatii datelor vehiculate in sistemul PSCID pentru asigurarea indeplinirii cerintelor de securitate legate de constrangerile privind lucrul cu date cu caracter personal, vor trebui respectate urmatoarele principii:

- **Confidenţialitate** - asigurarea protecţiei datelor împotriva acceselor neautorizate.
- **Integritate** - asigurarea protecţiei, exactitatii şi completitudinii datelor atat la nivelul modalitatii de stocare si gestionare a acestora, dar şi pentru asigurarea impotriva manipulării frauduloase a datelor/informatiilor din cadrul PSCID
- **Disponibilitate** - sistemul trebuie să asigure un proces de disponibilitate prin asigurarea redundanţei tuturor componentelor sistemului pentru a asigura utilizatorii de eventualele defecţiuni care pot surveni în timpul funcţionării precum si pentru asigurarea pastrarii coerentei si necoruperii datelor
- **Autenticitatea** - asigurarea autenticitatii partilor care participa la tranzactii
- **Ne-repudierea** - sistemul trebuie sa asigure un mecanism de prevenire a fraudelor prin care se dovedeste ca un utilizator a executat o anumita actiune.

Prin specificul si obiectivele acestui proiect se va asigura controlul centralizat al tuturor aspectelor legate de securitate (autentificare, autorizare, auditare, etc).

Ca si functionalitati care trebuie indeplinite pentru respectarea cerintelor de securitate vor fi asigurate:

- Fiind un sistem de securitate, solutiile implementate vor asigura functionarea platformei în condiţii de maxima siguranţă, asigurand instrumente de inventariere şi evaluare a riscurilor specifice, minimizarii sau contracararii acestora, atat prin măsuri si proceduri de lucru cat si prin solutii si instrumente informatice;
- Securitatea sistemului va fi administrată centralizat şi va dispune de mecanismele de administrare şi monitorizare a funcţionării infrastructurii;
- Autentificarea si controlul accesului utilizatorilor in sistem se va realiza in mod centralizat si integrat.

Implementarea unui proiect de o asemenea anvergura, complexitate si nivel de securitate necesar impune mai multe tipuri de politici de securitate:

- La nivel fizic se vor folosi politicile de securitate implementate in cadrul ADR
- La nivel de utilizatori prin pastrarea identitatilor electronice ale acestor centralizat in cadrul sistemului impreuna cu privilegiile acordate si modalitatea de access definita pentru fiecare serviciu electronic in parte

- La nivel de aplicatie prin auditarea tuturor activitatilor efectuate in sistem si asupra datelor gestionate de acesta.

Pentru gestiunea sistemului de certificate digitale, se va realiza integrarea sistemului propus cu sistemele de tip PKI deja existente in cadrul institutiilor partenere.

3.4.1. Auditare

Prin implementarea in cadrul PSCID a componentei de auditare, toate solicitarile de acces dar si accesele de utilizare a serviciilor de eGuvernare vor fi auditate.
Principalele informatii de auditare privind datele corespunzatoare identitatilor digitale si acceselor la serviciile de eGuvernare vor fi:

- Solicitari de emitere a identitatilor digitale;
- Solicitari de emitere a credentialelor aferente identitatilor digitale pentru accesarea serviciilor de eGuvernare;
- Solicitari de acordare a privilegiilor de acces la serviciile de eGuvernare;
- Accesari sau incercari de accesare a serviciilor de eGuvernare;
- Solicitari de schimbare a informatiilor corespunzatoare identitatilor digitale;
- Solicitari de schimbare credentialelor corespunzatoare identitatilor digitale;
- Solicitari de schimbare privilegiilor de acces;
- Terminari/revocari unei identitati digitale, a credentialelor de acces si a privilegiilor corespunzatoare.

3.4.2. Criptare

In cadrul PSCID criptarea reprezinta un element important tinand cont ca informatiile corespunzatoare identitatilor digitale, a privilegiilor corespunzatoare acestora si a credentialelor atasate acestor identitati sunt informatii foarte sensibile si informatii cu caracter personal. Criptarea este utilizata pentru a nu permite accesul neautorizat la informatiile confidentiale in cadrul tuturor componentelor arhitecturale:

- La nivelul bazelor de date care stocheaza datele de identitate digitala si credentialele aferente acestora
- In cadrul accesului federalizat intre PSCID si furnizorii de servicii electronice pentru transmiterea informatiilor de identitate

Pentru utilizatorii care detin credentiale de tip certificate digital (calificat si necalificat), pe langa criptarea canalului de comunicare se poate impune si autentificarea mutuala intre platforma si utilizatori care se bazeaza pe semnarea digitala a unor date de tip hash la momentul deschiderii sesiunii intre cele doua parti.

3.5. *CONFIDENȚIALITATEA DATELOR*

Tinand cont de nivelul de securitate necesar pentru implementarea unei astfel de solutii de management a identitatilor electronice ale cetatenilor, pentru asigurarea confidenţialitatii datelor si informaţiilor prelucrate, PSCID trebuie sa asigure:

- implementarea unei arhitecturi si infrastructuri software si hardware care să asigure stabilitatea, integritatea şi disponibilitatea datelor.

- criptarea datelor atat in trafic, prin securizarea comunicatiilor cat si in modul de stocare a acestora atat la nivelul bazei de date cat si disk, pentru acele date care se considera ca este necesar a fi protejate.

Solutiile de securitate solicitate in cadrul PSCID vor trebui sa asigure confidentialitatea datelor si aceasta va fi sustinuta de urmatoarele aspecte:

- Identitatile electronice (cu toate atributele corespunzatoare acestora), conturile de utilizatori corespunzatoare vor fi stocate intr-un sistem central.
- Autentificarea utilizatorilor in sistem se va face in mod unic, pe baza de conturi de utilizatori unice si pe baza de metode de autentificare pe baza de parole sau certificate digitale
- Autorizarea utilizatorilor se va face pe baza drepturilor de utilizare a serviciilor electronice la care au solicitat si au primit drept de utilizare.
- Actiunile in cadrul sistemului (acces, scriere, modificare, stergere, etc) efectuate atat de cetateni cat si de administratorii sistemului sunt auditate in sistemul de audit. Accesul in sistemul de audit va fi restrictionat doar operatorilor si administratorilor de securitate si doar in mod controlat, pe baza respectarii principiului nevoii de a cunoaste.

Soluţia propusă trebuie să asigure confidenţialitatea informaţiilor, ceea ce reprezintă o misiune critică. Informaţia dintr-un astfel de sistem trebuie protejată împotriva ameninţărilor în orice situaţie, fie când este stocată, fie când este transportată.

Pe lângă cerinţele enunţate mai sus, platforma şi instrumentele pentru asigurarea confidenţialităţii datelor trebuie:

- Să ofere suport pentru criptarea transparenta a datelor care sunt stocate în baza de date, la nivel de coloană, tabelă sau tablespace.
- Să realizeze criptarea traficului prin reţea între utilizator, aplicaţia de business şi baza de date, pentru a elimina posibilele încercări de interceptare a datelor când sunt transmise în mediile de comunicaţie.
- Să asigure confidenţialitatea informaţiilor vehiculate în conformitate cu modul de exploatare, pe verticală şi pe orizontală, a resurselor informaţionale ale sistemului.
- Să blocheze încercarea de utilizare neautorizată de resurse, servicii sau informaţii, să înregistreze evenimentul într-un fişier sau tabelă de supraveghere şi să semnaleze în timp real aceste evenimente personalului administrativ.
- Să nu permită persoanelor neautorizate modificarea sau alterarea semantică a informaţiilor.
- Să asigure calitatea şi consistenţa datelor, să facă identificarea sursei datelor iniţiale şi persoanele ce au introdus datele iniţiale.
- Să asigure posibilitatea de a restricţiona accesul utilizatorilor privilegiaţi (DBA) la datele manipulate de aplicaţiile de business, prin segregarea responsabilităţii.
- Să asigure posibilitatea de a defini factori de acces pentru a permite accesul la informaţii. Aceşti factori trebuie să includă: perioada din zi, tipul de acţiune, locaţia sau alţi factori personalizaţi.
- Să permită protejarea informaţiei stocate în baza de date la nivel de linie, prin oferirea accesului doar la un subset de informaţii pe baza rolului şi responsabilităţilor acelui utilizator.
- Să ofere suport pentru clasificarea datelor în cadrul bazei de date, astfel încât un utilizator să aibă acces doar la datele care corespund nivelului său de clasificare.

3.6. *ARHITECTURA TEHNICA*

Fig. 3 Arhitectura fizica PSCID

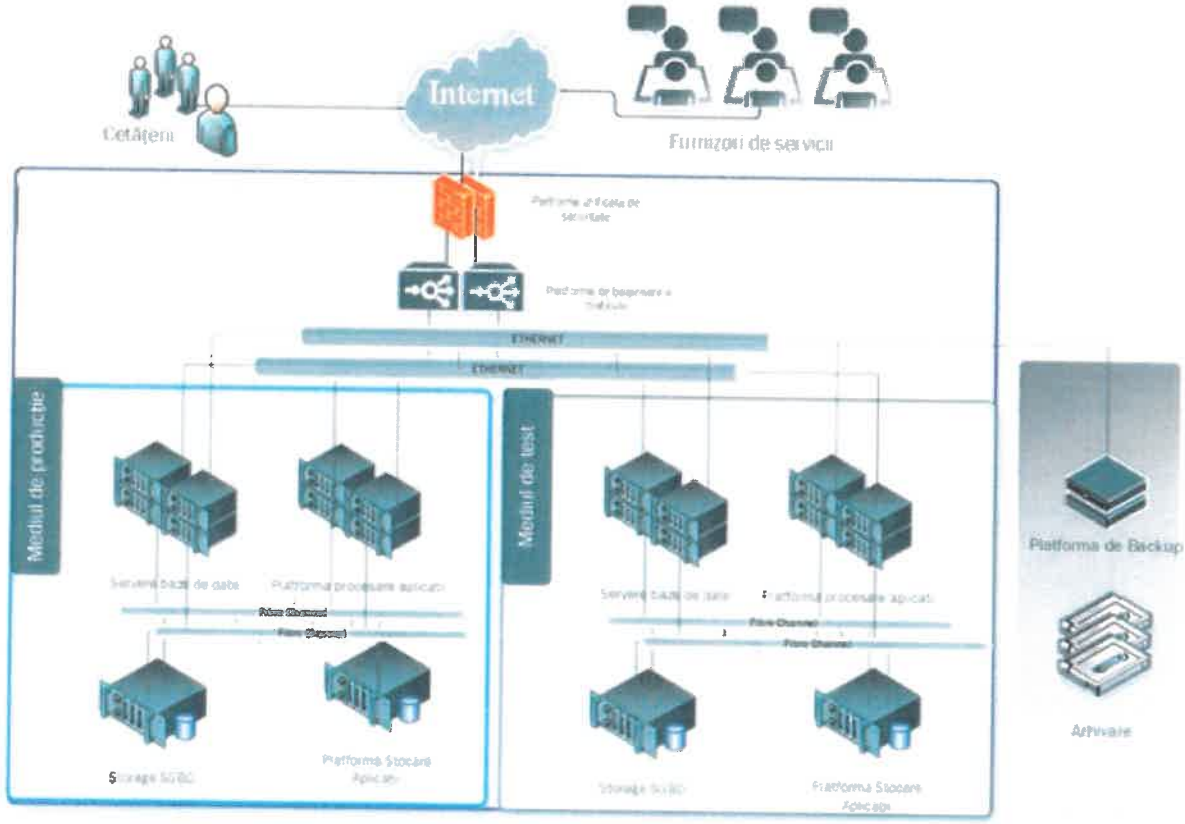
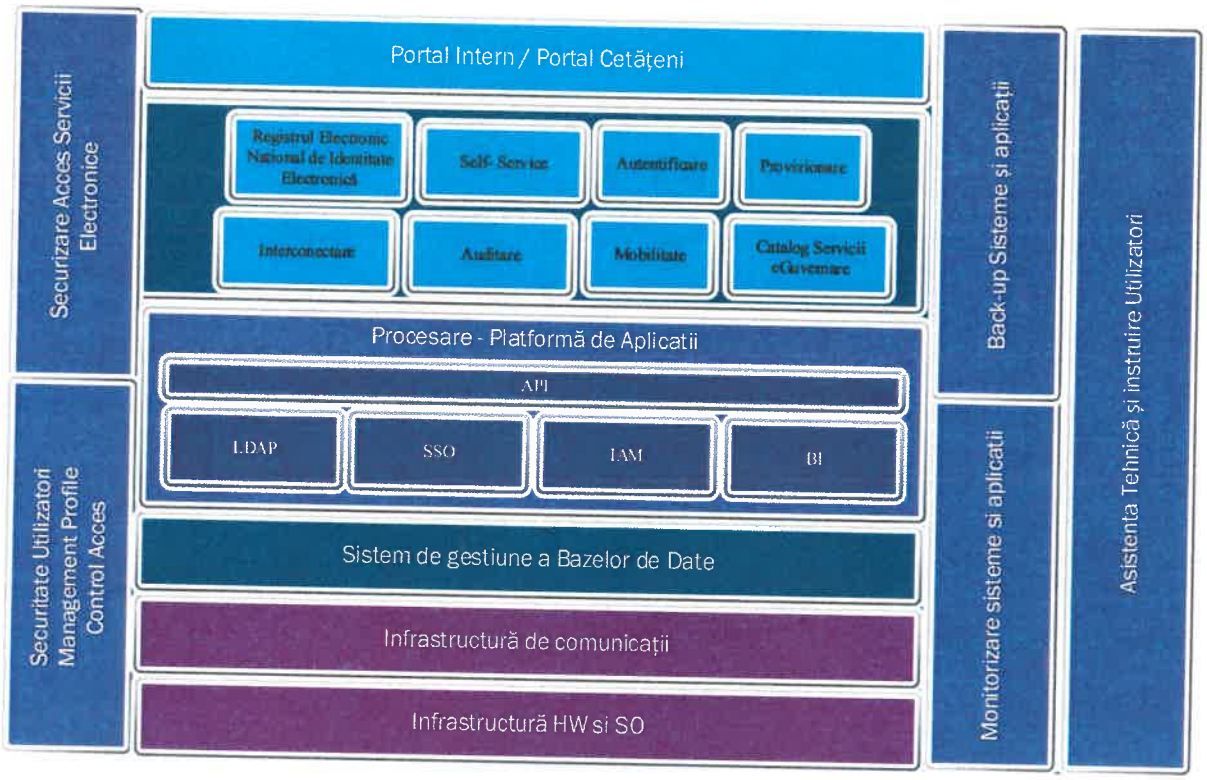
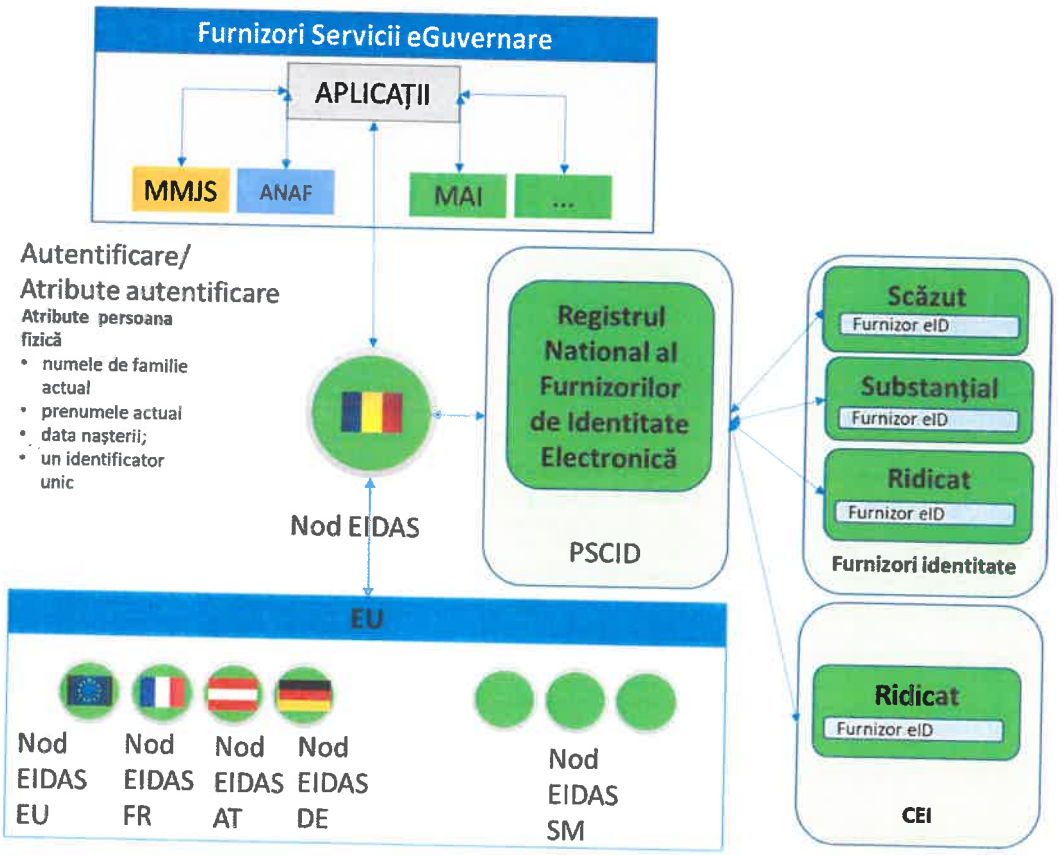
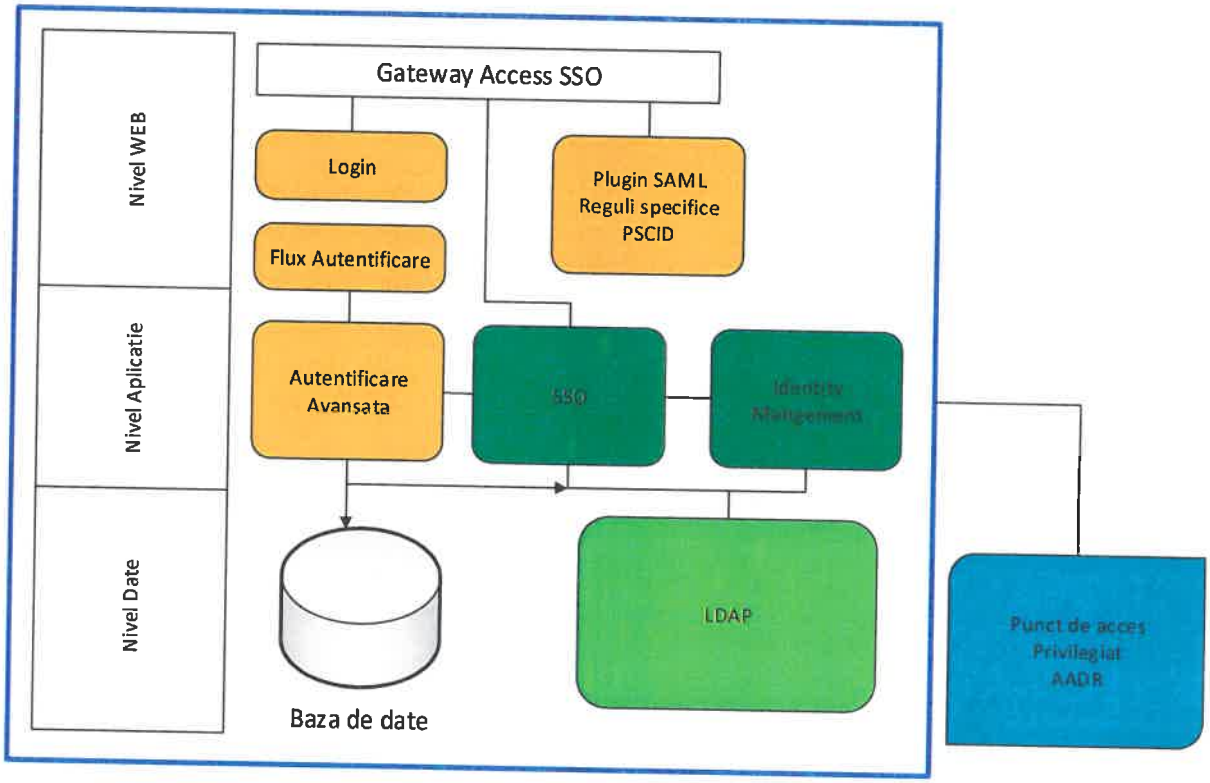


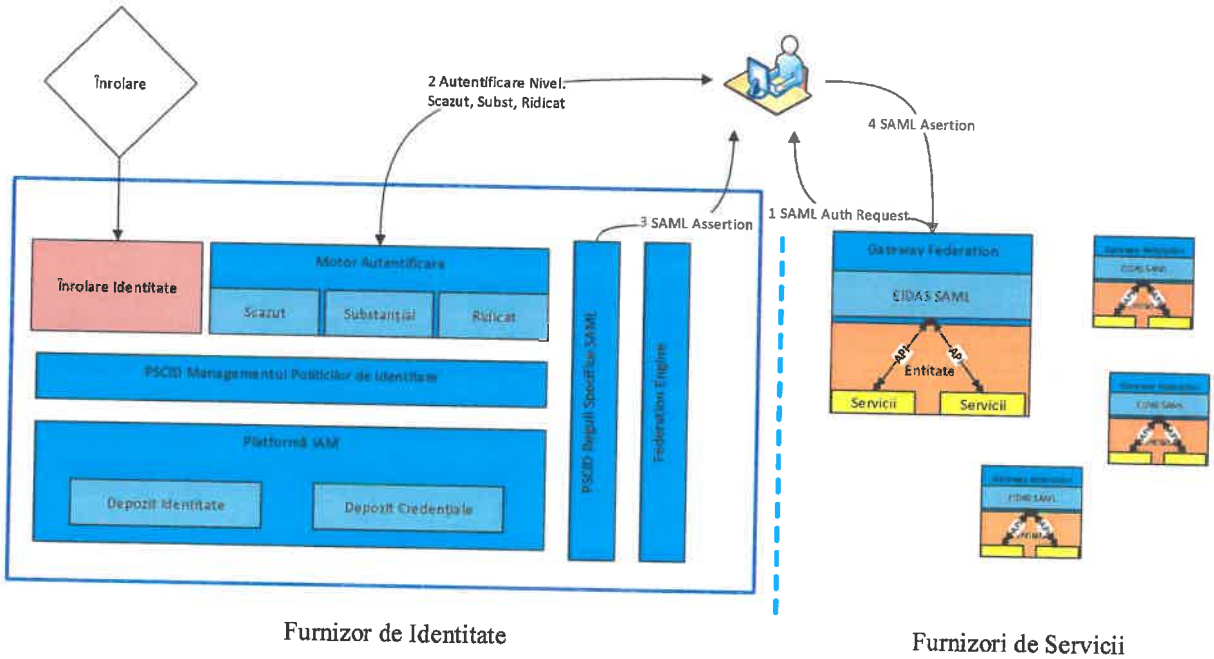
Fig. 4 Arhitectura logica PSCID


Securizare Acces Servicii Electronice
Portal Intern / Portal Cetățeni
Registrul Electronic National de Identitate Electronică
Self-Service
Autentificare
Provizionare
Interconectare
Auditare
Mobilitate
Catalog Servicii eGuvernare
Procesare - Platformă de Aplicatii
API
LDAP
SSO
IAM
BI
Sistem de gestiune a Bazelor de Date
Infrastructură de comunicații
Infrastructură HW si SO
Securitate Utilizatori Management Profile Control Acces
Back-up Sisteme și aplicații
Monitorizare sisteme si aplicatii
Asistenta Tehnică și instruire Utilizatori


Furnizori Servicii eGuvernare
APLICAȚII
MMJS
ANAF
MAI
...
Autentificare/
Atribute autentificare
Atribute persoana fizică
• numele de familie actual
• prenumele actual
• data nașterii;
• un identificator unic
Nod EIDAS
Registrul National al Furnizorilor de Identitate Electronică
PSCID
Scăzut
Furnizor eID
Substanțial
Furnizor eID
Ridicat
Furnizor eID
Furnizori identitate
EU
Nod EIDAS EU
Nod EIDAS FR
Nod EIDAS AT
Nod EIDAS DE
Nod EIDAS SM
Ridicat
Furnizor eID
CEI

Modul Furnizor de identitate



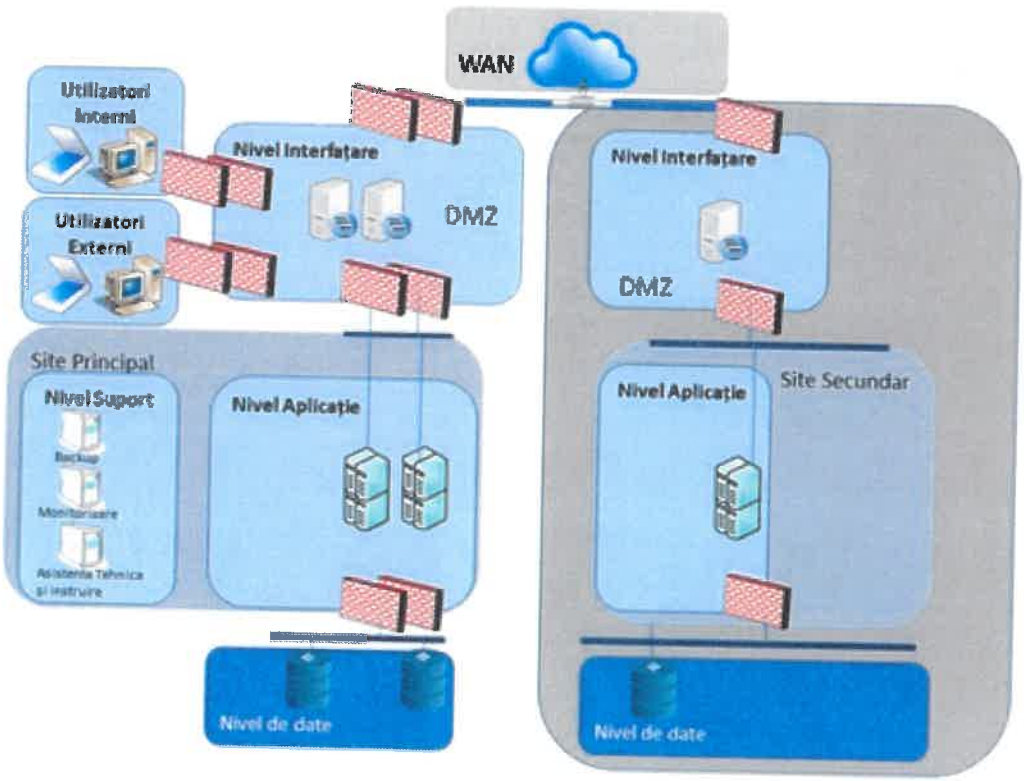


Furnizor de Identitate

Furnizori de Servicii

Fig. 5 Arhitectura DR

La momentul in care cloud-ul guvernamental va fi pus in productie, ADR va configura un site de tip Disaster Recovery pentru PSCID, la aceleasi capacitati cu cele ale mediului de productie. Configurarea site-ului secundar nu intra in spectrul cerintelor prezentei documentatii de atribuire.



3.6.1. Dimensionarea componentelor functionale si a celor de suport ale mediului de productie

Dimensionarea componentelor functionale si a celor de suport ale mediului de productie va trebuie sa asigure minimul de resurse de procesare dupa cum urmeaza:

Nr. crt.	Componenta	Numar minim de noduri	Disponibilitate minima	Numar core-uri fizice minime pe nod	Memorie RAM (GB) minim necesara per nod
1.	Portal	2	Cluster Activ-Activ	16	128
2.	Server web/Reverse proxy	2	Cluster Activ-Activ	8	64
3.	SGBD	2	Cluster Activ-Activ	16	256
4.	Analiza si Raportare – BI	2	Cluster Activ-Pasiv	16	256
5.	Securitate Utilizatori: Managementul profilelor Control acces LDAP Securizare acces servicii electronice Componenta de autentificare securizată a utilizatorilor Platforma de balansare a traficului de aplicatie	2	Cluster Activ-Pasiv	72	512
6.	Monitorizare date, sisteme si aplicatii	1		24	128
7.	Asistenta tehnica	1		12	128
8.	Monitorizarea logurilor si a traficului de retea (poate fi si HW appliance)	1		64	256
9.	Componenta de mascare a datelor	1		16	128
10.	Componenta de securizare a accesului la bazele de date	2	Cluster Activ-Pasiv	16	128
11.	Backup	1		16	64

3.7. *COMPONENTE HARDWARE SI DE COMUNICATII*

Cerintele minime pentru echipamentele hardware si de comunicatii sunt:

Nr.	Descriere	Cantitate
1.	Suport fizic de tip rack pentru montarea şi poziţionarea echipamentelor	5
2.	Consola de management general al echipamentelor de procesare	2
3.	Suport alimentare independenta si disponibilitate operationala - Surse neîntreruptibile (UPS)	5
4.	Platforma de procesare aplicaţii pentru mediul de productie	2
5.	Platforma de procesare aplicaţii pentru mediul de test/dezvoltare	1
6.	Echipamente de procesare aplicaţii pentru mediul de productie	14
7.	Echipamente de procesare aplicaţii pentru mediul de test/dezvoltare	10
8.	Platforma de interconectare - Echipamente de comunicatie si interconectare integrate in sasiu – Ethernet 10 Gbps	6
9.	Platforma de interconectare - Echipamente de comunicatie si interconectare integrate in sasiu – Fibre Channel	6
10.	Platforma de interconectare - Echipamente de comunicatie SAN – Fibre Channel	4
11.	Platforma de interconectare - Echipamente de comunicatie pentru interconectare interna - Ethernet 10 Gbps	2
12.	Platforma de stocare pentru baza de date si aplicaţii pentru mediul de productie/testare/dezvoltare	1
13.	Platforma de balansare a traficului de aplicatie	2
14.	Platforma unificată de securitate	2

Solutia ofertata trebuie sa respecte urmatoarele **cerinte generale**:

- Sistemele si echipamentele livrate trebuie sa fie noi, neutilizate si de ultima generatie. Ele trebuie sa asigure gradul necesar de performanta, fiabilitate si flexibilitate fiind proiectate si destinate pentru aplicatii critice de tip "enterprise level";
- Dispozitivele hardware trebuie sa fie astfel proiectate incat sa poata asigura scalabilitatea sistemului in cazul cresterii ulterioare a necesarului de resurse de calcul;
- Dispozitivele hardware trebuie sa fie compatibile cu caracteristicile retelei electrice din Romania astfel incat sa fie garantata conectarea fara probleme a acestora la reteaua electrica existenta a beneficiarului;
- Ofertantul va preciza care este greutatea totala a echipamentelor livrate si dimensiunile fizice ale acestora pentru a se putea verifica siguranta instalarii in locatia beneficiarului;
- Ofertantul va preciza in oferta care este puterea totala consumata de echipamentele livrate precum si caracteristicile de climatizare/ventilatie necesare, astfel incat beneficiarul sa poata asigura acest necesar in locatia unde urmeaza a fi instalate echipamentele;

- Toate aceste cerinte sunt dezvoltate la nivel de detaliu in cadrul documentatiei de atribuire. In acelasi timp cerintele nu sunt limitative ofertantii avand libertatea de a le dezvolta si extinde conform solutiei pe care o au in vedere sa o propuna si care trebuie să îndeplinească în totalitate cerintele beneficiarului;
- Ofertantii vor avea în vedere că toate cerintele si caracteristicile solicitate explicit pentru solutia propusa in cadrul documentatiei de achizitie au un caracter minim si obligatoriu.

Aplicatiile si serviciile ce vor alcatui intreaga solutie trebuiesc dimensionate optim in functie de necesarul de putere de procesare, spatiu de stocare, latenta si viteza mediilor de comunicatie, cerintele de securitate corespondente fiecarui nivel fizic si logic de infrastructura, aplicatii, servicii.

Avand in vedere prevederile Ordinului nr. 1068/1652/2018 din 4 octombrie 2018 pentru aprobarea Ghidului de achiziții publice verzi care cuprinde cerințele minime privind protecția mediului pentru anumite grupe de produse și servicii ce se solicită la nivelul caietelor de sarcini, Ofertantul va da o declarație scrisă în care va indica substanțele specifice prezente (substanțe înscrise pe lista REACH a substanțelor candidate cu o concentrație mai mare de 0,1% (procent de masă)) în întregul produs și în fiecare dintre următoarele subansambluri:

- placă de bază cu circuite, inclusiv CPU, RAM, unități grafice;
- unitate de afișaj, inclusiv retroiluminare;
- carcase și rame;
- tastatură externă, mouse și/sau trackpad;
- cabluri externe de alimentare cu curent continuu și curent alternativ, inclusive adaptoare și surse de alimentare.

3.7.1. Suport fizic de tip rack pentru montarea și poziționarea echipamentelor – 5 buc

Ansamblu modular standard de 19 inchi, cu 42U disponibili pentru pozitionarea echipamentelor.Se vor include reperele de montare necesare, inclusiv șine extensibile telescopic (sau soluții similare) cel puțin pentru echipamentele complexe de natura nodurilor de procesare, în scopul de a permite accesul fizic facil la componentele interne de tip hot-plug / hot-swap (surse, ventilatoare, plăci de extensie etc.) și deservirea acestora fără a fi necesară oprirea funcționării și/sau deconectarea echipamentului (ori de câte ori acest lucru este posibil din punct de vedere funcțional).
Structura internă a rack-ului va facilita poziționarea cablurilor, pentru distribuirea echilibrată a bugetului de conexiuni, respectiv pentru a implementa o schemă de asigurare a redundanței (la nivel de alimentare, interconectare SAN, LAN, etc.) și evitarea condițiilor de tip single-point-of-failure.
Suport fizic de tip rack pentru montarea și poziționarea echipamentelor, cu urmatoarele specificatii tehnice minimale:

Caracteristica	Cerinta tehnica minimala
Design	Design conceput pentru rutare optima a cablurilor combinata cu ventilare maxima.
Capacitate	Minimum 42U
Facilitati pentru intretinerea echipamentelor	Usi reversibile (balamalele pot fi montate atat pe stanga cat si pe dreapta). Montarea usilor sa nu necesite interventia a mai mult de o persoana.

montate	
Protectia accesului	Usi prevazute cu incuietoare cu cheie atat in fata cat si in spatele rack-ului.
Ergonomie	Intrari pentru cabluri atat in partea inferioara cat si in partea superioara. Unitatile de inaltime sa fie numerotate. Unitatile nefolosite sa fie acoperite cu panouri oarbe.
PDU	Pentru alimentarea echipamentelor se vor folosi unităţi de tip PDU cu ieşiri tipice standard IEC 60320. Unitatile de distributie a puterii vor fi de tip „switched" cu monitorizare pentru fiecare circuit si management, cu abilitatea de a reboota echipamentele. Ansamblul va fi echipat cu numărul şi structura de unităţi PDU, precum şi cu cablurile aferente, necesare alimentării tuturor surselor echipamentelor instalate. Interconectarea acestora se va realiza de aşa manieră încât sursele care formează un set redundant, pentru acelaşi echipament, nu se vor alimenta în acelaşi PDU. Această organizare are ca scop echilibrarea implicită a sarcinii precum şi evitarea situaţiei în care oprirea, accidentală sau planificată, a oricărei unităţi PDU să provoace oprirea alimentării oricărei surse în echipamentele critice echipate cu două sau mai multe surse şi nici să nu necesite reorganizarea cablurilor pentru menţinerea stării operaţionale. Echipamentele critice echipate cu o singură sursă vor fi grupate în perechi redundante, oricare dintre ele capabil să preia sarcina sau să acopere funcţionalităţile echipamentului pereche. Fiecare PDU va fi alimentat la cate un modul UPS distinct.

3.7.2. Consolă de management general – 2 buc

Consolă locală KVM - unitate montată în rack, cu urmatoarele specificatii tehnice minimale:

Caracteristica	Cerinta tehnica minimala
Descriere	Consola KVM cu Switch KVM 16 porturi încorporat;
Tip monitor	WXGA TFT cu iluminare LED;
Dimensiune monitor	Minim 17";
Rezoluţie maximă	Minim 1280 x 1024 la 60 Hz; Pentru sesiuni la distanta 1920 x 1200
Tip layout tastatură	US English;
Porturi de conexiune	16 porturi cu posibilitatea de inseriere a cate 16 conexiuni independente fiecare;
Numar minim de conexiuni simultane	1000
Management la distanţă	Acces de la distanta prin intermediul unei conexiuni Ethernet dedicate cu suport pentru IPv4/IPv6;
Management local	Acces local prin intermediul unei conexiuni Ethernet dedicate cu suport pentru IPv4/IPv6, respectiv prin conexiune seriala;
Functionalitate suplimentara	▪ Protectia accesului local si la distanta prin mecanism bazat pe utilizator si parola, respectiv prin mecanisme de

Caracteristica	Cerinta tehnica minimala
	autentificare multi-factor; ▪ Posibilitatea de a face upgrade de firmware/software prin intermediul interfetelor de administrare;
Conectivitate inclusa	Cabluri de acces acces la consolele KVM şi la porturile usb si video din nodurile de procesare astfel incat toate nodurile de procesare sa fie deservite de monitorul si tastatura incluse in consola;
Cerinte constructive	▪ Montabil în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive);

3.7.3. Surse neîntreruptibile (UPS) – 5 unitati/module

Se va implementa o structură eficientă de alimentare de tip UPS compusă unităţi independente / modulare de tip on-line dublă conversie, pentru asigurarea alimentarii PDU-urilor.
Aceasta structura trebuie sa ofere un timp de funcţionare in regim de avarie de minim 15 de minute la o încărcare preconizata de minim 50%.
Soluţia va furniza un nivel optim de disponibilitate operaţională; capacitatea preconizată şi suportul de uptime vor permite acomodarea echipamentelor solicitate precum şi rezerva necesară pentru extensiile ulterioare previzibile, fără a pune probleme de implementare.
Unităţile UPS trebuie sa permita extinderea timpului de functionare in regim de avarie prin cel putin un modul discret de baterii, integrabil in structura fara necesitatea opririi alimentarii echipamentelor deservite.
Componentele interne ale unităţilor UPS, inclusiv bateriile, vor fi de tip hot-swap şi vor permite deservirea (inclusiv înlocuirea acestora) fără oprirea sarcinii.
Unitatea UPS va include modul de management pentru monitorizare la distanţă, inclusiv software de management si idicatori frontali pentru suprasarcina si nivel incarcare module de baterii.

3.7.4. Platforma de procesare aplicaţii

In stransa legatura si prin integrarea cu celelalte elemente de infrastructura solicitate, specific cu platforma de stocare si platforma de virtualizare, platforma de procesare aplicaţii trebuie sa permita obtinerea urmatoarelor obiective functionale si operationale:

- Complexitate redusa a platformei, in scopul integrarii cu usurinta in mediul existent, atat din punct de vedere operational cat si functional;
- Platforma complet redundanta la nivelul tuturor elementelor componente, in scopul protejarii facile a datelor rezidente si efectuarii transparente a operatiunilor de administrare, update, upgrade si inlocuire a componentelor ce se pot defecta.
- Platforma ce include mecanisme de redundanta locala, integrate cu restul elementelor de infrastructura, pentru protectia continua si completa a aplicatiilor deservite si a datelor stocate, in eventualitatea unor defectiuni majore;
- Platforma scalabila in mod transparent pentru aplicatiile deservite si datele stocate, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate, conectivitate si performanta;

- Platforma bazata pe componente standard, in scopul integrarii facile cu setul de aplicatii si cerinte existente in infrastructura, precum si cu orice alte noi cerinte viitoare, fara costuri aditionale datorate investitiilor in alte platforme de unica functionalitate;
- Unelte de administrare integrate si facil de folosit, ce acopera intreaga functionalitate, independente de anumite elemente de infrastructura (sistem de operare, tehnologie de aplicatie, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;
- Functionalitati integrate de securitate, integrate cu restul elementelor de infrastructura, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
- Platforma ce include mecanisme integrate de agregare a resurselor fizice din infrastructura, mecanisme integrate de analiza predictiva, precum si mecanisme de aplicare de politici asupra resurselor fizice in scopul obtinerii maximului de performanta si eficienta indiferent de aplicatiile si serviciile deservite de platforma, asigurand disponibilitate maxima, timpi de raspuns la incidente si costuri operationale minime;
- Platforma integrata ce va permite reducere semnificativa a timpilor de nefunctionare a aplicatiilor si serviciilor, reducerea proceselor operationale, respectiv a timpilor de solutionare a incidentelor, diminuarea costurilor operationale.

Platforma de procesare aplicaţii va deservi nemijlocit platforma de virtualizare, alocand resursele fizice de procesare si comunicatie catre elementele virtuale din platforma (procesoare virtuale, elemente de comunicatie virtuale, memorie virtuala, etc).
Toate nodurile de procesare de date vor implementa aceeaşi arhitectură internă de procesor şi aceeaşi platformă de operare.
Pentru intreaga platforma de procesare se vor asigura mijloace de evaluare continuă a perfomanţei în configuraţia curentă, încă din faza de implementare, pe baza unor metrici bine definite şi prin utilizarea de instrumente de monitorizare care vor rula în background şi vor putea genera rapoarte detaliate utilizabile direct pentru reconfigurarea (fine-tuning) parametrilor relevanţi.
Soluţia/componentele oferite trebuie să îndeplinească următoarele cerinţe functionale generale:

- Dispozitivele hardware trebuie să fie astfel proiectate încât să poată asigura scalarea sistemului în cazul creşterii nevoii de putere de calcul;
- Arhitectura soluţiei propuse trebuie să includă următoarele caracteristici generale de fiabilitate, disponibilitate şi uşurinţă în efectuarea service-ului (Reliability Availability Serviceability-RAS) la nivel de servere sau şasiu:
  - componente redundante în interiorul sistemului (surse de alimentare electrică);
  - capabilităţi de auto-testare şi rezolvare a defectelor intermitente fără intervenţie umană;
  - dealocarea de tip hotplug şi izolarea componentelor defecte ale sistemului (de exemplu discuri, ventilatoare, subsisteme de alimentare cu energie electrică, adaptoare PCI);
  - diagnosticarea erorilor în timp real;
  - capabilităţi arhitecturale de prevenire a erorilor.

Platforma de procesare reprezintă un ansamblu modular pentru suportul procesării, în arhitecturi mixte eterogene, format din şasiu modular şi module de procesare si trebuie sa respecte urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Şasiu modular pentru suportul procesării centralizate;
Arhitectura	▪ Componenta de tip şasiu modular pentru suportul procesării centralizate, cu suport inteligent pentru optimizarea,

Caracteristica	Cerinta tehnica minimala
	balansarea si integrarea modulelor de procesare; ▪ Sasiul trebuie sa suporte interconectarea cu alte sasiuri similare si agregarea resurselor de procesare intr-o singura platforma, administrabila prin intermediul unui singur set unitar de unelte de management; ▪ Şasiul trebuie configurat pentru instalarea de noduri de procesare de tip blade sau similare, optimizate pentru asigurarea densităţii si puterii de calcul necesare; ▪ Sasiul trebuie sa suporte module de procesare in tehnologie CISC x86 ce pot fiecare acomoda minim 2 procesoare in acelasi modul; ▪ Şasiul va fi echipat cu toate componentele redundante, hot-plug / hot-swap şi utilizabile în mod concurent, pentru alimentare şi ventilare; ▪ Midplane de înaltă disponibilitate care suportă funcţii de tip hot-swap la nivel de server blade individual, module de interconectare LAN, surse de alimentare;
Dimensiune	Configurat cu toate modulele de procesare, comunicatie si management solicitate;
Interfete I/O	▪ Suport pentru minim 2 module I/O interne pentru interconectare în tehnologie, 10/25/40 Gbps Ethernet, 16/32 Gbps Fibre Channel sau echivalent convergent; ▪ Se vor oferta module de interconectare externa capabile sa maximizeze disponibilitatea ansamblului prin operare cat mai facila in caz de defectare minimizand necesitatea de reconfigurari LAN efectuate de administrator.
Management	Pentru a asigura un mediu de administrare strans integrat cu platforma, disponibil la toate nivelurile acesteia (module fizice de procesare, stocare, comunicatie, management), respectiv unificat din punct de vedere al interfetei de acces, sasiul modular pentru suportul procesarii centralizate trebuie sa fie administrat de componente redundante de management dedicate functiilor administrative primare, incluse in oferta.
Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;
Ventilatie	Sistem de ventilaţie redundant, instalat intern în şasiu;
Alimentare	Trebuie sa permita instalarea de surse de alimentare redundante ce pot functiona in sistem N+N si N+1. In configuratia ofertata sasiul trebuie sa fie echipat cu un minim de 4 surse in configuratie N+N.
Cerinte constructive	▪ Montabil în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive);

3.7.5. Echipamente de procesare aplicații

Se solicită echipamente de multi-procesare, echipate cu procesoare CISC x86 multi-core in conformitate cu functiile asigurate in cadrul solutiei preconizate.

Module de procesare aplicații pentru mediul de productie	14 buc
Module de procesare aplicații pentru mediul de test/dezvoltare	10 buc

Echipamentele de procesare aplicații vor respecta urmatoarele cerinte minime:

Caracteristica	Cerinta tehnica minimala
Descriere	Module lamelare de multi-procesare simetrică, echipate cu procesoare CISC x86 multi-core pentru mediul de productie, compatibile cu șasiurile ofertate;
Procesor	▪ Minim 2x Procesor cu 22 core-uri de procesare, frecvența minima 2,1 GHz, 30 MB memorie cache, suport pentru set extins de instructiuni, respectiv suport pentru tehnologii de virtualizare bazate pe hipervizor si suport pentru accelerarea operatiunilor de criptare;
Memorie	▪ Minim 384 GB 2666 MHz ECC DDR4, suport pentru corectie erori de tip SDDC sau echivalent, respectiv pentru configurare în mod spare şi pentru memory mirroring; ▪ Fiecare modul va putea scala la minim 3 TB RAM prin extindere ulterioară;
Interfete I/O	▪ Suport pentru minim 2 module I/O interne pentru interconectare în tehnologie 10 Gbps Ethernet, 16/32 Gbps Fibre Channel sau echivalent convergent; ▪ Minim 2 port 10 Gbps Ethernet integrat, suport pentru failover şi load balancing, suport pentru Virtual LANs (VLANs), IEEE 802.3ad Link Aggregation, Jumbo Frames (9 KB), IEEE 802.3x Flow Control, SR-IOV, PXE, IEEE 802.1Qaz DCBX; ▪ Functionalitati de offload pentru VXLAN, NVGRE si Geneve, RSS, RoCE v2; ▪ Minim 2 port 32 Gbps Fibre Channel sau echivalent convergent cu suport pentru NVM2-Over-Fabric;
Stocare interna	Minim 2 drive-uri SSD de 240 GB si controler RAID cu suport pentru RAID 1
Sloturi de expansiune	Suport pentru module PCI Express de tip GPU sau NVMe;
Management	▪ Procesor de management integrat, capabilităţi de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local şi la distanţă; ▪ Sistem de analiza a componentelor modulului (procesoare, memorie, discuri), alertare in cazul depasirii pragurilor optime de functionare, respectiv mecanisme automate de corectare a respectivelor erori si evenimente; ▪ Integrare intre modulul de management din fiecare sistem

Caracteristica	Cerinta tehnica minimala
	blade si modulul de management al sasiului / platformei suport de multi-procesare; ▪ Functii de monitorizare si acces de la distanta prin intermediul interfetelor standardizate: IPMI 2.0, SNMP v3. CIM, interfata web; ▪ Serverul va fi livrat împreună cu aplicaţia de management,ce trebuie să asigure cel puţin: inventarierea componentelor, monitorizarea stării de funcţionare, operatiuni de instalare si provizionare servere atat in mediu fizic cat si in mediu virtual (compatibil cu platforma de virtualizare ofertata), monitorizarea si raportarea informatiilor legate de alimentarea si consumul de energie, respectiv legate de starea sistemelor de ventilatie, trimiterea de alerte prin e-mail, acccesul la consola serverului prin retea (virtual KVM, inclusiv cu capabilitatea de montare de discuri virtuale pentru instalarea sistemului de operare); Aplicatia va fi licentiata pentru componente sau ansamblul de componente din sasiul suport de procesare;
Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;
Redundanta	Fiecare server lamelar trebuie să dispună de conectori redundanţi pentru alimentare electrică, semnale I/O, management;
Compatibilitate sisteme de operare	▪ Modulul de procesare oferit trebuie să fie compatibil şi să dispună de suport pentru următoarele sisteme de operare: Microsoft Widows Server 2012 R2/2016, SUSE Linux Enterprise Server 11/12, Red Hat Enterprise Linux 6/7, VMware vSphere 5.5/6.0;

3.7.6. Platforma de interconectare

In scopul interconectarii elementelor solutiei preconizate, respectiv interconectarea dintre platforma de procesare, platforma de stocare si restul de elemente de infrastructura, solutia trebuie sa includa o platforma redundanta, convergenta de comunicatie, ce va asigura un nivel ridicat de performanta si disponibilitate operationala.
Platforma de interconectare va fi formata din Echipamente de comunicatie si interconectare integrate in sasiu, Echipamente de comunicatie SAN, respectiv Echipamente de comunicatie pentru interconectare interna

3.7.6.1. Echipamente de comunicatie si interconectare integrate in sasiu

Pentru asigurarea conectivitatii directe si a integrarii cu restul elementelor din solutie, in special cu platforma de stocare consolidata si platforma de comunicatie, sasiul trebuie sa integreze cel putin

doua tipuri de echipamente de comunicatie atat in tehnologie 10 Gbps Ethernet cat si 32 Gbps Fibre Channel sau echivalent convergent.

Echipamente de comunicatie 10 Gbps Ethernet – 6 buc

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare si restul de elemente de infrastructura, respectiv pentru asigurarea conexiunilor transparente catre platforma de virtualizare si masinile virtuale disponibile in aceasta, sasiurile din platforma de procesare trebuie sa includa echipamente de comunicatie de 10 Gbps Ethernet sau echivalent convergent integrate. In acest sens, se vor respecta urmatoarele cerinte functionale specifice:

Caracteristica	**Cerinta tehnica minimala**
Descriere	Echipament de comunicatie 10 Gbps Ethernet
Interfete I/O	▪ Pentru functionalitati de switching la Layer 2 trebuie sa includa nu mai putin de 32 conexiuni active de tip 10 Gbps Ethernet intern catre modulele de procesare; ▪ 8 porturi 25 Gbps Ethernet, echipate cu cabluri de tip DAC cu lungime de cel putin 3m sau cu SFP-uri 25GB short reach si activate in configuratia ofertata;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 1 Tbps; ▪ Suport pentru agregarea conexiunilor; ▪ Arhitectura de tip low-latency cu functionalitati pentru QoS; ▪ Capabilitati de virtualizare a interfetelor de comunicatie (vNIC); ▪ Suport pentru operarea de tip activ/activ; ▪ Acces la interfetele de administrare la nivelul platformei, bazat pe roluri de acces, respectiv suport integrat pentru autentificare prin mecanisme Radius, TACACS; ▪ Suport pentru clasificarea si procesarea traficului (IEEE 802.1p), respectiv modelarea si optimizarea traficului bazata pe politici definibile; ▪ Support pentru PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz), DCBX (IEEE 802.1AB); ▪ Suport pentru SNMP v2 acces prin interfata web, SSH integrate in interfata de management a platformei;
Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;

Echipamente de comunicatie 32 Gbps Fibre Channel – 6 buc

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare si restul de elemente de infrastructura, respectiv pentru asigurarea conexiunilor transparente catre

platforma de virtualizare si masinile virtuale disponibile in aceasta, sasiurile din platforma de procesare trebuie sa includa echipamente de comunicatie de tip Fibre Channel 32 Gbps sau echivalent convergent integrate. In acest sens, se vor respecta urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Echipament de comunicatie 32 Gbps Fibre Channel sau echivalent convergent (FCoE);
Interfete I/O	▪ Pentru functionalitati de tip SAN trebuie sa includa nu mai putin de 24 conexiuni active de tip Fibre Channel sau echivalent convergent (FCoE) ce pot fi alocate atat intern catre modulele de procesare, cat si extern catre porturile de uplink; ▪ Porturile Externe trebuie sa suporte echiparea cu conectori SFP+, iar in configuratia ofertata un minim de 8 porturi trebuiesc efectiv echipate cu conectori SFP+ sau echivalent;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 1 Tbps; ▪ Acces la interfetele de administrare la nivelul platformei, bazat pe roluri de acces, respectiv suport integrat pentru autentificare prin mecanisme Radius, TACACS+ si LDAP; ▪ Suport atat pentru IPv4, cat si IPv6; ▪ Suport pentru SNMP v1, v2 si v3, acces prin interfata web, acces prin SSH integrate in interfata de management a platformei; ▪ Suport pentru transmiterea evenimentelor de stare direct catre modulele de management integrate in platforma de procesare;
Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;

3.7.6.2. Echipamente de comunicatie SAN – 4 buc

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare si restul de elemente de infrastructura, respectiv pentru asigurarea conexiunilor transparente catre platforma de virtualizare si masinile virtuale disponibile in aceasta, solutia trebuie sa includa 4 echipamente redundante de comunicatie de tip Fibre Channel 16/32 Gbps.

Cele patru echipamente vor respecta fiecare urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Echipament de comunicatie 16/32 Gbps Fibre Channel;
Dimensiune	Configurat cu toate modulele de comunicatie nu trebuie sa

Caracteristica	Cerinta tehnica minimala
	depaseasca 2U;
Interfete I/O	▪ Pentru functionalitati de tip SAN trebuie sa includa cel putin de 24 conexiuni active de tip 16/32 Gbps Fibre Channel; ▪ Porturile 16/32 Gbps Fibre Channel trebuie sa suporte echiparea cu conectori SFP+, iar in configuratia ofertata un minim de 24 porturi trebuiesc efectiv echipate cu conectori SFP+ de tip short-reach; ▪ 2 porturi Ethernet 1 Gbps Full-Duplex pentru acces extern la functiile administrative;

Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 1.5 Tbps;
	▪ Suport pentru tehnologii de tip N_Port ID Virtualization (NPIV) si Mirror/Span Port;
	▪ Suport pentru functionalitati de Trunking in scopul agregarii in topologie Full Fabric a mai multe module de comunicatie SAN, cu viteza minima de 120 Gbps per Trunk de comunicatie;
	▪ Suport pentru cel putin 128 de domenii de tip Fabric, respectiv posibilitatea de functionare in mod Full Fabric sau Access Gateway/NPV Mode;
	▪ Suport pentru FC-NVMe;
	▪ Acces la interfetele de administrare bazat pe roluri de acces, respectiv suport integrat pentru autentificare prin mecanisme Radius, TACACS+ si LDAP;
	▪ Suport atat pentru IPv4 cat si IPv6;
	▪ Suport pentru SNMP v2 si v3, acces prin interfata web, SSH;
	▪ Suport pentru sincronizarea de timp in protocol NTP;
	▪ Licentiere completa a tuturor facilitatilor oferite de echipament, dar nu mai putin decat urmatoarele:
	  ▪ Licenta monitorizare, management si diagnosticare;
	  ▪ Licenta Quality Of Service (QoS);

Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;
Alimentare	Minim 2 surse de alimentare redundante;
Accesorii	Toate accesoriile necesare.
Cerinte constructive	▪ Montabil în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporți, șuruburi/captive);

3.7.6.3. Echipamente de comunicatie 10 Gbps Ethernet pentru interconectare interna – 2 buc

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare si restul de elemente de infrastructura, respectiv pentru asigurarea conexiunilor transparente catre platforma de virtualizare si masinile virtuale disponibile in aceasta, solutia trebuie sa includa 2 echipamente redundante de comunicatie Ethernet 10 Gbps. Cele doua echipamente vor respecta fiecare urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Echipament de comunicatie 10/25 Gbps Ethernet cu functii Layer 2/3;
Dimensiune	Configurat cu toate modulele de comunicatie nu trebuie sa depaseasca 2U;
Interfete I/O	▪ Pentru functionalitati de switching la Layer 2/3 trebuie sa includa nu mai putin de 24 conexiuni active de tip 10/25 Gbps Ethernet; ▪ Porturile Ethernet 10/25 Gbps trebuie sa suporte echiparea cu conectori SFP+, iar in configuratia ofertata un minim de 12 porturi trebuiesc efectiv echipate cu conectori SFP+ 10G short-reach; ▪ 1 port Ethernet 1 Gbps Full-Duplex pentru acces extern la functiile administrative; ▪ 4 porturi 100 Gbps Ethernet, echipate cu cabluri de tip DAC cu lungime de cel putin 3m sau cu QSFP-uri 100GB short-reach si activate in configuratia ofertata;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 3 Tbps; ▪ Throughput total in pachete/secunda de minim 1 Tbps; ▪ Suport pentru agregarea conexiunilor atat in mod static cat si in mod LACP, cu un minim de 64 de grupuri de interfete cu cate 32 porturi per grup; ▪ Suport pentru functionalitati de tip Priority-Based Flow Control; ▪ Configurarea selectiva a distribuirii traficului peste conexiunile agregate atat pe baza adreselor IP sursa si destinatie, pe baza adreselor MAC sursa si destinatie, cat si o combinatie a acestor doua metode; ▪ Convergenta STP rapida si suport pentru VRRP, astfel incat sa se asigure redundanta completa la Layer 2/3; ▪ Suport pentru liste de acces (ACL) bazate pe VLAN, MAC si IP; ▪ Acces la interfetele de administrare bazat pe roluri de acces, respectiv suport integrat pentru autentificare prin mecanisme Radius, TACACS+ si LDAP; ▪ Suport pentru clasificarea si procesarea traficului (IEEE 802.1p, IP ToS/DSCP, ACL), respectiv modelarea si

Caracteristica	Cerinta tehnica minimala
	optimizarea traficului bazata pe politici definibile; ▪ Support pentru PFC (IEEE 802.1Qbb), ETS (IEEE 802.1Qaz), DCBX (IEEE 802.1AB); ▪ Suport pentru protocoale de rutare (RIP v1, RIP v2, OSPF v2/v3, BGP-4), cu un minim de 1 milion de intrari in tabela de rutare; ▪ Suport atat pentru IPv4 cat si IPv6; ▪ Suport pentru VXLAN EVPN fabrics; ▪ Suport pentru SNMP v1, v2 si v3, SSH, SFTP si SCP; ▪ Suport pentru sincronizarea de timp in protocol NTP;
Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;
Alimentare	Minim 2 surse de alimentare redundante;
Cerinte constructive	▪ Montabil în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive);

3.7.7. Platforma de stocare baza de date si aplicații

Solutia va include cate o platforma de stocare pentru aplicații pentru mediul de productie, respectiv mediul de testare/dezvoltare, platforme ce vor oferi servicii de rezidenta a tuturor datelor procesate in platforma de virtualizare, respectiv in restul de platforme de procesare ce fac parte din infrastructura, pentru totalitatea utilizatorilor, servciilor, aplicatiilor si masinilor virtuale.
In stransa legatura si prin integrarea cu celelalte elemente de infrastructura solicitate, platforma de stocare trebuie sa permita obtinerea urmatoarelor obiective functionale si operationale:

- Complexitate redusa a platformei, in scopul integrarii cu usurinta in mediul existent, atat din punct de vedere operational cat si functional;
- Platforma complet redundanta la nivelul tuturor elementelor componente, in scopul protejarii facile a datelor rezidente si efectuarii transparente a operatiunilor de administrare, update, upgrade si inlocuire a componentelor ce se pot defecta;
- Platforma ce include mecanisme de redundanta locala si la distanta, integrate cu restul elementelor de infrastructura, pentru protectia continua si completa a datelor stocate, in eventualitatea unor defectiuni majore;
- Platforma scalabila in mod transparent pentru datele stocate, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate, conectivitate si performanta;
- Platforma de stocare, in scopul integrarii facile cu setul de aplicatii si cerinte existente in infrastructura, precum si cu orice alte noi cerinte viitoare, fara costuri aditionale datorate investitiilor in alte platforme de unica functionalitate;
- Unelte de administrare integrate si facil de folosit, ce acopera intreaga functionalitate, independente de anumite elemente de infrastructura (sistem de operare, tehnologie de aplicatie, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;

- Functionalitati integrate de securitate si protectie criptografica a datelor stocate, integrate cu restul elementelor de infrastructura, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
- Mecanisme integrate de optimizare transparenta a datelor stocate, in scopul folosirii eficiente a spatiului de stocare disponibil, asigurand in acelasi timp costuri operationale minime si posibilitatea de a preveni suplimentarea capacitatii de stocare;
- Platforma ce include mecanisme integrate de optimizare a performantei, prevenind astfel upgrade-urile de performanta pentru un timp mai indelungat si asigurand in acelasi timp costuri operationale minime.

In vederea atingerii obiectivelor operationale descrise solutia trebuie sa includa un sistem de stocare cu arhitectură internă flexibilă, în care controller-ele vor fi active simultan, vor partaja intreaga momorie cache disponibila, vor putea accesa intreaga capacitatea instalata si vor permite accesul simultan, in mod nepreferential, la acelasi LUN.
Platforma de stocare pentru mediul de productie trebuie sa indeplineasca urmatoarele specificatii tehnice minimale:

Caracteristica	**Cerinta tehnica minimala**
Descriere	Platforma primara de stocare de inalta performanta, suport pentru stocarea datelor prelucrate de platformele de procesare aferente mediului de productie;
Arhitectura	Platforma primara de stocare de inalta performanta va fi echipata cu patru controller-e SAN, respectiv doua controller-e NAS, pentru a putea dispune de o configuratie redundanta de tip cluster activ-activ la nivelul echipamentului; Controller-ele trebuie sa fie de tip hot-swap; Echipamenul trebuie sa asigură o disponibilitate de 99,9999%;
Protocol de acces la date	Platforma primara de stocare va oferi acces la datele stocate atat prin protocol de tip block (SAN), prin FC (Fiber Channel) si NVMe-oF, precum si prin protocol de tip file (NAS), prin NFS si CIFS;
Porturi instalate	Platforma va dispune de minim 8 porturi 10 Gbps Ethernet, echipate efectiv cu conectori SFP+; Platforma va dispune de minim 16 porturi 32 Gbps FC, echipate efectiv cu conectori SFP;
Memorie RAM	Platforma primara de stocare va avea o cantitate de memorie RAM pentru cache si management de metadate de minim 512 GB per controler, pentru un total de minim 2 TB per sistem primar de stocare; Memoria RAM trebuie sa fie protejata prin mecanisme de mirroring si de stocare pe mediu non-volatil, in cazul unor avarii la sistemul de alimentare electrica.
Nivele RAID	Configurarea si optimizarea matricilor RAID in configuratii cu minim un disc de paritate asociate fiecarui set de discuri componente al unei matrici RAID; Sistemul de stocare trebuie sa includa discuri sau capacitate aditional pentru hot spare, conform bunelor practici definite de producator;
Tehnologie stocare	Suport pentru echiparea cu medii de stocare de tip NVMe;

Caracteristica	Cerinta tehnica minimala
	Suport pentru expansiune cu medii de stocare de tip NVMe sau SAS 12Gbps;
Capacitate instalata	Platforma primara de stocare de inalta performanta va oferi o capacitate minima utila ce se va incadra in urmatorii parametri: ▪ Minim 80 TB capacitate utila totala, formata din medii de stocare de tip NVMe in proportie de 100%;
Extensia capacitatii de stocare	Platforma primara de stocare va asigura urmatoarea capabilitate minima de extensie a capacitatii de stocare: ▪ Suport pentru cel putin 90 de discuri interne in sistemul de stocare preconizat, de tip hot-swap; ▪ Suport pentru module de expansiune cu sloturi de 2,5"; ▪ Modulele de expansiune se vor conecta la echipamentul de stocare prin magistrale de date redundante, cu latime de banda de cel putin 128 Gbps; ▪ Pentru intreaga solutie se va asigura scalabilitate la minim 1 PB capacitate de stocare adresabila de catre servere;
Performanta	Configuratia livrata trebuie sa livreze cel putin 300.000 IOPS, cu un profil de 75% citire, 25% scriere, IO Size 32KB. Aceasta performanta trebuie sa fie sustinuta in urmatoarele conditii: ▪ Capacitate alocata si activa de minim 70% din totalul disponobil; ▪ Durata de mentinere a parametrilor de minim o ora; ▪ Functionalitati de deduplicare, compresie si criptare active pe setul de date; ▪ Timp de raspuns catre servere de <1 ms; ▪ Mentinerea performantei chiar si in conditiile defectarii unui controller;
Managementul platformei	▪ Platforma primara de stocare va asigura un sistem de management si monitorizare integrat; ▪ Platforma primara de stocare va avea capabilitatea de monitorizare si management a mai multor echipamente din aceeasi gama intr-o singura instanta a interfetei, atat pentru serviciile SAN, cat si pentru cele NAS; ▪ Platforma primara de stocare va asigura provizionarea automata a sistemelor de fisiere; ▪ Platforma primara de stocare va asigura monitorizarea performantei si capacitatii platformei de stocare atat la nivel fizic cat si la nivel virtual; ▪ Platforma primara de stocare tebuie sa includa fara costuri aditionale cel putin posibilitatea administrarii prin intermediul unei interfete web securizate SSL si/sau aplicatie dedicata de management, precum si consola de administrare la distanta SSH. Toate functiile native ale sistemului de stocare, precum si functionalitatea licentiata separat vor fi accesibile in mod integrat prin intermediul acestor unelte de administrare, astfel incat operatiunile de configurare si administrare va putea fi efectuate indiferent de locatie si de modalitatea de acces;

Caracteristica	Cerinta tehnica minimala
	▪ Atat in scop administrativ cat si in vederea accesului la seturile de date, platforma primara de stocare va permite nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. De asemenea, va permite integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor si a drepturilor de acces la seturile de date partajate de sistem. Pentru sporirea securitatii in mecanismele de autentificare, echipamentul va permite integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp. Mecanismele de export ale volumelor prin intermediul protocolului CIFS vor beneficia nativ de suportul integrarii echipamentului de stocare cu sistemele de tip director si cu sistemele de sincronizare a informatiilor de timp; ▪ Uneltele de administrare prin interfata web si/sau aplicatie dedicata vor fi usor de folosit si vor implementa majoritatea actiunilor administrative (definirea de volume, LUN-uri, exportul seturilor de date indiferent de protocolul folosit pentru export, configurarea functiilor de partajare, optimizare si protectie a datelor, definirea relatiilor de replicare) intr-o singura interfata, fara a fi nevoie de acces la uneltele in linie de comanda. Uneltele vor permite atat configurarea si administrarea sistemului curent cat si orice alt sistem viitor de la acelasi producator, din aceeasi gama. De asemenea, va integra un panou unificat de afisare a informatiilor legate de performanta (inclusiv gradul de ocupare al procesoarelor, nivel I/O, latenta in functie de protocolul de comunicatie si tipul de export al volumelor, numarul de operatiuni efectuate asupra seturilor de date), informatiilor legate de gradul de ocupare (inclusiv gradul de ocupare per volum de date si tipul de partajare al resurselor), respectiv afisarea informatiilor legate de starea controller-elor, a relatiilor de replicare intre echipamente si a evenimentelor informationale si/sau de alertare survenite in functionarea oricarui element hardware sau functie software; ▪ Interfata de grafica administrare trebuie sa fie de tip HTML5; ▪ Tot ca parte a uneltelor standard de administrare, platforma primara de stocare tebuie sa includa posibilitatea de integrare nativa cu platforma centrala de procesare astfel incat va permite definirea volumelor, LUN-urilor, aplicarea politicilor si mecanismelor integrate de optimizare, crearea de copii de siguranta, analizarea si corectarea dinamica a parametrilor de export ai seturilor de date catre platforma centrala de procesare, direct din uneltele de management puse la dispozitie de platforma centrala de procesare, fara a folosi un alt set de unelte terte ce nu apartin nici de platforma primara de stocare, nici de cea de procesare. Astfel se obtine o platforma unitara de management, ce reduce efortul si costul administrativ, indiferent de natura

Caracteristica	Cerinta tehnica minimala
	operatiunilor efectuate; ▪ Platforma primara de stocare va permite accelerarea hardware a operatiunilor ce au loc intre platforma centrala de procesare si sistemul de stocare, prin degrevarea unor procese de la nivelul platformelor de procesare si preluarea lor la nivelul echipamentului de stocare. Aceasta functionalitate va permite accelerarea mutarii unei masini intre doua volume de date ale platformelor de procesare si accelerarea efectuarii unei copii identice a unei masini; ▪ Platforma primara de stocare tebuie sa includa suport pentru VAAI, VASA si VVols; ▪ Pentru asigurarea unui nivel optim de disponibilitate operationala, solutia preconizata va permite update si upgrade software si hardware al platformei fara intreruperea serviciilor si fara degradare de performanta; ▪ In scopul alocarii eficiente si dinamice a spatiului de stocare in functie de cerintele previzionate sau de moment, platforma primara de stocare tebuie sa includa nativ un mecanism de integrare directa la nivelul sistemului de operare ce acceseaza platforma primara de stocare, mecanism ce va permite executarea direct din sistemul de operare a actiunilor administrative ce privesc definirea de volume si LUN-uri, redimensionarea lor fara pierderea datelor stocate, configurarea si optimizarea parametrilor de conectare la aceste volume indiferent de protocolul folosit in exportul lor. Mecanismul va fi disponibil cel putin pentru sistemele de operare de tip server pentru care platforma primara de stocare va oferi suport de conectivitate directa: Windows, VMware vSphere; Ca parte a functiilor de administrare si diagnosticare, platforma primara de stocare tebuie sa includa standard un mecanism de alertare pe e-mail, configurabil pentru un set specific de adrese e-mail si/sau catre o platforma de suport disponibila la producatorul sistemului de stocare. De asemenea, va permite integrarea in unelte dedicate de management al infrastructurilor prin suport complet pentru protocolul SNMP versiunea 2 si 3 si prin existenta in mod gratuit a descriptorilor si parametrilor platformei astfel incat integrarea se va face in mod facil in uneltele de management ce nu au implicit profile definite pentru sistemul specific preconizat. Tot in scopul operatiunilor de management si diagnosticare sistemul va integra un set de led-uri ce afiseaza cel putin starea curenta a echipamentului;
Optimizarea capacitatii de stocare	Platforma primara de stocare va avea capabilitati de tip „Thin Provisioning” (alocarea catre nodurile de procesare a unei capacitati de stocare mai mare decat cea fizic disponibila), „Deduplicare In-Line” (reducerea in timp real a blocurilor de date identice la un singur set de blocuri de date unice in vederea optimizarii spatiului de stocare), respectiv capabilitati de tip „Compresie In-Line”

Caracteristica	Cerinta tehnica minimala
	(compresia in timp real a blocurilor de date unice in vederea optimizarii spatiului de stocare); Functiile de deduplicare si compresie trebuie sa fie asistate hardware de catre un modul dedicat pentru a nu introduce impact de performanta; Platforma primara de stocare va asigura rebalansarea datelor pe matricile de discuri in cazul in care sunt adaugate discuri suplimentare; Platforma primara de stocare trebuie sa includa un mecanism de instantiere a unui set de date disponibil la nivel de volum si/sau LUN, fara copierea datelor in instante multiple, ci prin folosirea unui singur set de date, dar adresabil de catre aplicatii si utilizatori ca instante complet diferite;
Protectia si replicarea datelor	Platforma primara de stocare va avea incoporate baterii ce asigura protectia controller-elor si a memoriei cache la cadererile de curent prin salvarea automata a datelor din cache pe mediile de stocare, inainte de oprirea echipamentului; Platforma primara de stocare trebuie sa includa mecanisme de realizare a copiilor complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp. Sistemul va permite si realizarea de copii ale oricarei copii de date. Copiile de date complete, sau bazate pe imagini, vor putea fi accesate atat in mod „citire", cat si in mod „scriere". Se va asigura suport pentru minim 1000 de copii ale volumelor de date (LUN); Echipamentul trebuie sa includa functionalitate de criptare a datelor prin mecanism AES-256, pentru toate mediile de stocare instalate in sistem. Echipamentul de stocare all flash ofertat include mecanisme de integrare directă cu echipamentul de realizare si stocare a backup-ului pe disc, cu deduplicare a datelor. Prin integrare directa, entitatea contractanta defineste mecanismul de copiere a datelor ce se va realiza direct intre echipamentul de stocare si echipamentul de backup pe disc deduplicat (mapare directa a echipamentului de backup la echipamentul de stocare si copiere datelor prin FC), fara necesitatea de trecere a datelor printr-un al treilea echipament de tip host (server); Va oferi tipuri de replicare diferite (sincron, asincron), per aplicatie sau grup de aplicatii, cu posibilitatea de a modifica tipul de replicare, fara resincronizare initiala. Toate functionalitatile software solicitate mai sus vor fi incluse in configuratia ofertata a echipamentului de stocare, respectiv pentru intreaga capacitate de stocare ofertata, fara costuri aditionale in cazul viitoarelor extensii de capacitate de stocare;
Sisteme de operare suportate	Platforma primara de stocare va suporta minim urmatoarele sisteme de operare: ▪ Microsoft Windows Server 2012 R2/2016/2019; ▪ Vmware vSphere 6.0/6.5/6.7;

Caracteristica	Cerinta tehnica minimala
	▪ Red Hat Enterprise Linux 7.x;
Conformitate cu standarde europene/cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;
Alimentare	Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al platformei de stocare (controller, sasiu discuri, etc) trebuie sa ofere alimentare redundanta prin cel putin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma;
Ventilatie	Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma;
Cerinte constructive	▪ Platforma de stocare trebuie să fie montabilă în rack-uri standard de 19"; ▪ Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporți, șuruburi/captive);

Solutia trebuie sa contina o platforma secundara de stocare si retentie pentru backup pe disc ce va indeplini urmatoarele specificatii tehnice minimale:

Caracteristica	Cerinta tehnica minimala
Descriere	Platforma secundara de stocare si retentie pentru backup pe disc, suport pentru protectia operationala a datelor stocate in platforma primara de stocare de inalta performanta;
Arhitectura	Sistem hardware dedicat protectiei datelor, tip appliance, certificat de producator; Echipament optimizat pentru transfer backup-uri, stocare si retentie pe termen lung, securizare si validare a datelor;
Protocol de acces la date	Platforma primara de stocare va oferi acces la datele stocate atat prin protocol de tip block (VTL), prin FC (Fiber Channel), precum si prin protocol de tip file (NAS), prin CIFS, NFS si NDMP;
Porturi instalate	Echipamentul trebuie sa includa minim 4 x 10Gbps Ethernet SFP+ si 4 x 16G Fiber Channel;
Memorie RAM	Minim 256GB RAM, cu implementare de mecanisme de protectie pentru protectia datelor in timpul procesului de scriere;
Nivel RAID	Configurarea si optimizarea matricilor RAID in configuratii cu minim doua disc de paritate asociate fiecarui set de discuri componente al unei matrici RAID si cate un disk hot-spare inclus pentru fiecare grup de discuri;
Tehnologie stocare	Suport pentru echiparea cu medii de stocare de tip SAS 12 Gbps; Suport pentru expansiune cu medii de stocare de tip SAS 12 Gbps;
Capacitate instalata	Echipamentul trebuie sa includa o capacitate utila de minim 90 TB;

	Echipamentul trebuie sa includa o capacitate de stocare de tip SSD destinata exclusiv memorarii si accesari rapide a indecsilor specifici procesului de deduplicare indiferent de capacitatea utilizata;
Extensia capacitatii de stocare	Platfroma trebuie sa permita posibilitatea de crestere a capacitatii de cel putin trei ori utilizand aceleasi resurse de procesare si memorie;
Performanta	Echipamentul va sustine un minim de 400 de sesiuni de transfer de date in paralel; Viteza de transfer de cel putin 9TB/h;
Managementul platformei	Platforma secundara de stocare si retentie pentru backup pe disc trebuie sa includa cel putin posibilitatea administrarii prin intermediul unei interfete web securizate SSL si/sau aplicatie dedicata de management, precum si consola de administrare la distanta SSH. Toate functiile native ale sistemului de stocare, precum si functionalitatea licentiata separat vor fi accesibile in mod integrat prin intermediul acestor unelte de administrare, astfel incat operatiunile de configurare si administrare va putea fi efectuate indiferent de locatie si de modalitatea de acces; Interfata de grafica administrare trebuie sa fie de tip HTML5; Monitorizarea tuturor componentelor solutiei, software si hardware, intr-o singura interfata grafica ce va permite personalizarea informatiilor in functie de cerintele administratorului; Componentele software si hardware ale solutiei trebuie sa permita integrarea cu aplicatii externe utilizand interfete software standard tip REST API;
Optimizarea capacitatii de stocare si securizarea datelor	Sistemul propus trebuie sa sustina deduplicarea datelor cu posibilitatea de a rula procese paralele de salvare si restaurare, utilizand interfete multiple de retea fara a afecta integritatea datelor; Procesul de deduplicare trebuie sa se desfasoare continuu, "inline", fara stocare temporara a datelor, iar factorul de deduplicare sa fie global indiferent de sursa acestor date; Echipamentul trebuie sa utilizeze un factor global de deduplicare pentru toate datele salvate sau arhivate, indiferent de sursa, protocol, sau interfata de retea prin care au fost transferate; Transferul datelor de la sursa la echipament hardware va putea utiliza toate resursele de retea disponibile peste conexiuni multiple prin mecanisme de tip load balancing si fail-over; Segmentele de date deduplicate trebuie sa poata fi securizate prin mecansime de tip WORM, protejate fata de eventuale actiuni de stergere ale unor interventii neautorizate; Politicile de securizare a datelor in echipament trebuie sa permita mai multe nivele de protectie inclusiv pentru perioade nedefinite indiferent de politica de retentie aplicata la momentul salvarii; Echipamentul trebuie sa sustina mecanisme de evaluare si corectie a datelor salvate, a sistemului de fisiere, prin care asigura verificarea continua a segmentelor de date deduplicate si disponibilitatea de restaurarea granulara sau completa a fiecarui proces de salvare finalizat cu succes;

	Procesul de expirare si stergere a segmentelor de date deduplicate trebuie sa se faca in mod automat permitand proceselor de salvare si restaurare sa se desfasoare fara oprire; Echipamentul trebuie sa utilizeze functii avansate de compresie hardware fara a utiliza resursele de procesare ale sistemului pentru a reduce cantitatea de date stocata; Echipamentul trebuie sa includa mecanisme interne de protectie de tip snapshot; Echipamentul trebuie sa permita criptarea segmentelor unice de date in mod compliant FIPS 140-2; Echipamentul trebuie sa permita replicarea datele intr-un sistem similar, iar procesul de replicare va transfera doar segmentele de date noi, unice, deduplicate, catre sistemul de la distanta; Administratorul va putea rula simultan mai multe masini virtuale direct din echipamentul dedicat protectiei datelor cu posibilitatea de a le transfera catre mediul de productie fara oprirea acestora sau actionarea unui proces de restaurare; Platforma secundara de stocare si retentie pentru backup pe disc trebuie sa permita integrarea nativa cu platforma primara de stocare de inalta performanta astfel incat transferul datelor in timpul procesarii politicilor de protectie sa utilizeze mecansime native de protectie ale platformei primare de stocare comunicand direct cu sistemul dedicat protectiei datelor, fara implicarea serverelor productive sau a unui server de backup;
Alimentare	Surse de alimentare redundante;
Sisteme de operare suportate	Platforma primara de stocare va suporta minim urmatoarele sisteme de operare: ▪ Microsoft Windows Server 2012 R2/2016/2019; ▪ Vmware vSphere 6.0/6.5/6.7; ▪ Red Hat Enterprise Linux 7.x;
Conformitate cu standardele europene / cerinte mediu	Certificare CE conform directivelor UE: ▪ Siguranta in exploatare: 2014/35/EU; ▪ Echipamente de joasa tensiune: 2014/35/EU; ▪ Compatibilitate electromagnetica: 2014/30/EU; ▪ Declaratie RoHS: 2011/65/EU;
Cerinte constructive	Platforma de stocare/retentie de mare capacitate va fi montabila in rack-uri standard de 19”;

3.7.8. Platforma de balansare a traficului de aplicatie

Solutia va include un complet format din cel putin doua echipamente care sa functioneze intr-un cluster care sa ofere o disponibilitate inalta a serviciilor de aplicatii. Acesta va oferii servicii transparente de balansare, accelerare si protejare a aplicatiilor. Platforma trebuie sa indeplineasca cel putin urmatoarele cerinte functionale specifice:

- Minim 8 interfete 1Gbps, SFP, din care cel putin 4 echipate cu conector de cupru;
- Minim 4 interfete 10Gbps, SFP+, toate echipate cu optice multimode, short distance;

- Stocare interna de cel putin 500GB;
- Memorie RAM, cel putin 32GB;
- Sursa de alimentare AC redundanta cu posibilitatea inlocurii lor fara intreruperea functionarii;
- Performanta de minim 20Gbps de procesare a traficului la L4/7 per echipament;
- Performanta de minim 10Gbps la compresia traficului in hardware;
- Performanta de minim 12Gbps la criptarea traficului in hardware;
- Performanta de minim 1.100.000 cereri pe secunda la nivel 7;
- Performanta de minim 10000 tranzactii SSL pe secunda folosind ECC si minim 20000 de tranzactii SSL pe secunda folosind RSA;
- Distributia incarcarii de procesare pentru cel putin protocoalele TCP si UDP;
- Suport pentru folosirea SNAT;
- Distributia incarcarii de procesare pe baza urmatorilor algoritmi: round robin, ratio, weighted ratio, dynamic ratio, least connections, weighted least connections, observed, predictive;
- Posibilitatea de monitorizare a serverelor de aplicatii folosind mecanisme de verificare pentru protocoalele standard;
- Posibilitatea de configurare a mecanismului de verificare specific fiecarei aplicatii;
- Monitorizarea disponibilitatii atat la nivel de nod cat si la nivel de serviciu si nivel de aplicatie;
- Posibilitatea de translatare atat a adreselor IP cat si a porturilor pe care ruleaza serviciile furnizate de serverele de aplicatii;
- Posibilitatea de manipulare a distributiei incarcarii de procesare pe baza informatiilor din headerele protocoalelor de aplicatie folosite;
- Capacitatea de trimite cereri gradual catre serverele de aplicatii nou adaugate;
- Capacitatea de a folosi o combinatie mixta de adrese virtuale si noduri IPv4 si IPv6;
- Capacitatea de insertie XFF in header HTTP, cu IP originator al clientului;
- Redirectare URL catre mai multe servere virtuale in functie de HTTP response code sau URL pattern;
- Capacitatea de a agrega si refolosi multiple sesiuni client intr-o singura sesiune server-side;
- Capabilitate de compresie HTTP pentru reducerea traficului;
- Capabilitate pentru caching multi-store pentru continut dinamic si static (RFC2616);
- Capabilitate "cookie encryption" pentru prevenirea "cookie session hijacking" si manipularea cookie-urilor;
- Capabilitati pentru optimizarea traficului LAN/WAN conform: RFC2582 (optimizare Reno asimetrica), RFC1323 (extensii TCP pentru retele de mare viteza), RFC3042, RFC2018, RFC3168;
- Protectie impotriva atacurilor de tip SQL injection;
- Protectie impotriva atacurilor de tip Web Scraping;
- Protectie impotriva atacurilor de tip Cross Site Scripting;
- Protectie impotriva atacurilor de manipulare a parametrilor HTTP;
- Protectie impotriva atacurilor de tip Cross Site Request Forgery;
- Protectie impotriva atacurilor de tip Brute Force;
- Protectie impotriva atacurilor axate pe XML;
- Protectie impotriva scurgerilor de date sensibile din cadrul aplicatiei;
- Protectie impotriva modificarilor intentionate de parametrii la aplicatii;

- Protectie impotriva atacurilor de tip Cookie Poisoning;
- Protectie impotriva atacurilor de tip Hidden Field Manipulation;
- Protectie impotriva atacurilor de tip Buffer Overflow;
- Protectie impotriva atacurilor de tip Cookie Manipulation;
- Protectie impotriva atacurilor de tip Request Smuggling;
- Protectie impotriva atacurilor de tip Session Hijacking;
- Protectie impotriva atacurilor de tip Broken authentication and session management;
- Ascunderea de catre utilizator a erorilor furnizate de aplicatii;
- Impunerea unor politici de securitate bazate pe GeoIP;
- Posibilitatea de securizare pentru tranzactiile de tip web services;
- Furnizarea unui mecanism de rollback pentru politicile de securitate;
- Functie de auto-invatare a parametrilor din cadrul unei politici de securitatea in timp real;
- Furnizarea de politici predefinite pentru diferite aplicatii;
- Posibilitatea generarii automate a politicilor si mecanismelor de securitate;
- Posibilitatea de asimilare automata a parametrilor unei aplicatii;
- Furnizarea de audit si raportare pentru fiecare politica de securitate;
- Posibilitatea de integrare cu solutii de evaluare a vulnerabilitatilor unor aplicatii;
- Posibilitatea definirii centralizate a politicilor de acces pentru diferite resurse protejate de catre sistem;
- Permite definirea de politici de acces pentru utilizatorii de la distanta;
- Suport pentru single sign on (SSO) distribuit pe mai multe domenii si resurse;
- Posibilitatea de definire a politicilor de acces folosind o interfata grafica intuitiva;
- Folosirea de ACL-uri dinamice pentru sesiunile autentificate si autorizare;
- Posibilitatea de integrare cu servere AAA de tipul Active Directory, LDAP, RADIUS;
- Posibilitatea de a face caching la credentialele utilizatorilor pentru care se foloseste SSO;
- Posibilitatea de definire a politicilor de acces pentru un portal web, o aplicatie tunelata sau acces la retea;
- Posibilitatea definirii a politicii de acces in mod granular;
- Suport pentru certificate digitale pentru utilizatorii platformelor Microsoft Windows;
- Posibilitatea de a exporta si importa politicile de acces;
- Licenta pentru minim 500 de utilizatori concurenti autentificati;
- Posibilitatea sincronizarii configuratiilor in cluster si intre clustere diferite;
- Sistem de operare pentru management independent de sistemul folosit pentru procesarea traficului;
- Sistem de operare pentru procesarea traficului modular;
- Mecanisme de configurare folosind interfata Web si CLI sau mecanisme API
- Extinderea functionalitatilor ADC prin limbaj de scripting capabil sa foloseasca declaratii conditionale (if/then) si bucle (for, while);
- Capacitatea de modificare/alterare cerere/raspuns in functie de: parametri standard HTTP (header, cookie, hostname, URN, etc), username, parametri ai certificatelor X.509;
- Acces la un feed de securitate de tipul IP intelligence, oferit de producator, pe toata perioada garantiei si suportului oferit pentru echipamente;

3.7.9. Platforma unificată de securitate

Solutia va include un complet format din cel putin doua echipamente care sa functioneze intr-un cluster care sa ofere o disponibilitate inalta a serviciilor de securitate de tip next generation firewall. Platforma trebuie sa indeplineasca cel putin urmatoarele cerinte functionale specifice:

- Minim 4 porturi de 100 GE QSFP28/ 40 GE QSFP+
- Minim 24 porturi 25 GE SFP28/ 10 GE SFP+ / GE SFP
- Minim 2 proturi de Management RJ45
- Storage intern: minim 2 TB SSD
- Surse AC redundante de tip Hot swappable
- Performanta firewall pachete: 240 Gbps
- Performanta trafic firewall (pachete per secunda): 225 Mpps
- Performanta IPS: 44 Gbps
- Performanta Threat Protection: 23 Gbps
- Performanta SSL Inspection: 30 Gbps
- Performanta control de aplicatii: 86 Gbps
- Sesiuni concurente: 50.000.000
- Conexiuni noi pe secundă: 460.000
- Politici firewall: 200.000
- Procesare trafic de tip IPSec VPN: 140 Gbps
- Procesare trafic de tip SSL VPN: 11 Gbps;
- Tunele IPSec VPN (site-to-site): 100.000
- Tunele IPSEC VPN (gateway – gateway): 40.000
- Configurații HA : activ/activ, activ/pasiv.
- Suport pentru protocoale de rutare dinamice
- Supentru pentru inspectia traficului bazat pec el putin urmatoarele module de securitate: IPS, Antivirus, Filtrare Web, Control Aplicatii etc.
- Suport VPN de tip site-to-site si Remote Access
- Suport Traffic Shaping
- Suport SD-WAN
- Update-uri de securitate automate si in timp real
- Platforma hardware, sistemul de operare si licentele/update-urile de securitate trebuie sa fie furnizate de la acelasi producator
- Suport pentru rutare statica si rutare bazata pe sursa
- Protocoale dinamice de routare: OSPF, ISIS, BGP4
- Suport pentru trafic de tip Multicast
- Suport pentru functionare in mod Virtual Wire
- Suport pentru functionare in mod explicit web si FTP proxy: FTP, HTTP si HTTPS
- Suport IPsec VPN:
  - Site-to-site
  - Client-to-site (remote access)
- Suport SSL VPN
- Suport pentru vpn de tip Remote Acces bazat pe client nativ ale sistemului de operare OSx
- Suport pentru definirea de mai multe instante/partitii virtuale

- Solutia trebuie sa permita distribuirea procesarii de trafic a instantelor virtuale intr-un cluster de tip HA: Activ-Pasiv.
- Solutia trebuie sa permita activarea selectiva a traficului ce se doreste a fi procesat de ASIC-uri.
- Sistemul va fi livrat cu urmatoarele licente: IPS, Application Control, Antivirus, Webfiltering, Antispam
- Update gratuit pentru sistemul de operare al echipamentelor pe perioada de garantie si suport

3.7.10. Unitate de banda

Solutia ofertata trebuie sa îndeplinească următoarele cerințe tehnice:

Descriere	Librarie de benzi modulara pentru retentia datelor pe termen lung;
Arhitectura	Unitate scalabila compatibila LTO-8, LTO7 si LTO-6; Scalabilitate pana la minim 6 unitati de citire/ scriere de tip Full Hight si minim 240 de casete instalate;
Interfete de conectare suportate	8 Gb/sec Fibre Channel si 6 Gb/sec SAS;
Unitati de citire scriere instalate	Minim doua unitati LTO-8, Full High, fiecare cu doua porturi 8 Gb/sec Fibre Channel;
Capacitate	Minim 80 de casete instalabile in configuratia livrata;
Unitati de stocare livrate	50 de casete LTO-8 si 12 casete de curățare;
Managmentul platformei	Interfata grafica de administrare de la distanță, astfel încât să poată fi monitorizat și gestionat cu ușurință de oriunde. Funcțiile includ: ▪ Informații de stare pe unitate și sistem ▪ Operațiuni de configurare a sistemului și raportare ▪ Erori de sistem și jurnale de stare ▪ Capacități de upgrade de firmware pentru bibliotecă și unitate ▪ Teste de diagnostic și informații ▪ Deplasarea cartușelor în scopuri de întreținere și gestionare ▪ Suportul cartușului de curățare ▪ Securitate și control al accesului ▪ Suport SNMP pentru comunicare IP ▪ Gestionarea partiționării și criptării ▪ Compatibil HTTPS ▪ Suport pentru protocolul de rețea IPv6 și IPv4
Securitate	Criptare AES 256-bit sau echivalent 256-bit;
Alimentare	Surse de alimentare cu redundanta;
Cerinte constructive	Libraria de benzi trebuie să fie montabilă în rack-uri standard de 19"; Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporți, șuruburi/captive);

3.8. *COMPONENTELE SOFTWARE*

3.8.1. Componenta de Portal

Portalul platformei PSCID reprezinta punctul de acces catre serviciile electronice expuse de PSCID si reprezinta componenta prin intermediul careia:

- **Cetateanul**:
  - se inregistreaza in vederea solicitarii accesului la serviciile de eGuvernare si obtinerea identitatii sale electronice unice la nivelul PSCID
  - selecteaza serviciile de eGuvernare pe care doreste sa le utilizeze
  - stabileste modalitatea de acces si de utilizare a credentialelor la nivelul fiecarui serviciu in parte
- **Furnizorii de servicii de eGuvernare**
  - Inregistreaza serviciile electronice pentru care vor utiliza autenficarea oferita de PSCID
  - Prezinta modalitatile de autentificare si tipurile credentialele posibile a fi utilizate pentru accesarea serviciilor proprii.
- **Furnizorul de identitati electronice** prezinta Catalogul Serviciilor Electronice proprii si modalitatile de interconectare a identitilor proprii cu PSCID

Componenta de Portal va asigura principalul punct de acces direct pentru utilizatori la modulele sistemului si va trebui sa raspunda la urmatoarele cerinte minime:

- Să ofere suport pentru tehnologii şi standarde deschise;
- Interfaţă web standardizată, simplă şi intuitivă;
- Interfaţă cu utilizatorii bogată în funcţionalităţi care să ofere un nivel ridicat de accesibilitate, conform cu cerinţele nivelului I (A) de accesibilitate WCAG versiunea 1.0;
- Componenta de management de conţinut care să permită stocarea şi gestionarea într-o manieră sigură şi eficientă a tuturor secţiunilor ce vor fi publicate prin intermediul portalului;
- Să ofere suport multi-lingvistic pentru instalare şi prezentare;
- Un framework unic de dezvoltare a portalului, astfel încât indiferent de tipul de conţinut publicat în portal sau de tipul de aplicaţii, modul de integrare al acestora în portal să fie consistent şi sigur;
- Servicii şi extensii ale portalului modulare, care să permită dezvoltarea ulterioară de noi functionalităţi;
- Arhitectură orientată pe servicii, astfel incât toate serviciile implementate pentru gestionarea conţinutului în portal (publicare, căutare, versionare, etc.), să poata fi reutilizate şi incluse în alte aplicaţii;
- Administrarea şi dezvoltarea portalului se va putea realiza facil, utilizând doar un browser web;
- Să imbunătăţească experienţa utilizatorilor prin utilizarea unor tehnologii bazate pe Web 2.0 si AJAX;
- Să ofere acces către toate resursele prezente în cadrul portalului printr-o singură autentificare, la deschiderea sesiunii;
- Să ofere functionalităţi Web 2.0, pentru a asigura interacţiunea dintre utilizatorii portalului;
- Grad ridicat de securitate a sistemului, care să garanteze confidenţialitatea şi securitatea datelor utilizatorilor pentru accesul neautorizat atât dinafară cât şi din interiorul sistemului;
- Să ofere posibilitatea de a utiliza un director LDAP pentru a stoca şi administra utilizatorii portalului;
- Mecanisme de grupare a serverelor portal in clustere de servere de aplicaţii atât în topologii de

tip activ-activ cât şi activ-pasiv;

- Stoparea temporară a unui nod din cluster pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale;
- Mecanisme de balansarea dinamică a încărcării sistemului între resursele administrate în cadrul aceluiaşi cluster;
- Mecanisme de scalare a sistemului pe orizontală (Scale Out) şi verticală (Scale Up), pentru asigurarea scalarii solutiei in situatia in care numarul de utilizatori va creste in viitor, fara modificarea configuratiilor solutiei;
- Suport pentru specificaţiile standardelor international privind dezvoltarea interfetelor de portal;
- Suport pentru servicii web, pentru integrare si interoperabilitate;
- Rapoarte analitice asupra tuturor acţiunilor utilizatorilor, care să ofere posibilitatea de a analiza traficul şi activitatea utilizatorilor pe portal;
- Să conţină un motor de căutare performant, care se permită efectuarea de interogări în toate sursele de informaţie prezente în mediul portal.
- Trebuie să ofere capabilităţi de urmărire şi analiza a traficului şi să permită colectarea şi raportarea de metrici pentru funcţionalităţil, incluzand accesul la pagini, elementele constitutive ale acestora (web part, widget, portlet) şi documente. Prin aceste metrici portalului trebuie să permită identificarea eventualelor tipare de utilizare (usage patterns) cum ar fi durata vizitelor pe o anumita pagina sau frecvenţa accesului la o pagină într-o anumită perioadă de timp
- Metricile colectate trebuie sa poată fi corelate cu utilizatorul pemitand apoi filtrarea datelor după atribute din profil cum ar fi locaţia utilizatorului, departamentul sau funcţia
- Trebuie sa permită colectarea urmatoarelor tipuri de metrici:
  - Trafic la nivelul intregii componente
  - Trafic la nivel de pagina
  - Metrici referitoare la conectarea utilizatorilor
  - Metrici la nivel de elemente şi performantele acestora (frecventa utilizarii, timpi de raspuns)
  - Metrici referitoare la operatiile de cautare realizate prin interfata unificata
  - Metrici referitoare la documentele din accesate

3.8.2. Server web si Reverse Proxy (DMZ)

Pentru protejarea zonei de aplicatii, in zona de interfatare DMZ se vor instala puctele de intrare in sistem pentru utilizatori prin intermediul serverelor web si reverse proxy al caror principal scop este:

- Să permită, din punct de vedere tehnic, vizualizarea layout-ului şi a resurselor Portal într-un browser Web;
- Să se integreze cu cel puţin o soluţie de tip Single-Sign On pentru autentificarea unitară a utilizatorilor;
- Să permită, din punct de vedere tehnic, accesarea aplicaţiei din browsere tradiţionale (Internet Explorer, Mozilla Firefox, Opera etc.), cât şi de pe dispozitive mobile;
- Să asigure prin componentele software ale serverului Web funcţionarea în cluster pentru a asigura balansarea încărcării şi disponibilitatea maximă a aplicaţiei;
- Sa ofere posibilitatea de rulare pe diverse platforme hardware si pe sistemele de operare majore de pe piata (Windows, Linux si UNIX)

Serverele web trebuie sa permita prezentarea continutului sistemului catre utilizatori si transferul de date dinspre client spre sistem (prin intermediul browserelor web). In acelasi timp, serverele web trebuie sa asigure primul nivel de securitate software din punct de vedere al accesului – configurare in mod reverse proxy, suport pentru SSL si autentificare de baza (in conjunctie cu serverele de control acces ale solutiei).
Comunicatiile cu exteriorul retelei trebuie sa se realizeze atat criptat cat si in clar, in functie de tipul informatiei. Serverele web trebuie sa permita integrarea cu solutii de accelerare hardware a criptarii/decriptarii si sa dispuna de functionalitati de rescriere a adreselor URL.
Din motive de securitate si usurinta in utilizare, serverul web trebuie sa permita implementarea unui mecanism de tip SSO in conjunctie cu solutia de control acces si in acelasi timp sa ofere suport pentru autentificare cu certificate digitale prin integrare cu solutia de control acces si cu o infrastructura PKI.
In plus, serverele web trebuie sa ofere suport pentru IPv4 si IPv6 astfel incat sa permita utilizarea in contextul noilor scheme de adresare Internet.
Serverele web trebuie sa poata rula pe toate distributiile majore de sisteme de operare prezente pe piata (Windows, Linux, Unix).

3.8.3. Componenta SGBD

Sistemul de gestiune al bazelor de date relationale trebuie sa fie un sistem de gestiune a bazelor de date de tip relational si sa ofere posibilitatea de a rula pe diverse platforme hardware precum si pe sistemele de operare majore existente pe piata (Windows, Linux, Unix), oferind urmatoarele capabilitati:

- va permite folosirea pentru procesările de tip SQL a minim 32 de nuclee de procesare (core-uri fizice procesor)
- posibilitatea de a suspenda temporar operatii consumatoare de resurse (de exemplu incarcari masive de date), cu reluarea ulterioara a acestora in momentul cand sistemul permite precum si posibilitatea de a implementa scheme de prioritate in modul de accesare a bazei de date in functie de tipul de utilizator inclusiv limitarea numarului de procesoare folosite de baza de date fara a fi necesara folosirea unei solutii de virtualizare;
- trebuie sa ofere un mecanism de connection pooling care sa optimizeze folosirea resurselor server-ului la operatiile de tip login/logout

Baza de date trebuie sa permita functionarea intr-o arhitectura de disponibilitate inalta de tip cluster activ-activ asigurandu-se toleranta la defecte hardware sau nefunctionare planificata, scalabilitatea si disponibilitatea crescuta a sistemului. Din punct de vedere al performantei bazei de date, fiecare nod al cluster-ului bazei de date trebuie sa poata fi capabil sa acceseze date din memoria cache a celorlalte noduri reducand astfel la minim necesitatea de a citi blocurile de date direct de pe disc Totodata arhitectura de tip cluster trebuie sa ofere o disponibilitate de tip 24x7 in cazul aparitiei unei defectiuni hardware la unul din serverele cluster-ului de baza de date. Securitatea tranzactionala in cazul aparitiei unor erori hardware sau software in clusterul de baza de date trebuie sa fie tratata de mecanismele interne ale bazei de date iar in cazul unei defectiuni hardware si/sau software sa permita reconectarea automata la nodul sau nodurile ramase disponibile.

Din punct de vedere al operatiunilor de administrare baza de date trebuie sa ofere mecanisme interne de monitorizare si diagnosticare continua si care sa puna la dispozitia administratorilor informatii pentru usurarea luarii deciziilor in administrare, automatizand colectarea de paramteri

de funcţionare ai bazei de date, precum si stocarea acestora pentru a putea furniza o imagine pe termen lung a modului de funcţionare a bazei de date. Solutia de baza de date trebuie sa ofere un utilitar grafic pentru modelarea relaţională şi dimensională a datelor precum si o unealta cu interfata grafica accesibila web pentru administrarea bazei de date, care sa includa urmatoarele facilitati:

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

Din punctul de vedere al operatiunilor de backup, baza de date trebuie sa permita operatiuni de backup si restaurare a datelor in regim de lucru online, salvarea totala si/sau partiala a bazei de date atat pe disc cat si direct pe banda iar toate aceste operatiuni sa fie facute intr-o forma unitara, centralizata si usor de administrat. De asemenea pentru optimizarea timpului alocat acestor operatiuni baza de date trebuie sa permita compresia si efectuarea de backup incremental si sa permita citirea si scrierea paralela (simultan din/in mai multe fisiere) in timpul operatiilor de backup si restore. In functie de nevoie baza de date trebuie sa permita, pe baza datelor de backup restaurarea partiala asigurand o imagine consistenta a acesteia de la un moment de timp specificat de cel ce realizeaza operatia de restaurare. Pentru asigurarea consistentei datelor in situatia nefavorabila a unui incident, baza de date va permite interogarea directa a tabelelor afectate, prezentand imaginea datelor exact asa cum erau acestea la un moment anterior in timp si va permita anularea unei tranzactii care a fost comisa sau chiar restaurarea rapida a datelor la nivel de tabela.

Ca si mecanisme de securitate oferite, baza de date trebuie sa permita aplicarea simultana a mai multor politici de securitate pe un acelasi obiect al bazei de date precum si posibilitatea de a restrictiona accesul utilizatorilor la nivel de inregistrare si coloana intr-o tabela. Din prisma activitatilor de audit baza de date va oferi o lista cu operatiile pe care un grup sau o clasa de utilizatori le poate executa si va avea abilitatea de a se ajusta la gradul de detalii, capturate de catre facilitatea de audit prin introducerea de politici de audit care sa determine cand un utilizator este sau nu auditat (spre exemplu situatia cand utilizatorul acceseaza doar anumite informatii dintr-o tabela sau cand conectarea nu se face printr-o anumita aplicatie).

3.8.4. Componenta de Business Intelligence

Componenta de Business Intelligence (analiza si raportare) va avea rolul de a permite accesul din interfata web, mobil sau PC la informatii si analizate avansate sub forma de rapoarte si dashboard-uri prezentate sub diverse forme (tabular, graphic, harta, combinatii de reprezentari). Modulul trebuie sa permita analize avansate si integrarea cu multiple surse de date, atat interne institutiei, dar si externe, pentru a permite lucratorilor sa ia decizii informate si de a trimite rapoarte si analize statistice catre alte institutii sau intern.
In cadrul solutiei, va exista posibilitatea de vizualizare de rapoarte si dashboard-uri intr-un mod dinamic, si cu posibilitati avansate de a interactiona direct cu datele (capabilitati de tipul "drill").

Componenta de business intelligence va oferi o interfata web prin care utilizatorii sa poata interactiona cu toate componentele sistemului, atat pentru accesul la rapoartele si tablourile de bord existente, cat si pentru a crea noi analize ad-hoc. Componenta de BI va oferi posibilitatea de a prezenta informatia in formate multiple cum ar fi grafice, tabele, tabele pivotante, combinatii de grafice si tabele, harti, iar atunci cand un raport include o reprezentare multipla (ex text si grafic) a aceleiasi informatii, componenta de business intelligence va trebui sa permita afisarea informatiei fara a repeta executia interogarii. Pentru o mai buna vizualizare si intelegere a informatiilor afisate, este necesar ca aplicatia de raportare sa poata afisa pe o harta anumite valori identificate ca si critice, sa semnalizeze depasirea unor praguri ale acestor valori, sa semnalizeze aparitia unor evenimente.

Componenta de BI trebuie să ofere posibilitatea modelarii datelor si prezentarii informatiei intr-un format familiar utilizatorilor finali, astfel incat acestia sa poata accesa informatiile disponibile fara a cunoaste structura si particularitatile fiecarei baze de date accesate. Acest nivel de metadate expus utilizatorilor trebuie sa fie comun la nivelul tuturor modulelor sistemului de raportare si analiza.
În cadrul acestei componente, rapoartele vor putea fi construite pe baza datelor existente in diverse surse de date structurate sau nestructurate, de pe platforme diferite (Oracle, SQL Server, DB2, SQL Anywhere, fisiere de tip csv, fisiere xls, fisiere txt, etc.), in mod transparent pentru utilizatorul final.

Rapoartele analitice vor putea fi construite pe un numar variabil de interogari analitice, fara ca instrumentul de business intelligence sa limiteze numarul de astfel de interogari. O aplicatie de analiza sau raportare trebuie sa nu fie limitata la un anumit numar de surse de date, si sa permita analiza simultana a fara a se limita la un anumit numar de surse de date.
Modulul de Business Intelligence trebuie sa permita conectarea la sursele de date interne, dar si adaugarea de surse de date externe, crearea de asocieri automate sau manuale intre diferitele surse de date, tabele si incarcarea acestor date in memorie pentru analize performante si de mare viteza.
Numarul de utilizatori al solutiei de tip BI este de 50.

Cerinte functionale
Pentru intelegerea mai buna a informatiilor prezentate, componenta de BI trebuie sa aiba urmatoarele functionalitati generale:

- Posibilitatea de drill down / drill up (afisarea datelor aggregate si detalierea acestora pe baza ierarhiilor implementare) sau drill through (posibilitatea de a naviga catre un alt raport/dashboard preluand contextul raportului din care s-a declansat actiunea), atat pentru rapoarte cat si pentru grafice.
- Trebuie sa permita analiza In-Memory pentru o performanta ridicata si pentru lucrul cu volume mari de date.
- Trebuie sa permita crearea de modalitati de vizualizare moderne prin tehnici avansate de intelegere si asociere a datelor
- Trebuie sa permita conectarea simultana la multiple surse de date si crearea automata a unui model asociativ a datelor pentru a nu limita analiza si raportarea la modele ierarhice
- Trebuie sa permita asocierea automata a datelor din diverse surse pe baza informatiilor identificate in surse si sa recomande automat cele mai potrivite asocieri

- Trebuie sa permita identificarea automata, direct din surse de date a eventualelor anomalii sau redundante
- Trebuie sa permita crearea de mai multe pagini de calcul in cadrul aceleiasi aplicatii de analiza si pastrarea selectiilor facute anterior pentru o analiza consistenta
- Trebuie sa permita salvarea ca "bookmark-uri" a anumitor selectii specifice pentru analize rapide sau generarea de rapoarte rapide
- Trebuie sa permita crearea de prezentari dinamice direct din aplicatiile de analiza cu descoperiri din date, rapoarte si statistici si din prezentare sa se poata intra imediat in aplicatie pentru detalii suplimentare din aceeasi interfata
- Trebuie sa permita inserarea de imagini grafice, text, adnotari in prezentarile de raportare direct din aplicatiile de analiza si raportare (interfata de prezentare/analiza)
- Trebuie sa permita o cautare in toate datele analizate direct din interfata de analiza
- Trebuie sa permita capabilitati avansate de integrare a datelor, prin crearea de legaturi din surse de date multiple, fara a fi nevoie de aplicatii externe (pentru modelarea datelor de ex.) sau "Data Warehouse"
- Trebuie sa permita crearea modelului de date analizate direct in memoria serverului, intr-o maniera dinamica, automata.
- Trebuie sa nu aiba restrictii la numarul de aplicatii de analiza, aplicatii de tip panou de bord, sau numarul de rapoarte generate
- Aplicatiile de analiza si rapoartele trebuie sa poata fi accesate dintr-un portal web din intranet sau internet de un numar nelimitat de utilizatori (care vor avea drept de « read »/doar vizualizare a rapoartelor)
- Trebuie sa contina o interfata adaptabila automat la orice dispozitiv mobil de tip smartphone sau tableta
- Trebuie sa permita integrarea de aplicatii de analiza in orice interfata web – analize incorporate
- Trebuie sa permita utilizatorilor cu drepturi corespunzatoare crearea/modificarea de aplicatii si pagini personalizate pe model de analize self-service, pe care ulterior sa le poata face publice / accesibile de catre alti utilizatori
- Trebuie sa permita publicarea analizelor personalizate intr-un flux colaborativ pentru a permite accesul mai multor utilizatori la aplicatii personalizate
- Va permite accesarea informatiilor prin portalul de business intelligence, iar prin folosirea functionalitatilor instrumentului de raportare, va permite salvarea rapoartelor in diferite formate cum ar fi Excel, PDF, Word, HTML, Powerpoint etc.
- Componenta de business intelligence va permite modificarea tablourilor de bord sau a rapoartelor (fara costuri de licentiere suplimentare) si va oferi posibilitatea includerii rapoartelor/graficelor in tablouri de bord pentru toti utilizatorii finali, fara costuri de licentiere suplimentare. xxx
- Trebuie sa permita crearea si configurarea pe baza unui orar prestabilit de trimitere de rapoarte in format Word, PDF, Excel, HTML via email sau intr-o locatie de stocare accesibila centralizat.
- Componenta de BI nu trebuie sa limiteze accesul utilizatorior la o singura sursa de date, permitand combinarea rezultatelor obtinute de pe platforme diferite la momentul interogarii, astfel incat setul de date rezultat sa fie unitar. Pentru functionare optima si cu performanta ridicata, componenta de business intelligence trebuie sa se poata conecta simultan la multiple surse de date, sa incarce in memoria serverului de analiza datele necesare folosind algoritmi de compresie avansati, si sa permita analiza asociativa, nerestrictionata de anumite interogari SQL specifice.

- Trebuie sa permita utilizatorilor sa descopere informatii, fara a fi necesare cunostinte de baze de date sau limbaj SQL. De asemenea, nu trebuie sa limiteze la o anumita structura ierarhica analiza de informatii, ci in momentul selectarii oricarui camp de date sa asocieze automat acel camp cu informatiile relevante si nerelevante intr-o interfata grafica intuitiva.
- Solutia trebuie sa beneficieze de un motor de cautare avansat, care sa permita cautarea in toate sursele de date analizate dar si in obiectele de vizualizare (rafice, tabele, etc.) astfel incat un utilizator sa poata accesa rapid si in orice moment informatii de raportare si analiza specifice.
- Utilizatorii sistemului vor putea fi preluati din sisteme LDAP, insa componenta de raportare va trebuie sa ofere capabilitati proprii de definire a rolurilor pentru restrictionarea in detaliu a accesului la rapoarte. Alternativ, solutia va putea fi integrata prin mecanisme proprii cu baza de date cu utiliatori fara sa fie nevoie replicarea acesteia.
- Instrumentul de raportare trebuie sa ofere un mecanism de programare a executiei rapoartelor sau a preincarcarii in serverul de BI a unui set de date astfel incat sa minimizeze timpii de executie ai interogarilor analitice, in functie de sursele de date.
- Componenta de BI va trebui sa permită vizualizarea trasabilitătii unei componente dintr-un raport, si dacă aceasta reprezintă o valoare calculată să permită vizualizarea formulei de calcul utilizate, integrand informatiile de calcul din instrumentul de business intelligence cu reguille de transformare aplicate in instrumentul de ETL. Componenta de Business Intelligence trebuie sa aiba integrat propriul modul ETL.

Cerințe pentru componenta de raportare cu format fix

Această componentă trebuie sa asigure posibilitatea de generare de rapoarte cu continut fix pentru utilizatorii care nu au, prin natura activităţii pe care o desfasoara, necesitati de modificare de rapoarte sau creare de rapoarte noi sau în cazul rapoartelor de natura oficiala, cu forma fixa, destinate consumului în masa sau imprimarii şi distribuirii în forma fizica.

Solutia de Business Intelligence trebuie sa beneficieze de un modul de generare, distributie si planificare automata de rapoarte catre utilizatori cheie.

Rapoartele trebuie sa poata fi trimise automat la anumite ore prin email in format PDF sau Microsoft Office. Calitatea imaginilor grafice din rapoarte trebuie sa fie foarte buna pentru a permite vizualizarea graficelor dar si marire de calitate (zoom in).

Solutia trebuie sa permita crearea si publicarea de rapoarte in format HTML pentru a putea fi afisate usor pe orice site web.

Crearea de rapoarte pentru distributie trebuie sa se faca din simplu din aplicatiile de analiza, folosind actiuni de tip drag-and-drop, editor dedicate de rapoarte, creare, atasare si editare de imagini grafice.

Un raport trebuie sa permita consolidarea de informatii din mai multe aplicatii de analiza, care la randul lor acceseaza una sau mai multe surse de date.

Rapoartele trebuie sa poata fi trimise automat, si in functie de utilizatorii recipient sa permita filtrarea informatiilor persoanlizate pentru utilizatori.

Rapoartele trebuie create si gestionate centralizat pentru a fi distribuite in functie de necesitati la un numar are de recipient.

Componenta de raportare cu format fix va permite reprezentarea informatiei atat in format tabular cat si in format grafic. Selectia datelor ce urmeaza a fi afisate in aceste rapoarte se va face dinamic, utilizatorul putand preciza la momentul de executiei criteriile de filtrare a informatiei.

Din punct de vedere al surselor de date, componenta de raportare cu format fix trebuie sa permita accesarea informatie din surse de date de tehnologii diferite cum ar fi:

- baze de date relationale: SQL Server, Oracle, DB2, etc.

- baze de date multidimensionale: SQL Analysis Services, Oracle OLAP, etc.
- fisiere: XML, CSV/Tab, Excel, MDB.
- Servicii Web.

Cerinte de platforma

- Componenta de analiza si raportare manageriala trebuie fie scalabila si sa dispuna de mecanisme de clustering a componentelor (de prezentare sau la nivel de server de acces la date), astfel incat sa poata fi folosite resurse hardware suplimentare.
- Componenta de BI va oferi functionalitati de incarcare a datelor si analizelor direct in memoria serverului pentru optimizarea performantei si pentru a evita supra-incarcarea surselor de date tranzactionale.
- Componenta de raportare trebuie sa ofere suport pentru functionarea si in cazul in care unul din servere este nefunctional (de exemplu mentenanta sau defect), fara ca utilizatorul sa fie deconectat de la sistem (continuarea activitatii trebuie sa fie transparenta pentru utilizatori).
- Modulul de analiza si raportare trebuie sa detina propriul modul SDK care sa permita conectarea via web service pentru printarea de rapoarte, crearea, copierea sau stergerea de rapoarte sau obiecte analizate, schimbarea modelului de Securitate si adaugarea sau monitorizaarea performantei
- Platforma trebuie sa permita rapid crearea de solutii compatibile cu standardul JSR168, Web Services, sau alte standard de integrare portal
- Modulul de BI trebuie sa poata fi accesat via portal sau direct de pe statii de lucru Windows, Mac OS sau Linux
- Modulul de raportare trebuie sa fie compatibil cu o serie de standard deschise cum ar fi: Websockets, REST, HTML5, CSS3, Javascript, ODBC, OLEDB, LDAP, ActiveDirectory, TLS/SSL, XML
- Trebuie sa suporte integrarea Microsoft Active Directory NTLM/Kerberos si/sau alte sisteme LDAP
- Toate informatiile in tranzit trebuiesc sa fie criptate cu TLS
- Platforma trebuie sa ofere un set complet de API-uri si sa permita dezvoltarea web folosind tehnologii ca HTML5, JavaScript si CSS
- Modulul de BI trebuie sa permita securitate avansata, acces diferentiat pe roluri al utilziatorilor, acces diferentiat la aplicatii de analize diferite
- Modulul trebuie sa permita instalarea tuturor componentelor sale pe un singur server, cu posibilitatea de a fi scalabil usor intr-o arhitectura de inalta disponibilitate si balansarea incarcarii
- Administrarea utilizatorilor, monitorizarea performantei si gestionarea accesului trebuie sa se faca centralizat, dintr-o interfata de administrare web
- Utilizatorii care creaza aplicatii de analiza, raportare si vizualizare a datelor trebuie sa beneficieze de un instrument de tip "asistent de creare" aplicatii de vizualizare, dar si posibilitatea accesarii lor prin script-uri
- Aplicatiile si obiectele utilizate in analiza trebuiesc sa fie create prin metode simple de tip "drag and drop"
- Modulul trebuie sa aiba un asistent de incarcare a datelor, care sa creeze legaturi automat sau manual intre diferite surse de date, cum ar fi: baze de date ODBC, pagini web, fisiere Excel, etc.

- Platforma trebuie sa permita crearea de grupuri de aplicatii specific pe fiecare linie de serviciu si restrictionarea accesului utilizatorilor catre aplicatii din liniile de care nu apartin
- In cadrul unui grup de aplicatii, configurarea utilizatorilor si rolurilor trebuie sa permita restrictionarea doar la anumite aplicatii, dar si in cadrul aplicatiilor de analiza doar la informatii specifice rolului (de exemplu: utilizator din Ilfov sa aiba acces doar la infromatii din judetul Ilfov in cadrul aceleieasi aplicatii de raportare cu date din toata tara)
- Platforma trebuie sa contina propriul modul ETL integrat si posibilitatea de normalizare si pregatire scriptica a datelor pentru analize
- Platforma trebuie sa permita crearea unui model de date unitar care sa poata fi folosit de mai multe aplicatii de analiza si raportare

3.8.5. Componenta de mascare a datelor

Sistemul propus asigură confidenţialitatea informaţiilor necesare pentru operare, accesul la interfaţa de administrare făcându-se pe baza de nume de utilizator şi parolă. Totodată sistemul asigură integritatea datelor transmise, actualizate, vizualizate sau înregistrate.
Toate informaţiile despre utilizatori vor fi confidenţiale în limitele stabilite prin politica de securitate. Aceste limite sunt stabilite în funcţie de rolul pe care îl are fiecare utilizator în cadrul sistemului informatic propus. De asemenea se vor respecta legislaţia şi reglementările internaţionale privind protecţia intimităţii şi a datelor personale.
Prin intermediul unei componente specializate de administrare, persoanele acreditate (administratori de sistem) vor putea restricţiona accesul în anumite zone ale sistemului informatic, la anumite documente sau date, după cum va fi necesar, pentru a acorda drepturi doar anumitor utilizatori sau grupuri de utilizatori.
Cu ajutorul acestei politici, utilizatorii vor putea vizualiza, modifica sau adăuga documente/înregistrări numai în limita drepturilor de acces asociate, asigurându-se confidenţialitatea datelor.
Din motive de securitate parolele utilizatorilor nu vor fi păstrate în baza de date, ci se vor păstra criptate într-un director LDAP centralizat.

Cerinţe pentru componenta de mascare a datelor
În vederea îndeplinirii obiectivelor stabilite cu privire la mediul de testare/dezvoltare şi totodată pentru asigurarea confidenţialităţii informaţiilor şi protejării datelor cu caracter personal, sistemul informatic va inlcude o componentă de mascare pentru transferul din bazele de date de producţie în cele de testare/dezvoltare.
Astfel se asigură prevenirea accesului utilizatorilor neautorizati la informatiile sensibile, dar asigură accesul personalului IT si echipelor externalizate la date de test consistente, îndeplinind in acelasi timp regulile de conformare privind confidenţialitatea şi protecţia datelor cu caracter personal.
Existenta unor date de testare consistente si suficiente reprezintă o necesitate pentru realizarea unui proces de testare eficient si concludent, fără date de testare similare condiţiilor de utilizare extreme (atât din punct de vedere cantitativ cat si calitativ) orice testare realizata asupra sistemului nu va fi relevanta referitor la funcţionarea acestuia in producţie.
Soluţia trebuie sa îndeplinească următoarele caracteristici tehnice minime:

- Soluţia trebuie să poata profila date existente pentru descoperirea automata a modelului de date şi a conţinutului sensibil.
- Soluţia trebuie să asigure generarea de date în conformitate cu următoarele formate:

  - Oracle DB Server, MySQL
  - Microsoft SQL Server
  - PostgreSQL, Ingres
  - Sybase
  - Fişierele XML, SQL, CSV, fişiere JSON, fişiere HTML
- Soluţia trebuie să permită să repete procesul de generare a datelor dupa ce modelul de date a fost definit,, în scopul de a recrea datele pentru testele.
- Soluţia trebuie să dispună de posibilitatea creării de date invalide, bazate pe cererile utilizatorilor
- Soluţia trebuie să fie capabilă să modifice date sensibile cu un conţinut alternativ. O astfel de capacitate trebui să includă următoarele funcţii:
  - Conservare genului - atunci când substituirea nume, nume masculine sunt substituite numai cu alte nume de sex masculin, şi în mod similar de sex feminin, cu doar nume feminine.
  - Conservarea integrităţii semantice - păstrarea constrângerilor aplicate unui set de date ca o valoare maximă sau pentru numere de card de credit
  - Valoarea Cumulată - valorile totale şi medii ale unei coloane mascată de date ar trebui să fie păstrate, fie strâns sau cu precizie
- Abilitatea de a extrage în mod condiţionat seturi de date intacte referenţial, în mod constant din multiple tipuri de baze de date sau fişiere
- Soluţia trebuie să dispună de capacitatea de a asocia cazuri de testare cu atributele de date necesare, de a le găsiţi în conţinutul de date existente şi de a le rezerva pentru utilizatori autorizaţi.
- Soluţia trebuie să aibă capacitatea de a descoperi automat relaţiile între date şi să ofere, de asemenea, posibilitatea administratorilor să modifice regulile de descoperire utilizate.
- Soluţia trebuie să furnizeze o analiză a datelor şi a metadatelor bazelor de date descoperite
- Urmare a procesului de descoperire, soluţia trebuie să furnizeze rapoarte şi documentare privind datele descoperite.
- Soluţia trebuie să dispună de capacitatea de a înţelege modelele de date, în scopul de a menţine integritatea referenţială într-o bază de date. De asemenea, soluţia trebuie să fie capabilă de a înţelege modelele de date, în scopul de a menţine integritatea referenţială între diferite baze de date.
- Soluţia trebuie să dispună de posibilitatea modificării datelor generate
- Soluţia trebuie să fie capabilă să ruleze într-un mod de test regulile de anonimizare pentru a testa efectul pe care îl are mascarea, înainte de a aplica mascarea la datele complete existente
- Soluţia trebuie să permită o mascare directă a datelor
- Soluţia trebuie să permită programarea rulării funcţiilor de mascare a datelor.
- Soluţia trebuie să fie capabilă să lucreze şi cu date care nu sunt 100% corecte, pentru a putea folosi aceste date greşite în timpul procesului de testare. Soluţia trebuie să fie configurabilă ca şi aceste date să fie prelucrate.
- Soluţia trebuie să fie capabilă să genereze date invalide pentru a fi folosite in teste specifice.
- Soluţia trebuie să ofere posibilitatea extragerii unui subset de date care să fie mascate şi să poată fi prelucrate în procesul de testare.
- Soluţia trebuie să suporte autentificarea folosind integrarea cu sisteme de tip LDAP
- Soluţia trebuie să ofere mecanisme de control a accesului la date bazate pe utilizatori, roluri şi grupuri
- Soluţia trebuie să ofere suport pentru utilizatori dintr-un director LDAP cu posibilitatea de criptare a transportului folosind TLS (LDAPS)

- Soluția trebuie să ofere rapoarte care sa evidențieze date vulnerabile care trebuiesc mascate
- Soluție trebuie să fie capabilă să identifice dimensiuni de date care există în mediul de producție și să lege aceste informații fie cu informații personale sintetice sau informații mascate pentru a crea date similare celor din producție, care să poată fi provizionate, fără să conțină date reale
- Soluția trebuie să conțină o interfață tip portal prin care se va face administrarea datelor, înregistrarea și rezervări de date.
- Soluția trebuie să permită construcția de teste și procese folosind metodologia Agile.

3.8.6. Componentele de gestiune a utilizatorilor si de securitate

Din punct de vedere al componentelor necesare pentru a asigura cerintele de gestiune a utilizatorilor si de securitate prezentate in prezentul proiect, au fost identificate urmatoarele:

1. *Componenta de securizare acces servicii electronice* – care va securiza accesul la serviciile electronice catre beneficiarii acestui sistem si pentru securizarea accesului integrarii la nivel de servicii web
2. *Componenta de control al accesului utilizatorilor la sistem* - va asigura in principal:
   a. Control al accesului la componentele de aplicatii web si portal si Single Sign On
   b. Administrare centralizata a politicilor de acces la aplicatii si servicii
   c. Evaluare a riscurilor legate de conectare si acces
3. *Componenta de stocare centralizata a profilelor de utilizator (LDAP)* - va asigura gestionarea stocarea efectiva a informatiei despre utilizatori si grupurile de securitate definite
4. *Componenta de administrare unitara a profilelor de utilizato*r:
   a. Gestionarea automatizata de conturilor de utilizatori in sistem in functie de politici de acces la resurse
   b. Vedere unitara a tuturor resurselor alocate unui utilizator
   c. Integrareadirecta cu toate componentele functionale din cadrul sistemului pe baza de tehnologie fără agenti
   d. Raportari evenimente de securitate si auditare avansata
5. *Componenta de autentificare securizată a utilizatorilor*
6. *Componenta de monitorizare a logurilor si traficului de retea* - va permite monitorizarea log-urilor de la componentele sistemului precum si a fluxurilor de comunicații prin preluarea traficului de la dispozitive de tip TAP
7. *Componenta de securizare a accesului la bazele de date* – va asigura testarea vulnerabilităților bazelor de date, descoperirea și clasificarea datelor confidențiale și va monitoriza accesul utilizatorilor la bazele de date conform politicilor implementate

3.8.6.1. Securizare Acces Servicii Electronice

Datorita cerintelor de integrare ale sistemului PSCID cu sisteme externe, este necesara securizarea accesului la serviciile web expuse către aceste sisteme externe si de a scadea costurile operatiunilor administrative legate de controlul accesului la aceste servicii, prin implementarea unei componente de securizare a accesului la interfete web in mod centralizat.
Avand in vedere rolul important al acestei componente se solicita implementarea unei solutii de tip „COTS", care sa satisfaca cel putin urmatoarele cerinte functionale si tehnice:

- Soluția va avea capacitatea de a comunica și de a schimba date cu acuratete, în mod eficient, sigur și constant cu diferite sisteme informatice, aplicații software și retele în diverse setari, asigurând procesele de lucru operaționale ale institutiilor implicate.
- Solutia Gateway WS/API va oferi o arhitectura de tip proxy de servicii web — de tip Web Services si API - Application Programming Interface cu functionalitati de translatare de date.
- Ofera capabilitati de WS/API firewall si funcții de control acces pe baza de politici de acces de tip RBAC
- Solutia trebuie sa realizeze conversia XML-JSON direct fara a fi nevoie de scheme separate pentru XML si JSON. Tranformarea XML-JSON trebuie sa fie bidirectionala, XML-JSON si JSON-XML
- Solutia trebuie sa detecteze automat atasamentele SOAP
- Solutia trebuie sa permita definirea si detectarea de atasamente neasteptate sau incompatibile, precum fisere executabile.
- Solutia trebuie sa detecteze cererile XML inclusiv daca acesta sunt nested.
- Solutia trebuie sa detecteze cererile XML cu un numar foarte mare de atribute ceea ce indica un atac la nivel de continut

Solutia trebuie:

- Sa limiteze marimea documentului XML incluzand sau nu dimensiunea atasamentului
- Sa detecteze vulnerabilitati de genul SQL-injection sau XPATH-injections
- Sa poata limita numarul de mesaje pe o perioada de timp: pe secunda, pe minut, pe ora si pe zi
- Sa poata limita numarul de conexiuni concurente catre un anumit serviciu web expus
- Sa poata preveni atacuri de tip "replay": mesaj autentic cu credentiale valide repetat de foarte multe ori
- Sa aiba posibilitatea stergerii, inlocuirii, criptarii sau mascarii de date confidentiale
- Solutia trebuie sa monitorizeze tranzactile in timp real si sa permita vizualizarea statisticilor pe perioade de timp.
- Sa aiba un mechanism de alertare in cazul detectarii de activitati/interogari cu un volum anormal de date
- Sa poata cripta si decripta mesaje XML
- Sa suporte WS-Security si XML Encryption
- Sa valideze semnatura pentru a determina daca un mesaj este de incredere
- Sa valideze cerificatele pe baza unei liste de certificate revocate
- Sa poata bloca accesul de la o lista de ip-uri sau subnet-uri
- Sa poata permite accesul pe baza unei liste de adrese IP sau subnet
- Sa permita urmatoarele metode de autentificare:
  - HTTP Basic si HTTP Digest
  - WS-Security Username token si Binary Security token
  - Security Assertion Markup Language (SAML) assertion
  - Certificat X.509
  - ticket Kerberos
  - token OAuth
  - cheie API
  - Token Web JSON
- Sa suporte SAML 1.2 si 2.0.

- Sa poata fi integrat cu solutii de tip directory incluzand directoare compatibile LDAP v.3, RADIUS si Microsoft ActiveDirectory
- Sa blocheze accesul pe baza de context si attribute: ora, inceracri de login, locatia ultimului login
- Sa poata converti alte tipuri de tokenuri intre-un token SAML.
- Sa aiba o functie de Cache al tokenului pentru a oferi functionalitatea de SSO peste mai multe backenduri care ofera servicii web
- Sa poata monitoriza si alerta in cazul in care unul sau mai multe servicii API expuse nu sunt disponibile
- Sa poata monitoriza si alerta in cazul in care unul sau mai multe servicii API expuse au o performanta deteriorate, sub nivelul unei limite pentru: timp de raspuns si numar de reincercari
- Sa poata prioritiza traficul pe baza clientului, utilizatorului si attribute de servicii
- Sa dispuna de un mecanism de cache pentru:
  - rapunsuri la interogari care sa reduca traficul catre backend-uri,
  - atribute interogate din surse externe
  - tokenuri de Securitate pentru evitarea cererilor repetate de autorizare si autentificare
- Sa ofere tablouri de bord si rapoarte configurabile
- Sa ofere flexibilitate pentru auditarea evenimentelor, permitand configurarea tipurilor de evenimente auditate
- Sa permita logarea evenimenteleor la nivel de servicii, client, si tranzactii
- Sa ofere urmatoarele optiuni de logging:
  - fisier log local
  - server Syslog
  - Windows Event Log
  - Baza de date
  - trap SNMP
  - Email
- Sa permita posibilitatea separarii evenimentelor de securitate de cele care privesc tranzactiile
- Să permită definirea de servicii web şi api pentru aplicaţii care nu au aceste funcţionalităţi implementate.

3.8.6.2. Controlul accesului utilizatorilor la sistem

PSCID va fi compus din mai multe componente, fiecare indeplinind cerinte functionale specifice. Pentru a se asigura un control al accesului centralizat, unificarea experientei de utilizare dar si pentru a creste nivelul de securizare si a scadea costurile operatiunilor administrative legate de controlul accesului la aplicatiile si componentele sistemului, se doreste implementarea unei componente de securizare a accesului la interfete web in mod centralizat. Avand in vedere rolul important al acestei componente se solicita implementarea unei solutii de tip „COTS", care sa satisfaca cel putin urmatoarele cerinte functionale:

- Sa protejeze resursele de tip web impotriva acceselor neautorizate – atât din interiorul cat si din exteriorul retelei
- Nici o resursa web din interiorul sistemului nu trebuie sa poată fi accesata direct din exterior, orice acces realizandu-se prin intermediul serverelor web proxy
- Sa integreze controlul accesului pentru componentele sistemului
- Sa ceara utilizatorilor sa introduca date de identificare pentru accesul la aplicatii

- Sa permită impunerea unor filtre de acces (operațiuni de autorizare) – cel putin interval orar si locatie de retea de unde s-a initiat cererea de acces
- Sa permită administratorului sistemului sa aleaga metode de autentificare si autorizare diferite pentru fiecare grup de resurse in parte
- Sa ofere o interfață de administrare de tip web pentru accesul facil la configurari, care sa poată fi accesata doar de către administratorii de securitate ai solutiei
- Sa ofere SSO – autentificare unica pentru accesul la resurse; pe parcursul unei singure sesiuni de lucru utilizatorul fi autentificat o singura data, dupa care va putea accesa fără reautentificare toate aplicatiile web pentru care are drept de acces.
- Fiecare utilizator sa fie identificat de sistem pe baza unei sesiuni
- Sistemul sa permită administratorilor terminarea manuala a sesiunilor utilizatorilor
- Dupa un timp configurabil de inactivitate sesiunile utilizatorilor trebuie sa fie terminate in mod automat
- Numarul de sesiuni pe care un utilizator le poate deschide trebuie sa poată fi limitat de către administratori
- Toate evenimentele de acces – autentificari reusite, autentificari nereusite, autorizari reusite, autorizari nereusite trebuie sa poată fi auditate
- Datele colectate prin auditarea accesului trebuie sa fie stocata într-o baza de date pe care sa poată fi rulate in caz de nevoie rapoarte
- Solutia trebuie sa implementeze urmatoarele reguli pentru a valida o parola noua:
  1. Compunere parola
     - numar minim/maxim de caractere pentru parola
     - case sensitive – case insensitiv
     - numar minim de caractere alpha numerice (cifre si litere)
     - numar minim de caractere non-alpha numerice (caractre speciale, punctuatie, non-printabile)
     - numar minim de caractere speciale
     - numar minim de caractere de punctuatie
     - numar minim de caractere non-printabile
     - numar maxim de caractere repetitive
     - datele personale (de exemplu, nume prenume) nu trebuie sa fie continuta in parola.
  2. Expirare parola
     - numarul de zile pana cand utlizatorul trebuie sa isi schimbe singur parola
     - numarul de autentificari esuate inainte de a dezactiva userul
     - numarul de zile de inactivitate inainte de a dectiva user-association
  3. Reutilizare parola
     - procentul de caractere din noua parola care trebuie sa difere in ultima parola.
     - numarul de parole inainte de a putea refolosi o parola noua
     - numarul de zile inainte ca un utilizator sa poata refolosi o parola
     - daca o parola a expirat, atunci solutia trebuie sa autentifice utilizatorul o singura data si sa forteze schimbarea parole.
- Administrarea utilizatorilor trebuie sa suporte urmatoarele servere ldap: Microsoft Active Directory, Microsoft AD Global Catalog, Microsoft Active Directory Lightweight Directory Services (LDS), IBM Tivoli Directory Server, CA Directory, Open Ldap, Oracle Internet Directory, Red Hat Directory Server
- Toate componentele software ale solutiei de control acces trebuie sa permită rularea in mod disponibilitate ridicata

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

- Stocarea configuratiilor si a politicilor de acces la resursele web sa se realizeze într-o baza de date, fără a exista nevoia unui depozitar proprietar de date
- Sa permită accesarea simultana a mai multor surse de identitati pentru realizarea autentificarii si autorizarii
- Toate politicile de control al accesului trebuie sa poată fi definite utilizand interfață web a solutiei, fără a necesita cunostinte de programare sau rularea de scripturi pe server
- Sa suporte cel putin urmatoarele metode de autentificare:
    - Nume de utilizator si parola
    - Certificate digitale x.509
    - Smart card
    - Token-uri fizice cu PIN
    - API-uri de autentificare pentru dezvoltari
- Schimbarea comportamentului standard (refuza acces sau permite acces pentru resursele neprotejate)
- Nivelul de auditare trebuie sa fie configurabil (succes, nereusita, etc)
- Sa realizeze criptarea informatiei transferata intre componentele sistemului si clienti
- Solutia de control acces sa ofere integrare cu solutia de stocare a profilelor de utilizatori si cu cea de administrare unitara a profilelor utilizatorilor
- Solutia de control acces trebuie sa fie implementata folosind o arhitectura pe mai multe nivele. De exemplu:
    - Nivel server de acces- server central de control acces, care primeste si trateaza cererile de autentificare, autorizare si auditare
    - Nivel proxy - integrare cu serverele web de tip proxy pentru blocarea tentativelor de acces la resursele protejate
    - Nivel de integrare – solutia de control acces trebuie sa foloseasca directorul centralizat de utilizatori al solutiei (LDAP)
    - Nivel de stocare – datele sistemului de control acces (politici de acces, date de auditare) trebuie sa fi stocate într-o componenta specializata de tip baza de date, separat de serverele de acces pentru a asigura ca toate serverele de acces au acces la aceleasi informații
- Sa ofere posibilitatea de rulare pe diverse platforme hardware si pe sistemele de operare majore de pe piata (Windows, Linux si UNIX)

Componenta de securizare a accesului privilegiat pentru echipamentele de tip comunicatii si servere

- Solutia trebuie sa aiba posibilitatea de a oferi acces pe baza de roluri definite pentru a evita accesul neautorizat sau al unui utilizator cu rol diferit la serverele critice.
- Solutia trebuie sa permită integrarea cu un server LDAP extern unde sunt tinuti utilizatorii.
- Solutia trebuie sa ofere posibilitatea de a oferi accesul la resurse pe baza unui program de timp care sa poată fi definit.
- Solutia trebuie sa ofere posibilitatea de a reduce controlat si granular privilegiile conturilor de tip "superuser" pentru administratorii de aplicatii Microsoft si "root" pentru UNIX/Linux.
- Solutia trebuia sa permită definirea de politici de acces la resurse pe baza criteriilor multiple: interval orar, metoda de acces, metoda de logare, etc.
- Soluția trebuie să monitorizeze integritatea fișierelor și a programelor utilizând cel putin următoarele criterii: informații aferente HDD (dimensiune fisier, proprietar fișier etc), precum

și algoritmi de digital hashing. În cazul în care un fișier monitorizat se dovedește a fi diferit de parametrii inițiali, soluția trebuie să genereze un eveniment înregistrat în fișierul de log și/sau o alertă e-mail. În cazul în care fișierul care a fost modificat reprezintă un program executabil, soluția trebuie să poată fi configurată pentru a bloca executarea programului până la momentul în care fișierul este considerat din nou de încredere.

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

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

3.8.6.3. Componenta de administrare unitara a conturilor de utilizator

Datorita specificului datelor cu caracter personal gestionate in cadrul PSCID este solicitata o componenta care sa asigure managementul centralizat al drepturilor de acces ale utilizatorilor in sistem, componenta care are un rol esential in arhitectura de securitate si administrare a sistemului. Se solicita implementarea unei solutii de tip „COTS", care sa satisfaca cel putin urmatoarelor cerinte functionale si tehnice:

- Sa ofere o imagine unitara a conturilor de acces asociate unui utilizator
- In functie de specificul fiecarui angajat in parte si de regulile din sistem, acestuia ii vor fi alocate in mod automat resurse (conturi de acces in sisteme)
- Orice schimbare in profilele de utilizatori, care ar putea avea impact asupra drepturilor de acces la alte sisteme (de exemplu schimbarea pozitiei, departamentului, etc) trebuie sa se reflecte in schimbarea rolurilor asociate utilizatorilor repectivi in mod automat
- In cazul in care un angajat este mutat pe o alta pozitie in organizatie, care implica schimbarea drepturilor de acces, componenta de administrare utilizatori trebuie sa ii revoce drepturile de acces la sistemele la care acesta nu mai are drept de acces conform noii pozitii si sa ii acorde drepturile suplimentare necesare
- In cazul in care angajatul pleaca din organizatie componenta de administrare utilizatori va trebui sa revoce automat toate drepturile de acces ale utilizatorului, astfel încât sa se previna tentativele de acces neautorizat
- Cand un utilizator pleaca din organizatie sau accesul nu mai este necesar in urma schimbarii rolului, solutia trebuie sa permită atât revocarea automata cat si manuala a acestuia , conform cu politicile de acces din sistem
- Trebuie sa expună o interfață web către utilizatori (self-service) care sa permită vizualizarea si modificarea informatiilor din profilul propriu
- Trebuie sa expună o interfață web către administratori care sa permită vizualizarea si modificarea informatiilor din profilul propriu si profilele angajatilor administrati
- Interfata expusa către utilizatori si administratori trebuie sa permită doar nivelul de acces de care acestia au nevoie, fără a afisa meniuri sau functionaliati neutilizabile de către acestia conform pozitiei si rolului in organizatie
- Sistemul trebuie sa permită lansarea de cereri pentru alocare de roluri si resurse
- Sa permită definirea drepturilor de acces ca set de baza specific pozitiei in organizatie si roluri suplimentare (care vor fi alocate la cerere, pe baza de aprobare)
- Sa implementeze fluxuri de aprobare conform structurii organizatorice pentru alocarea de resurse suplimentare regulilor de acces de baza
- Utilizatorii trebuie sa poată urmarii stadiul cererilor proprii - in timp real, la orice moment, folosind interfață grafica web
- Administratorii trebuie sa poată urmarii stadiul cererilor proprii si alocate lor - in timp real, la orice moment, folosind interfață grafica web

- Pentru depanare şi verificare, administratorii trebuie să poată urmări stadiul cererilor utilizatorilor din subordine – in timp real, la orice moment, folosind interfața grafică web, dar fără a putea interveni in fluxul solicitării.
- Pentru integrare usoară cu celelalte sisteme, fluxurile de creare/modificare/revocare conturi pentru utilizatori trebuie să fie configurabile prin interfața web.
- Pentru eficientizarea operatiunilor de resetare a parolelor, utilizatorii trebuie sa isi poată configura intrebari si raspunsuri cheie pentru resetarea parolelor de acces la resurse dintr-un punct unic (interfață web)
- Resetarea parolei de către utilizator trebuie să genereze o parolă temporară ce va fi trimisă utilizatorului prin email.
- Pentru evitarea blocajelor in operarea sistemelor (de exemplu pentru situatiile in care utilizatorii sunt temporar indisponibili), solutia trebuie sa permită administrarea delegata a drepturilor de acces
- Solutia trebuie sa ofere posibilitatea rularii periodice a unor rapoarte de utilizare (numar resetari parole intr-un interval de timp, utilizatori care au un anumit tip de cont de acces, conturi inactive)
- Sa pastreze istoricul rapoartelor rulate; pentru fiecare rulare sa ofere detalii pentru fiecare utilizator inclus in raport
- Monitorizarea periodica a modificarilor aparute in system si actualizarea drepturilor de acces conform cu noile date
- Monitorizarea conturilor orfane in sistem si executarea unor acțiuni corective automate care sa previna utilizarea frauduloasa a acestora

Administrare si Securitate

- Sistemul trebuie sa poată fi integrat cu solutia de control acces pentru asigurarea SSO (autentificare unica)
- Sistemul trebuie sa identifice utilizatorul la inceputul sesiunii de lucru (sa ceara introducerea unui nume de utilizator si parola sau integrare in SSO)
- Filtrarea accesului la activitatile din sistem trebuie sa se faca pe baza de roluri, unde rolurile reprezinta grupari logice de drepturi de acces
- Suporta politici avansate de parole: lungime parola, numar si tipuri de caractere necesare, sa impiedice reutilizarea acelelasi parole in mod repetat dupa expirare, dictionar de parole care nu trebuiesc utilizate
- Sa poată genera parole in mod automat la inregistrarea utilizatorilor
- Sa poată inregistra in sistemele destinatie parole pentru conturile de sistem administrate
- Politici de parole multiple pentru aceeasi resursa
- Operatiunile de administrare a cererilor de aprobare din sistem trebuie sa se poată realiza folosind interfață grafica a solutiei
- Alocarea de drepturi de acces către utilizatori pe baza de politici de acces asociate anumitor departamente, pozitii sau altor atribute legate de profilul utilizatorului
- Sa ofere facilitați de administrare a rolurilor de acces din organizatie, cu posibilitatea alocarii de resurse in functie de rol
- Sa permită definirea de ierarhii de roluri in mod vizual
- Pentru orice set de utilizatori, administratorii sa poată specifica nivelul de acces pentru fiecare resursa ce urmeaza a fi alocata, astfel încât fiecare utilizator sa aiba doar drepturile de acces necesare indeplinirii sarcinilor de lucru specifice

3.8.6.4. Componenta stocare centralizata a profilelor de utilizatori - LDAP

Componenta de stocare a profilelor utilizatorilor, de tip director central LDAP, va fi apelata de toate modulele solutiei pentru preluarea datelor de autentificare la aplicatii. Se solicita implementarea unei solutii de tip „COTS" care sa indeplineasca urmatoarele cerinte tehnice si functionale:

Stocare centralizata profile utilizatori

- Stocarea utilizatorilor sa se realizeze in mod centralizat
- Sa permită accesarea datelor despre utilizatori atât din baze de date cat si din directoare LDAP, cu posibilitatea de agregare selectiva a profilelor si expunerea acestor informații in format LDAP către alte sisteme
- Sa asigure securitatea datelor private
- Pentru asigurarea unui nivel ridicat de acesibilitate, sa ofere o interfață grafica web pentru consultarea datelor despre utilizatori si operarea componentei
- Sa reprezinta sursa unica de profile de utilizatori pentru autentificarea in toate componentele functionale
- Directorul de utilizatori centralizat trebuie sa fie conform cu standardul LDAP v3 sau echivalent
- Componenta trebuie sa permită integrarea cu alte sisteme fără a utiliza agenti
- Sa permită protejarea datelor la acces – autentificare la interogarea directorului (nume utilizator si parola)
- Sa permită filtrarea accesului astfel încât fiecare utilizator sa poată citi doar datele de care are nevoie
- Filtrarea trebuie sa se poată realiza la nivel de atribut LDAP
- Sa permită criptarea parolei fiecarui utilizator in parte
- Sa permită integrarea cu celelalte componente ale sistemului general astfel încât sa existe o singura sursa de utilizatori pentru toate nivelele (aplicatie, baza de date, etc)
- Sa ofere posibilitatea de rulare pe diverse platforme hardware si pe sistemele de operare majore de pe piata (Windows, Linux si UNIX)
- Să ofere interfață de administrare
- Să permită migrarea de date din alte servere LDAP (Active Directory, Oracle Directory)
- Criptarea parolelor trebuie să folosească ultimele versiuni de algoritmi, incluzând scrypt şi bcrypt
- Să permită căutări dinamice atât pentru conturi cât şi pentru grupuri

3.8.6.5. Componenta de autentificare securizată a utilizatorilor

Soluția de autentificare securizată trebuie să asigure următoarele funcționalități:

- Soluția trebuie să permită autentificarea utilizatorilor care folosesc dispozitive mobile pentru acces, indiferent de sistemul de operare şi browser-ul web al dispozitivului mobil
- Soluția trebuie să permită definirea unui template personalizat pentru zona de logare a utilizatorilor
- Soluția trebuie să permită autentificarea bazată pe 2 factori cu personalizarea metodei de autentificare pe baza de tipul utilizatorului care se autentifică

- Soluția trebuie să permită autentificarea pe baza de: OTP (one time password), RSA SecureID, Kerberos, certificare digitale X.509, HTML forms, perechi întrebare / răspuns – ca factor suplimentar față de autentificarea prin nume utilizator și parolă
- Soluția trebuie să permită integrarea cu Microsoft Active Directory sau echivalent pentru autentificarea facilă a utilizatorilor interni
- Soluția trebuie să permită integrarea LDAP pentru autentificarea utilizatorilor externi
- Soluția trebuie să permită auto-înrolarea utilizatorilor pentru primirea credențialelor de acces de tip cod acces de unică folosință (OTP) și validarea / invalidarea automată a solicitărilor pe baza tipului de utilizator sau alte criterii predefinite
- Soluția trebuie să permită autentificarea facilă a utilizatorilor înregistrați în sistem prin implementarea următoarelor funcționalități
    - Autentificarea utilizatorilor la resurse specifice se va realiza pe baza de nume utilizator și parolă
    - În cazul detectării unui nivel de risc ridicat, autentificarea utilizatorilor se va realiza prin cod acces de unică folosință (OTP), solicitată suplimentar față de nume utilizator și parolă
    - Procesul de autentificare a utilizatorilor la resurse nu trebuie să implice transmiterea parolei utilizatorului, pe canalele de comunicație, de la dispozitivul utilizator la sistemele de management al autentificării
- Soluția trebuie să permită stabilirea unei perioade de timp de inactivitate la expirarea căreia sesiunea utilizatorului este închisă automat. Perioada de timp de inactivitate trebuie să fie un parametru configurabil în cadrul soluției.
- Soluția trebuie să permită stabilirea numărului de încercări eșuate de introducere a codului de acces temporar (OTP) după care sesiunea utilizatorului este închisă automat. Numărul de încercări eșuate trebuie să fie un parametru configurabil în cadrul soluției.
- Soluția trebuie să salveze informații de audit referitoare la toate tentativele de autentificare, atât pentru tentativele eșuate cât și pentru autentificările reușite
- Soluția trebuie să permită integrarea cu metode de autentificare specifice unor anumite categorii de utilizatori, prin asigurarea de API-uri sau servicii web capabile să gestioneze credențialele de autentificare utilizate de aceste metode
- Soluția trebuie să permită implementarea de acțiuni automate în cazul încercărilor succesive de autentificare eșuate – astfel de acțiuni automate trebuie să includă închiderea sesiunii sau chiar închiderea contului utilizatorului.
- Soluția trebuie să permită stabilirea politicilor privind:
    - parolele de access: complexitate, perioadă de valabilitate
    - codurile de acces de unică folosință (OTP): complexitate, perioadă de valabilitate
    - parolele de acces la funcțiile de administrare a solutiei: complexitate, perioadă de valabilitate
- Soluția trebuie să ofere mai multe opțiuni de integrare bazate pe standarde: OATH, RADIUS, REST, SAML și SOAP.
- Soluția trebuie să se integreze cu sistemele SSO si access management
- Soluția trebuie să ofere posibilitatea de face administrare la nivel de organizatie
- Soluția trebuie să conțină minim următoarele roluri:
    - Organization admin – are privilegiile necesare pentru administrarea la nivel de organizatie,
    - User admin – are privilegiile necesare pentru adminstrare utilizatori la nivel de organizatie
    - Customer support - are privilegiile necesare pentru a lucra la cazuri și pentru a gestiona apelurile utilizatorilor finali.

- Analist - are privilegiile necesare pentru a analiza cazuri pentru a găsi tendinţe şi modele ascunse de atacuri

- Soluţia trebuie să asigure menţinerea tuturor datelor de audit privind autentificarea şi activitatea utilizatorilor şi administratorilor într-o baza de date relaţională, precum şi exportarea log-urilor soluţiei în format Syslog către sisteme externe de analiză a log-urilor
- Soluţia trebuie să ofere un set de rapoarte predefinite privind managementul şi activitatea utilizatorilor şi administratorilor – rapoarte ce pot fi vizualizate în cadrul soluţiei sau exportate către instrumente de raportare externe
- Soluţia trebuie să analizeze în timp real a riscurile pentru a proteja datele şi tranzacţiile sensibile.
- Soluţia trebuie să protejeaze atat canalele web, mobile şi să integreaze datele din toate canalele de comunicare pentru o analiză cuprinzătoare a riscurilor.
- Soluţia trebuie să efectueze o analiză transparentă, inteligentă a riscurilor pentru a oferi o mai mare siguranţă că utilizatorul este corect.
- Soluţia trebuie să asigure autentificarea securizată a utilizatorilor la resursele publicate.
- Soluţia trebuie să asigure autentificarea utilizată a utilizatorilor care utilizeaza dispozitive mobile de tip smartphone şi tabletă pentru actualizarea informaţiilor.
- Soluţia de autentificare nu trebuie să necesite modificarea aplicaţiei cu care se conecteaza. Soluţia de autentificare trebuie să se integreze cu aplicaţiile existente fără să necesite modificarea acestora.
- Soluţia de autentificare trebuie să asigure autentificarea sigură a utilizatorilor atât la conectarea acestora (login) cât şi la utilizarea unor funcţionalităţi specifice.

Soluţia de autentificare securizată trebuie să analizeze permanent nivelul de risc aferent autentificării utilizatorilor, pe baza cel puţin a următorilor parametri:

- Locaţia geografică din care se solicită accesul comparativ cu locaţia sediului utilizatorului
- Echipamentul utilizat pentru autentificare
- Comportamentul al utilizatorului

Soluţia trebuie să suporte metode out-of-band, cum ar fi notificările push şi parolele unice (OTP) livrate prin e-mail, text sau voce pentru autentificarea step-up.
Soluţia trebuie să ofere seturi de reguli implicite, care acoperă modele tipice de atacuri şi impersonări, uşor de utilizat şi personalizate.
Soluţia de autentificare securizată trebuie să detecteze automat situaţiile în care există un risc de autentificare şi în aceste situaţii să solicite o autentificare suplimentară de tip: cod acces de unică folosinţă (One Time Password – OTP), întrebare de securitate sau similar.
Soluţia de autentificare trebuie să realizeze analiza de risc la fiecare tentativă de acces la aplicatie sau de efectuare a unei operatiuni sensibile.

Pe baza analizei de risc, soluţia de autentificare va putea iniţia urmatoarele acţiuni:

- Permite accesului utilizatorului la sistemul informatic sau la funcţionalităţile sensibile
- Solicită utilizatorului un element de securitate suplimentar: cod acces de unică folosinţă (One Time Password – OTP) sau întrebare de securitate
- Iniţiază unui flux de analiză manuală, de către operatori umani, a tentativei de acces a utilizatorului – în urma analizei operatorul va putea acorda sau refuza accesul la sistem
- Refuză accesului utilizatorului la sistem

Soluția de autentificare trebuie să asigure următoarele funcționalități specifice analizei de risc:

- Analiza de risc este efectuată în timp real, la realizarea unei operațiuni de autentificare sau de acces la funcționalități sensibile
- Regulile și parametrii de calcul pot fi create / personalizate de către Beneficiar
- Pentru funcționalități diferite pot fi utilizate reguli și politici diferite
- Analiza de risc poate rula în background (pentru o perioadă de prestablită), fără ca rezultatele să fie aplicate operațiunilor utilizatorilor. Datele și rezultatele analizei sunt salvate în baza de date.
- Soluția trebuie să permită configurarea de excepții pe baza cărora regulile specifice analizei de risc să nu fie aplicate pentru anumiți utilizatori sau pentru anumite categorii de utilizatori

Soluția trebuie să includă cel puțin posibilitatea configurării următoarelor reguli / parametri pentru efectuarea analizelor de risc:

- Adresa IP a utilizatorului
- Țări cu nivel de risc crescut
- Zone hopping
- Utilizator necunoscut
- Verificare a ID-ului dispozitivului utilizat pentru autentificare
- Verificare Machine Fingerprint
- Verificare comportament utilizator

Soluția de autentificare securizată nu trebuie să implice transmiterea parolei utilizatorului prin canalale de comunicație.
Pentru generarea parolei de unică folosință, soluția de autentificare trebuie să includă o aplicație specifică, disponibilă atât pentru stațiile de lucru ale utilizatorilor cât și pentru download gratuit din Apple Store si Android Marketplace. Versiunea mobilă a aplicației pentru generarea parolei de unică folosință va fi disponibilă cel putin pentru sistemele de operare: iOS, Android,. Aplicația instalată pe dispozitivele mobile trebuie să poată genera parole de acess valabile chiar și în cazul lipsei conexiunii la o rețea de comunicație.
De asemenea, soluția trebuie să permită și utilizarea unei opțiuni prin care codul de acces de unică folosință este generat de către o componentă a soluției și după aceea este transmis către utiizator prin SMS sau e-mail.
Soluția trebuie să includă opțiunea de configurare a valabilității aplicației fixe/mobile pentru generarea codurilor de unică folosință precum și opțiunea de excludere din cadrul sistemului a unei aplicații a cărei valabilitate nu a expirat dar care rulează pe un echipament ce nu este de încredere.

3.8.6.6. Componenta de monitorizare a logurilor si a traficului de retea

Componenta de monitorizare a logurilor si traficului de retea va permite monitorizarea log-urilor de la componentele sistemului precum si a fluxurilor de comunicații prin preluarea traficului de la dispozitive de tip TAP. Acest modul va permite procesarea logurilor si a traficului de retea în timp real, prin probe dedicate, pentru extragerea, analiza și detectarea eventualelor evenimente de securitate care pot afecta functionarea PSCID - detecția rapidă a incidentelor de securitate, a utilizării incorecte a resurselor de rețea sau a performanțelor neoptimale.

Cerinte generale

- Solutia trebuie sa ofere capabilități de monitorizare real-time a device-urilor de securitate, switch-uri si routere de retea, Windows si Unix/Linux, servere de aplicatii, servere de baze de date si solutii de stocare
- Solutia propusa va include si un echipament de tip TAP
- Solutia trebuie sa identifice atacuri in timpul colectarii datelor
- Solutia trebuie sa ofere posibilitatea colectarii de log-uri, iar arhitectura de stocare sa suporte stocarea datelor atat online cat si arhivat pentru investigatii
- Solutia trebuie sa ofere posibilitatea colectarii de evenimente din segmente de retea separate la nivel de firewall
- Solutia trebuie sa ofere monitorizarea traficului de rețea prin captura acestuia in mod continuu si prin monitorizarea unor metadate de tip flow
- Solutia trebuie sa ofere prin intermediul unei console centrale vizibilitate unificată asupra întregii infrastructuri de comunicații prin agregarea datelor primite pe baza traficului de retea si loguri de la diferite siteme, precum și detecția rapidă a incidentelor de securitate si a utilizării incorecte a resurselor de rețea
- Solutia trebuie sa permita crearea incidentelor de securitate atat manual cat si automat
- Solutia trebuie sa ofere o interfata de vizualizare a alertelor si incidentelor de securitate
- Solutia trebuie sa ofere posibilitatea criptarii transmisiei datelor
- Solutia trebuie sa garanteze integritatea informatiilor colectate
- Solutia trebuie sa fie scalabila si sa acopere o gama larga de implementari, de la medii mici pana la medii distribuite.
- Pentru a nu creste incarcarea serverelor fizice actuale si a serverelor de virtualizare, solutia ce va fi ofertata in format de unul sau mai multe hardware appliance.
- Solutia trebuie sa aiba optiunea de a adauga componente fără a fi nevoie de inlocuirea hardware-ului existent, a software-ului sau a licentelor
- Solutia trebuie sa suporte cel putin 20000 EPS sustinute sau 50GB date procesate pe zi
- Solutia trebuie sa ofere posibilitatea de a rula query-uri in timp real pentru detectia anomaliilor
- Solutia trebuie sa ofere posibilitatea raportarii si investigarii pe datele stocate
- Solutia trebuie sa ofere posibilitatea instalarii componentelor si in mediu virtual
- Solutia trebuie sa ofere licentele necesare atât pentru sistemele de operare, cat si pentru aplicatii terte

Cerinte minime

- Solutia trebuie sa colecteze datele in format brut cu performante ridicate de analiza in timp real
- Interfata web a solutiei trebuie sa suporte cel putin urmatoarele optiuni de investigare detaliata: drill down, interogare pe o informatie specifica, filtre si cautari
- Solutia trebuie sa ofere posibilitatea de a salva profile pentru vizualizarea log-urilo si pentru scopuri de investigatii
- Solutia trebuie sa ofere cel putin urmatoarele intervale de timp pentru investigatii: ultima, ora, ultimele 24 ore, ultimele 2 zile, ultimele 5 zile, toata ziua, toate datele si interval de timp personalizate
- Solutia trebuie sa ofere capabilități de corelare de baza in timp real
- Solutia trebuie sa ofere capabilități de investigare detaliata direct din pagina de sumarizare a evenimentelor
- Solutia trebuie sa ofere posibilitatea crearii si administrarii regulilor de corelare direct in dinterfata web, fără a fi nevoie de unelte terte aditionale

- Solutia trebuie sa ofere capabilități de alertare pentru regulile de corelare folosind cel putin: SMTP, SNMP si Syslog
- Solutia trebuie sa ofere posibilitatea rularii de scripturi in momentul identificarii unei alerte
- Solutia trebuie sa ofere posibilitatea de a modifica criticalitatea alertelor generate
- Solutia trebuie sa ofere o interfață pentru constructia de reguli pentru rapoarte, diagrame, alerte, corelari, suficient de flexibila si fără a fi nevoie de limbaje de script-ing complexe
- Solutia trebuie sa ofere suport pentru descarcarea si instalarea actualizarilor aplicatiei/aplicatiilor direct din consola web sau din linia de comanda
- Solutia trebuie sa ofere funcții de auto monitorizare pentru verificarea starii tuturor componentelor folosind interfață web, incluzand cel putin urmatorii parametrii: CPU, memoria sistemului, memoria proceselor, stare si rata de capturare
- Solutia trebuie sa permită crearea de tablouri de bord personalizate
- Solutia trebuie sa ofere posibilitatea investigarii detaliate (drill-down) direct din tablourile de bord
- Solutia trebuie sa ofere acces pe baza de roluri
- Solutia trebuie sa permita autentificare prin Active Directory sau Pluggabe Authentication Modules (PAM)
- Solutia trebuie sa ofere interfață web cu suport HTML5
- Solutia trebuie sa ofere posibilitatea de a crea parsere personalizate pentru sursele de evenimente sau aplicatii ce nu sunt suportate de aplicatie
- Solutia trebuie sa ofere posibilitatea monitorizarii surselor de evenimente pentru cazul in care sursa nu mai trimite evenimente sau se inchide
- Solutia trebuie sa ofere posibilitatea colectarii log-urilor fără agent, agentul fiind folosit numai in cazurile in care colectarea fără agent nu este posibila pentru sursa de evenimente
- Solutia trebuie sa ofere posibilitatea secretizare a informatiilor din evenimentele colectate
- Solutia trebuie sa ofere functionalitati de auditare ale sistemului
- Solutia trebuie sa ofere posibilitatea alertarii utilizatorilor in cazul identificarii unui incident de securitate
- Solutia trebuie sa ofere conectivitate externa cu serviciile de cloud ale furnizorilor pentru descarcarea informatiilor aditionale: APT, definitii Botnet, retele malitioase, zero-day/compromitere, rapoarte suplimentare, parsere noi, reguli pentru rapoarte si diagrame
- Solutia trebuie sa permită detectarea atacurilor din interior prin stabilirea unui tip al comportamentului în rețea și compararea în permanență a traficului observat în timp real cu tiparele observate în trecut
- Solutia trebuie sa permită introducerea în analiză a informațiilor ce provin de la alte tipuri de tehnologii cum ar fi web-proxy, IDS/IPS, firewall sau NAC
- Solutia trebuie sa includa informații GeoIP in scopuri de investigatii
- Solutia trebuie sa ofere functionalitati de raportare. Rapoartele trebuie sa includa cel putin accesul bazat pe roluri: read&write, read only, no access
- Solutia trebuie sa suporte expresii regulate (RegEx) pentru crearea rapoartelor
- Solutia trebuie sa ofere cel putin urmatoarele optiuni la afisarea rapartelor: tabular, area, bar, bubble, column, line, pie, step line, step area, spline area, spline
- Solutia trebuie sa ofere optiunea de a programa rularea rapoartelor: ad-hoc, ora de ora, zilnic, saptamanal, lunar
- Solutia trebuie sa permită export-ul rapoartelor in cel putin urmatoarele formate: PDF si CSV

- Solutia trebuie sa ofere rapoarte, reguli si diagrame predefinite. Personalizarea rapoartelor, regulilor si diagramelor trebuie sa fie posibila
- Solutia trebuie sa ofere posibilitatea de a configura Identity Feed pentru a adauga domenii Active Directory, statii si utilizatori pentru log-uri si sesiuni non-Windows
- Solutia trebuie sa ofere posibilitatea de a configura liste pentru obtinerea de informatii contextuale despre statii, utilizatori sau adrese IP
- Solutia trebuie sa ofere posibilitatea de a exporta din interfața web log-urile sau pachetele de trafic colectate
- Solutia trebuie sa fie capabila sa automatizeze si sa orchestreze raspunsul si mitigarea pentru incidentele de securitate
- Solutia trebuie sa dispuna de mecanisme complet automate de prelucrare a incidentelor de securitate, mecanisme capabile sa fie declansate automat sau manual la interventia utilizatorului
- Solutia trebuie sa fie capabila sa identifice utilizarea incorecta a conturile cu privilegii de administrare
- Solutia trebuie sa fie capabila sa identifice schimbarea credentialelor de acces si a privilegiilor de acces
- Solutia trebuie sa fie capabila sa identifice login-urile administrative neuzule in functie de locatie, timp sau durata, pe baza utilizarii unor algoritmi de analiza comportamentala a utilizatorilor
- Solutia trebuie sa fie capabila sa identifice accesul utilizatorilor de administrare cu credentialele compromise
- Solutia trebuie sa fie capbila sa identifice sis a clasifice incidentele de securitate inclusive faza atacului si riscul acestuia
- Solutia trebuie sa fie capabila sa identifice traficul generat de Botnet, DDoS, scanari de vulnerabilitate, bitcoin, tunelare http/dns, command and control, exfiltrare, remote administration tools
- Solutia trebuie sa fie capabila de identificarea atacurilor pe baza de IOC introduse in sistem folosind STIX
- Solutia trebuie sa fie capabila de identificarea atacurile de tip "Remote Execution of Procedure Call"
- Solutia trebuie sa fie capabila de identificarea atacurilor care sunt parte din aceeasi campanie cu vizualizare detaliata asupra hosturilor si a atacurilor implicate in campanie
- Solutia trebuie sa fie capabila de detectie a atacurilor necunoscute pentru care nu exista semnaturi specifice
- Solutia trebuie sa fie capabila sa detecteze anomaliile si deviatiile de la modelul de baza detectat in infrastructura
- Solutia trebuie sa fie capabila de gestionare a informatiilor de trafic atat din mediul virtual cat si din mediul fizic
- Solutia trebuie sa dispuna de un API capabil sa fie folosit in automatizarea incidentelor de securitate
- Solutia trebuie sa dispuna de un tool de management a cazurilor pentru incidentele de securitate procesate cu posibilitatea de adaugare de note si fisiere de catre utilizatori
- Solutia trebuie sa fie capabila sa foloseasca feed-uri de securitate comerciale si open source configurabile de catre utilizator

3.8.6.7. Componenta de securizare a accesului la bazele de date

Pentru a creste nivelul de securizare si a scadea costurile operatiunilor administrative legate de controlul accesului la bazele de date, se consideră necesară utilizarea unei solutii software pentru bazele de date ofertate, care să satisfaca cel putin urmatoarele cerinte functionale si tehnice:

- Implementeaza posibilitatea autentificarii bazată pe 2 factori a administratorilor de baze de date, cu personalizarea metodei de autentificare pe baza de tipul utilizatorului care se autentifică sau a bazei de date la care se realizeaza autentificarea.
- Definirea de politici de acces individualizate pentru bazele de date, in functie de rolul acestora.
- Identificarea datelor cu caracter personal din bazele de date cu generarea unui raport care sa prezinte informatiile identificate.
- Stabilirea de politici de securitate complexe pentru accesul si modificarea datelor din bazele de date, cum sunt :
  - Modificarea datelor sa poata fi realizata doar prin intermediul aplicatiilor specifice, utilizatorii – inclusiv cu drept de administrator, sa nu poata modifica datele din baza de date
  - Utilizatorii – inclusiv cu drepturi de administrator de baza de date sau administrator al sistemului de operare pe care ruleaza baza de date sa nu aiba dreptul de a opri/reporni baza de date sau masina pe care ruleaza baza de date. In caz de necesitate, aceste operatiuni sa poata fi realizate cu aprobarea unui supervizor
  - Copierea bazelor de date sa fie permisa doar pentru aplicatiile specifice de back-up. Utilizatorii – inclusiv cei cu drepturi de administrator de baza de date sau administrator al sistemului de operare pe care ruleaza baza de date sa nu aiba dreptul de a copia sau sterge baza de date
- Definirea de politici de acces pentru implementarea unei functionalitati de tip firewall in functie de porturi, adresa sursa, tipul conectarii precum si momentul conectarii la baza de date
- Definirea de roluri, astfel încât pe baza grupurilor din care face parte un utilizator, sa i se permită accesul la diferite functionalitati.
- Definirea si administrarea politicilor de securitate a bazelor de date sa fie realizata centralizat, indiferent de tipul bazei de date (ex : Oracle, Microsoft SQL Server etc.) sau de sistemul de operare pe care ruleaza baza de date (Windows, Linux, Unix etc).
- Pentru bazele de date cu nivel inalt de confidentialitate, solutia trebuie sa ofere posibilitatea definirii unui proces de aprobare, astfel incat inaintea acordarii accesului la baza de date, utilizatorul sa solicite aprobarea unei alte persoane. Accesul se va permite numai dupa obtinerea aprobarii de acces.
- Accesul administratorilor la bazele de date se va realiza doar pe baza unei analize de risc, analize ce va include cel putin analize privind locatia utilizatorului, momentul initierii cererii de acces si istoricul respectivului utilizator.

3.8.6.8. Platforma de securizare a mașinilor virtuale

Solutia ofertata trebuie sa include o platforma de securizare a masinilor virtuale, platforma ce se va integra cu solutia de virtualizare oferita pentru a asigura functionarea in conditii de siguranta a acesteia.

Platforma de securizare a masinilor virtuale trebuie sa asigure urmatoarele functionalitati minime:

- Asigura un sistem de autentificare bazat pe 2 factori pentru accesul privilegiat atat la solutia de virtualizare oferita cat si la masinile virtuale configurate in cadrul platformei de virtualizare. Sistemul de autentificare trebuie sa asigure personalizarea metodei de autentificare in functie de tipul utilizatorului care se autentifică sau de tipul masinii la care se realizeaza autentificarea.
- Monitorizeaza permanent procesele vitale care ruleaza pe platforma de virtualizare – in cazul functionarii defectuoase a unui astfel de proces, solutia trebuie sa asigure repornirea automata a procesului cu notificarea operatiunii catre un grup de utilizatori predefiniti.
- Monitorizeaza permanent accesul la platforma de virtualizare si la masinile virtuale configurate in cadrul platformei precum si operatiunile efectuate asupra acestora. Oprirea sau repornirea unei masini virtuale nu va fi permisa indiferent de nivelul de acces al utilizatorului – inclusiv pentru utilizatori de tipul root sau Windows Admin. In cazul speciale, operatiunile de oprire/repornire a unei masini virtuale sunt permise cu aprobarea unui supervizor.
- Monitorizeaza permanent resursele platformei de virtualizare:
  - solutia va permite configurarea drepturilor de acces la nivel de director/fisier – inclusiv pentru utilizatori de tipul root sau Windows Admin.
  - pentru fiecare masina virtuala din cadrul platformei, solutia va permite configurarea aplicatiilor care au dreptul de a rula pe masina respectiva
  - pentru fiecare masina virtuala din cadrul platformei, solutia va permite configurarea nivelului maxim de incarcare a resurselor de procesare (CPU, RAM). La atingerea acestui nivel, solutia va permite alocarea de resurse suplimentare pentru rularea in conditii de performanta a aplicatiilor specifice
  - pentru fiecare masina virtuala din cadrul platformei, solutia va asigura inregistrarea operatiunilor executate de utilizatorii cu drepturi de administrare (de tip root / Windows Admin etc) pentru a garanta securitatea sistemelor si pentru audit
  - pentru fiecare masina virtuala din cadrul platformei, solutia va permite stabilirea unei liste de comenzi interzise (de tip blacklist) care nu vor putea fi rulate pe masina respectiva nici de utilizatorii cu drepturi de administrare (de tip root / Windows Admin etc)
- Definirea de politici de acces pentru implementarea unei functionalitati de tip firewall in functie de porturi, adresa sursa, tipul conectarii precum si momentul conectarii la platforma de virtualizare
- Accesul administratorilor la platforma de virtualizare se va realiza doar pe baza unei analize de risc, analize ce va include cel putin analize privind locatia utilizatorului, momentul initierii cererii de acces si comportamentul anterior al respectivului utilizator.

3.8.7. Monitorizare date, sisteme si aplicatii

Având în vedere complexitatea tehnică și funcțională a PSCID, precum și importanța acestuia, devine esențială necesitatea implementării unei soluții de management de aplicații și infrastructură care să elimine discontinuitatea serviciilor oferite de IT către zona functionala, unificând în acest fel cele două componente. Sistemul de monitorizare trebuie să fie instalat și implementat în nodul central. Pentru înaltă disponibilitate, soluția trebuie să poată fi instalată și în centrul Disaster Recovery fără costuri suplimentare (licențe software) pentru Beneficiar.

Monitorizare infrastructura de aplicații

Se solicită implementarea unei solutii de tip „COTS" care să îndeplinească urmatoarele cerinte tehnice si functionale:

- Soluţia trebuie să ofere o imagine globală a întregului sistem pentru a detecta proactiv, diagnostica şi rezolva orice problemă de performanţă şi disponibilitate în ordinea priorităţii dictate de business.
- Soluţia trebuie să ajute managerii IT şi de aplicaţie să înţeleagă nivelurile acceptate ale serviciilor livrate către utilizatorii finali, pentru a asigura continuitatea sistemului în condiţii optime.
- Sistemul trebuie să fie instalat şi implementat în nodul central. Soluţia ofertată va oferi o interfaţă grafică cu posibilitatea de a monitoriza disponibilitatea şi performanţa componentelor (timp mediu de răspuns între două componente, instantaneu şi istorie lunară, reprezentări grafice de instantanee, istoria de perturbări, processor, memorie şi degradare de performanţă).
- Sistemul va genera alerte clasificate în funcţie de gravitatea evenimentelor, cu privire la interfeţele, la aplicaţiile monitorizate; alertele se vor trimite destinatarilor desemnaţi prin email-uri de avertizare pentru evenimente critice.

Soluţia pentru Sistemul de monitorizarea a performanţelor aplicaţiilor trebuie să fie una consacrată în piaţă care să poate oferi o perspectivă asupra aplicaţiilor web din toate punctele de vedere (sistem, reţea, aplicaţie şi experienţa utilizator).
Solutia va trebui sa monitorizeze minim tranzactiile pentru aplicatiile web – Java, .Net si medii SOA – pentru toti utilizatorii in regim de 24 ore/zi si 7 zile/saptamina si sa detecteze eventualele probleme inainte ca acestea sa afecteze utilizatorul final;
Sistemul de monitorizarea a performanţelor aplicaţiilor va fi utilizat pentru a asigura o strategie de monitorizare în timp real a perfomanţelor aplicaţiilor web utilizate (portal, website, acces web, etc.) ce va permite:

- monitorizarea experienţei utlizatorului final prin urmărirea tranzactiilor de tip „end-to-end business" pentru a se asigura ca utilizatorul final foloseste cu succes aplicatiile in parametrii proiectati si urmariti de departamentul de IT (încărcarea datelor, răspunsul la cererile lansate din aplicaţie, modul de rulare a scripturilor la nivel client web, etc.);
- identificarea si prioritizarea problemelor care ar afecta calitatea serviciilor catre utilizatorul final prin analizarea in timp real a tranzactiilor individuale pentru fiecare utilizator;
- furnizarea şi gestionarea informaţiilor referitoare la calitatea serviciilor oferite utilizatorilor - măsurarea serviciilor de tip Service Level Agreements (SLA);
- asigurarea unei vizibilităţi a tranzacţiilor de grad înalt;
- determinarea rapidă a sursei problemelor de performanţă;
- trierea şi identificarea elementelor de infrastructură, precum şi analiza cauzelor principale;
- prioritizarea şi trierea incidentelor care se bazează cu adevărat pe impactul asupra activităţii;
- corelarea experientei utilizatorilor cu performanta aplicatiilor si cu impactul asupra regulilor de business (obtinute in urma monitorizarii) in vederea oferirii de solutii pentru imbunatatirea aplicatiilor si a comunicatiilor;
- asigurarea monitorizării aplicaţiilor în mod proactiv şi predictiv;
- creşterea frecvenţei de raportare şi asigurarea unei continue îmbunătăţiri a performanţelor;
- asigură monitorizarea istorică, dar şi în timp real a performanţelor aplicaţiilor şi experienţei utilizatorilor;
- analizarea traficului SSL, precum şi importarea şi gestionarea cheilor private pentru accesul la aplicaţiile sigure prin SSL;

- monitorizarea aplicațiilor din perspectiva sistemelor pe care rulează și a rețelei;
- stabilirea de profile de comportament normal pe baza datelor adunate în timp și evidențierea abaterilor de la aceste praguri;
- Sistemul trebuie să asigure monitorizarea și analizarea performanțelor în amănunt, de tip deep-dive până la nivel de cod;
- Soluția trebuie să poata monitoriza aplicatii Java, .Net, servere de aplicatii, servere Web, servere de baze de date si platforma de virtualizare oferite;
- Soluția trebuie să poata identifica proactiv orice micșorare a performantelor aplicatiilor web și să propuna solutii de rezolvare mapate pe infrastructura;
- Soluția trebuie să functioneze în medii complexe SOA sau virtualizate;
- Soluția trebuie să ofere o imagine globală a întregului sistem pentru a detecta proactiv, diagnostica și rezolva orice problemă de performanță și disponibilitate în ordinea priorității dictate de business;
- Soluția trebuie să ajute managerii de aplicație să înțeleagă nivelurile acceptate ale serviciilor livrate către utilizatorii finali, pentru a asigura continuitatea sistemului în condiții optime;
- Se va oferi un sistem centralizat pentru monitorizarea și gestionarea tuturor componentelor din cadrul proiectului;
- Sistemul centralizat trebuie să fie instalat și implementat în nodul central. Soluția ofertată va oferi o interfață grafică cu posibilitatea de a monitoriza disponibilitatea și performanța componentelor (timp mediu de răspuns între două componente, instantaneu și istorie lunară, reprezentări grafice de instantanee, istoria de perturbări, processor, memorie și degradare de performanță);
- Sistemul va genera alerte clasificate în funcție de gravitatea evenimentelor, cu privire la interfețele, la aplicațiile monitorizate; alertele se vor trimite destinatarilor desemnați prin email-uri de avertizare pentru evenimente critice;
- Sistemul va permite monitorizarea in aceeasi interfata, alaturi de celelalte componente hardware si software, a componentei de portal si a platformei de aplicatii. Sistemul va permite realizarea de corelari intre performantele serviciilor oferite de componenta portal si performanta platformei de aplicatii prin utilizarea de tablouri de bord predefinite;
- Sistemul va permite realizarea de operatiuni de tip drill-down in vederea determinării componentelor care generează blocaje/probleme de performanta;
- Solutia trebuie sa permita stabilirea unor praguri minime de performanta pentru anumite metrici cheie si sa genereze alerte in cazul in incalcarii acestor praguri.

Funcționalitățile cheie ale Solutiei de monitorizarea a performanțelor aplicațiilor:

- Managementul tranzacțiilor;
- Managementul centrat pe activitate;
- Realizarea hărților vizuale pentru trierea aplicațiilor ce arată în mod dinamic componentele implicate în tranzacții;
- Identificarea automată a tranzacțiilor;
- Starea de funcționare a paginilor web si timpul de raspuns;
- Monitorizarea tranzacțiilor pe toată durata de viață a acestora
- Monitorizarea performanței aplicațiilor trebuie să se faca indiferent de modul de acces: brower web, browser mobile, aplicație mobile.
- Soluția trebuie să permită deschiderea automata de tickete de suport în aplicația de suport, atunci când o problemă de performanță este detectată.

- Soluția trebuie să rețină datele în mod istoric și să reevalueze pragurile de performanță ale aplicației, astfel încât se va considera funcționare ok dacă parametrii de perfromanță sunt neschimbate după o perioadă de cel puțin 7 zile.

Monitorizarea infrastructurii server

Soluția de monitorizare a sistemelor trebuie să ofere următoarele funcționalități:

- Capabilitatea de a monitoriza sisteme Windows, UNIX și Linux, Solaris, HP-UX.
- Capabilitatea de administrare a tuturor resurselor de la o singură consolă.
- Accesul la consola de administrare trebuie să se realizeze prin browser web și GUI.
- Soluția trebuie să permită autentificarea folosind integrare cu LDAP.
- Monitorizarea următorilor parametri:
    - Procesor: utilizarea fiecărui procesor din sistem și compararea gradului de utilizare curentă cu praguri critice predefinite si configurabile
    - Sistem de fișiere: spațiul ocupat din sistemul de fișiere și comparația acestuia cu praguri critice predefinite și configurabile.
    - Memorie și I/O - utilizare
    - Starea serviciilor sistemului
        - procese/servicii care ruleaza și resurse consumate de fiecare proces/serviciu
        - procese/servicii care ar trebui să ruleze și sunt oprite
    - Performanțele serverelor de baze de date și ale serverelor de aplicații.
- Emiterea de alarme - soluția trebuie să poată emite alerte prin mai multe mijloace: e-mail, mesaje în consolă, mesaje administrative
- Acțiuni corective: soluția trebuie să se poată configura astfel încât să execute acțiuni corective automate (fără intervenția administratorilor) în cazul detectării de erori sau în cazul degradării performanțelor.
- Agenții pentru fiecare sistem nu trebuie să interfereze cu operațiile normale ale sistemului pentru a nu afecta performanțele acestuia.
- Instalare/configurare agenți dintr-o singură locație pentru toate sistemele și componentele monitorizate.
- Extensibilitate facilă pentru includerea scripturilor customizate de monitorizare a aplicațiilor dezvoltate în interiorul organizației.
- Construirea profilurilor sau template-urilor de monitorizare, simultan pentru sisteme similare.
- Modificarea modelelor de resurse prin schimbarea, de exemplu, a nivelurilor pragurilor.
- Posibilitatea modificării intervalelor de monitorizare.
- Capabilitatea de a vizualiza atât date în timp real cât și din trecut pentru orice sistem dintr-o consolă web, centralizată, pentru monitorizare.
- Capabilitatea de a trimite rezultatele de la colectarea datelor și analiză la aplicația de corelare a evenimentelor.
- În cazul în care unul din serverele de monitorizare nu își poate îndeplini funcțiunile, agentul, fără intervenția administratorilor, trebuie să poată transmite informațiile către alt server de monitorizare.
- Sistemul trebuie să ofere posibilitatea criptării comunicației care se realizează între componentele sistemului.
- Soluția trebuie să fie scalabilă și să utilizeze mecanisme de alertă pentru a monitoriza performanța, capacitatea și disponibilitatea serverelor (virtuale și fizice), a dispozitivelor de

rețea, a echipamentelor de electroalimentare - UPS-uri și grupuri electrogeneratoare cu SNMP precum și a aplicațiilor (de ex. MSExchange, Sharepoint, VMWare).

- Soluția ar trebui să aibă suport pentru arhitectură distribuită pe mai multe niveluri, oferind un nivel ridicat de scalabilitate.
- Soluția trebuie să furnizeze un mecanism de descoperire automată a infrastructurii utilizând protocoalele SNMP (v1, v2 și v3), WMI și SSH.
- Soluția trebui să dispună de interfață de utilizator Web intuitivă și fiabilă. Măsurile de securitate (acces bazat pe roluri) trebuie furnizate pentru a permite diferite niveluri de acces precum și de control atât pentru utilizatori, cât și pentru grupuri de utilizatori.
- Soluția trebuie să ofere posibilitatea de a personaliza modalitatea de prezentare vizuală și de a crea grupuri de dispozitive de infrastructură (dinamice și statice) bazate pe filtre predefinite.
- Soluția trebuie să furnizeze metodă de import/export a informațiilor despre elementele monitorizate într-bază de date externă sau într-un alt format.
- Soluția trebuie să susțină intervale de interogare și praguri de notificare configurabile (cel puțin 1 minut rata de interogare) atât la nivel de dispozitiv cât și / sau grup de dispozitive.
- Soluția trebuie să ofere suport pentru următoarele protocoale pentru import / interogare SNMP (v1, v2c, v3), WMI, SSH, Telnet, CSV.
- Soluția trebuie să ofere suport pentru Multi-Tenancy – trebuie să se poată crea vizualizări pentru segmente de public distincte, cu posibilitatea de a accesa numai părți ale unui serviciu/sistem, pe baza contului/grupului de utilizator.
- Soluția trebuie să ofere tablouri de bord care conțin date care sunt relevante numai pentru anumită persoană/grup/rol.
- Soluția trebuie să ofere posibilitatea monitorizării infrastructurii folosind atât agenți instalați cât și fără instalarea de agenți pe elementele monitorizate.
- Soluția trebuie să permită utilizatorilor să monitorizeze apariția unui anumit text în fișiere de jurnal pentru pentru a declanșa evenimente. Monitorizarea directoarelor pentru creșterea dimensiunii fișierelor, timpul de existență a fișierelor, modificările fișierelor și alte opțiuni importante trebuie de asemenea furnizate.
- Sistemul trebuie să furnizeze API-uri deschise care să permită integrarea ușoară cu alte sisteme informatice.
- Sistemul trebuie să ofere integrare cu LDAP.
- Soluția trebuie să furnizeze mecanisme interne pentru disponibilitate înaltă (HighAvailability).
- Soluția trebuie să ofere suprimarea alertelor în timpul perioadelor de nefuncționare programate cunoscute (mentenanță / upgrade etc).
- Soluția va oferi acces și raportarea pentru evenimentele istorice.
- Soluția trebuie să integreze evenimente, erori și alerte într-un singur ecran. Evenimentele trebuie să fie corelate și de-duplicate pentru a preveni evenimente de tip furtună, iar soluția trebuie să dispună de capabilități ce permit executarea de activități corective automate pentru remedierea alertelor.
- Soluția trebuie să permită crearea de reguli de corelare a evenimentelor.
- Soluția trebuie să ofere utilizatorului posibilitatea de a crea scheme de agregare și politici de retenție a datelor colectate.
- Soluția trebuie să fie capabilă să execute diverse scripturi în cazul apariției unei alarme.
- Soluția trebuie să ofere de posibilitatea de a defini diferite evenimente la diferite niveluri sau de urgență (de exemplu, critică, gravă, avertizare etc.).

- Soluția trebuie să permită politici de notificare configurabile, prin care să pot fi definiți destinatarii alertelor în funcție de ora din zi, gazdă, eveniment, severitate etc.
- Soluția trebuie să poată trimite notificări prin e-mail despre alarme către utilizatori sau grupuri de utilizatori.
- Soluția trebuie să furnizeze SDK-uri pentru crearea de agenți personalizați, cum ar fi de ex. Perl, Java, C, Visual Basic.
- Soluția trebuie să furnizeze tablouri de bord Out-of-the-box, precum și tablouri de bord personalizate pentru afișarea corelată a datelor care acoperă infrastructura monitorizată.
- Sistemul trebuie să fie capabil să mențină/stocheze date istorice pentru a oferi evaluări de performanță și capacitate, precum și analiză predictivă pentru a preveni întreruperile.
- Soluția trebuie să suporte raportarea istorică a performanțelor pentru elementele monitorizate.
- Capacitățile de raportare ar trebui să includă flexibilitatea pentru a permite crearea de rapoarte în diferite formate (csv, pdf, png, jpg, html, etc), capacitatea de a automatiza și programa livrarea de rapoarte.
- Soluția ar trebui să ofere posibilitatea de a măsura performanța "normală" și să determine valori normale de funcționare și modele bazate pe ora din zi, săptămână etc. Capacitatea de a genera alarme bazate pe valorile normale de funcționarea trebuie să fie disponibilă.
- Abilitatea de a crea pagini de rapoarte personalizate pentru anumiți utilizatori care prezintă date de raportare specifice pentru nevoile utilizatorilor.
- Abilitatea de a crea tranzacții sintetice pentru a monitoriza timpul de răspuns al utilizatorilor finali pentru web și aplicațiile clientului
- Soluția trebuie să furnizeze bază de date ce stochează datele pe termen lung pentru analiza tendințelor cât și pentru planificarea capacității sau rapoarte.
- Soluția trebuie să furnizeze un sistem statistic automat de analiză a datelor bazat pe deviația standard.
- Soluția trebuie să ofere un sistem de răspuns la încălcarea pragurilor de monitorizate configurate.
- Soluția trebuie să fie capabilă să identifice resursele Top N și Bottom N bazate pe orice metric de performanță monitorizat; trebuie să furnizeze rapoarte care să arate atât perioadele curente, cât și cele istorice.
- Soluția trebuie să fie capabilă să colecteze informații despre funcționarea echipamentelor de rețea. Vor trebui colectate, fără a se limita la, informații ca: utilizare procesor, utilizare memorie, utilizare interfețe, erori pe interfețe, politici de QoS, teste de performanță servicii.
- Soluția propusă trebuie să aibă opțiuni de a se integra cu soluția de Help Desk, pentru a crea solicitări de servicii (sau incidente), bazate pe evenimentele detectate.

3.8.8. Componenta de Backup

La nivelul sistemului se vor putea configura politici de backup, recuperare și restaurare pentru sistemele de operare, fișierele de configurare, aplicații și baze de date.
Indiferent de modelul sau mediul de stocare ale datelor, accesarea datelor salvate se va face în condiții de siguranță, cât mai facil și fără să implice costuri suplimentare.

Cerinte tehnice

- Solutia trebuie sa asigure protectia sistemelor de productie, a datelor si aplicatiilor ce vor rula pe aceste sisteme, sa monitorizeze aplicarea politicilor de protectie si recuperare a

datelor, sa utilizeze mecanisme de deduplicare si compresie si sa permita replicarea continua a masinilor virtuale.

- Licentierea solutiei trebuie sa fie calculata dupa numarul de procesoare fizice in utilizare pe sistemele de calcul ale infrastructurii de productie.
- Licentierea trebuie sa fie de tip perpetual, nu se accepta cea pe baza de abonament, tip subscription.
- Solutia trebuie sa asigure protectia sistemelor virtualizate si fizice, a sistemului de operare, a fisierelor si aplicatiilor ce ruleaza pe aceste sisteme prin politici de protectie unitare sau distincte.
- Administratorul trebuie sa utilizeze o singura interfata de administrare a politicilor de protectie si resturare a datelor pentru toate politicile de protectie indiferent de sistemele de protejat.
- Solutia trebuie sa permita configurarea politicilor de protectie in mod independent pentru protectia unui fisier, a sistemului de operare, a imaginii intregului sistem sau pentru o aplicatie specifica.
- Sursa datelor, sistemul sau aplicatia de protejat, trebuie sa comunice in mod direct si securizat cu sistemul dedicat pentru protectia datelor folosind mecanisme de autentificare.
- Solutia va permite protectia unui numar nelimitat de masini virtuale si de aplicatii ce ruleaza pe sistemele licentiate conform matricei de complianta a producatorului.
- Solutia trebuie sa poata sustine protectia statiilor de lucru tip MS Windows, Linux si MacOS, utilizand aceiasi consola de administrare pentru toate politicile de protectie si restaurare.
- Solutia sustine deduplicarea globala a datelor, la sursa sau destinatie, prin segmentare variabila pentru fiecarui proces de protectie indiferent de retea sau protocolul de transfer utilizat.
- Procesul de deduplicare trebuie sa se desfasoare fara stocare temporara si fara sisteme de calcul intermediare intre sursa si destinatie, utilizand un altgoritm global de deduplicare.
- Solutia va permite ca procesele de salvare sa transmita peste retea numai segmentele de date noi, sau cele modificate fata de procesul de salvare anterior, avand intotdeauna disponibil ultimul set de date, tip full backup, in echipamentul dedicat protectiei datelor fara a initia trafic aditional in retea.
- Solutia va include capabilitati de protectie la nivel de bloc de date pentru sisteme fizice si pentru masinile virtuale. Restaurarea acestor date fiind disponibila atat ca imagine completa cat si granular.
- Transferul datelor de la sursa la destinatie trebuie sa poata fi criptat, la fel si stocarea segmentelor de date deduplicate in echipamentul dedicat, indiferent de politicile de retentie aplicate.
- Solutia trebuie sa permita protectia mediilor virtuale la nivel de bloc de date fara agenti instalati in masinile virtuale cu posibilitatea de a transfera datele peste o retea IP sau Fibre Channel.
- Solutia trebuie sa protejeze sisteme de calcul de tipul Microsoft Windows, Linux CentOS, Debian, Fedora, Red Hat, SuSE, Oracle Linux, AIX, HP-UX si Solaris.
- Solutia trebuie sa utilizeze module dedicate pentru protectia aplicatiilor ca Microsoft Exchange, Microsoft SQL, Microsoft SharePoint, Oracle, SAP, DB2, Informix, MySQL, PostgreSQL si MongoDB.

- Solutia va permite protectia oricarui tip de baze de date, integrat politicilor de protectie pastrand eficienta procesului de deduplicare si a consistentei datelor prin politicile de protectie centralizate.
- Solutia va permite definirea si rularea unor rutine automate, inainte sau imediat dupa desfasurarea procesului de salvare a datelor, in functie de cerintele specifice ale aplicatiei de protejat.
- Solutia trebuie sa ofere posibilitatea de a rula rapoarte combinate cu informatii aferent desfasurarii proceselor de protectie de la toate componentele software si hardware ale solutiei.
- Solutia trebuie sa includa mecanisme automatizate de replicare a datelor salvate astfel incat catalogul actualizat sa utilizeze datele replicate la distanta in cazul in care va fi solicitat.
- Solutia va permite ca o singura operatiune de protectie sau restaurare sa fie impartita in fluxuri de date paralele pentru acelasi client sursa imbunatatind indicatorii de performanta ai procesului.
- Solutia trebuie sa permita restaurarea datelor inapoi la clientul sursa in format compresat.
- Solutia trebuie sa permita notificari tip SNMP traps v3.
- Solutia va include servicii de replicare a masinilor virtuale tip VMware, in mod sincron sau asincron, local sau la distanta, cu jurnalizarea informatiilor modificate pe o perioada de timp determinata.
- Acest jurnal se va putea pastra local sau in locatia secundara pentru o restaurare rapida a masinii virtuale din momentul anterior aparitiei erorii sau coruperii acesteia.
- Replicarea masinilor virtuale trebuie sa utilizeze capabilitati de deduplicare si compresie ce vor rula in mod continuu pentru a eficientiza transferul datelor de la un centru de date la altul.
- Licentierea solutiei trebuie sa includa un minim de 28 de procesoare fizice.

3.8.9. Soluție de disaster recovery

Soluția de disaster recovery propusă trebuie să asigure următoarele caracteristici:

- Să asigure funcționalități de disaster recovery prin automatizarea și orchestrarea restaurării sistemelor în site-ul de rezervă
- Să asigure funcționalități de disaster recovery prin închiderea site-ului principal și pornirea serviciilor în site-ul secundar în cazul unui pericol iminent identificat
- Să asigure funcționalități de migrare planificata a site-ului pentru a permite derularea diverselor activități în site-ul principal (mentenanță, relocare, etc.)
- Să permită rularea de scenarii de testare fără a influența funcționalitatea site-ului principal
- Să permită, în funcție de caracteristicile mediului de comunicație avut la dispoziție, utilizarea mecanismelor de replicare la nivel mașină virtuala și/sau storage
- Să fie compatibilă cu soluția de virtualizare ofertata și sistemul să includă licențele necesare pentru realizarea replicării la nivel mașină virtuala peste medii WAN
- Să fie compatibilă cu soluția de stocare ofertata și sistemul să includă licențele necesare pentru realizarea replicării la nivel storage
- Soluția trebuie să fie licențiată astfel încât să asigure protecția tuturor mașinilor virtuale din mediul de producție, dar nu mai puțin de 40 de mașini virtuale.
- Solutia trebuie sa permita restaurarea elementelor critice ale sistemului in maxim 3 ore de la aparitia evenimentului care a dus la indisponibilizarea sistemului. In cadrul propunerii tehnice,

ofertantii vor prezenta o propunere de plan de disaster recovery prin care vor trata modul in care vor face disponibile serviciile / functionalitatile sistemului in intervalul de 3 ore amintit. Planul final va fi agreat in cadrul etapei de analiza. In timpul implementarii, furnizorul va efectua impreuna cu Autoritatea Contractanta 2 simulari ale procesului de disaster recovery.

3.8.10. Componenta de preluare date din documentele de identitate, liveness test si face comparison

Componenta de preluare date din documentele de identitate

Acesta componenta este destinata preluarii datelor din documentele de identitate si va fi folosita pentru preluarea datelor special codificate. Aceste informații sunt găsite în partea de jos a documentelor de identitate care pot fi citite de mașină.
MRZ (machine readable zone) se compune din 1, 2 sau 3 rânduri de text, scrise cu font de tip OCR-B, care a fost creat pentru a facilita operațiile de recunoaștere optică a caracterelor.
Standardul pentru MRZ este detaliat în Doc ICAO 9303 și ISO / IEC 18013-1: 2018.

Componenta trebuie sa indeplineasca urmatoarele cerinte tehnice:
- Sa functioneze pe urmatoarele platforme: Android, IOS, Linux si Windows Server;
- Sa preia automat din documentele de identitate minim urmatoarele informatii: clasa documentului, numar/serie document, MRZ complet, data emiterii, data expirarii, tara emitenta, data nasterii, sex, nume, nationalitate;
- Sa returneze poza documentului validat si poza user-ului;
- Sa citeasca datele din cip-ul NFC din cadrul documentului (valabil doar pentru pasaport electronic).

Componenta de liveness test

Componenta de liveness test este destinata validarii ca persoana care doreste sa se inroleze in carul sistemului "este vie". Acesta componenta va mapa geometria de baza a fetei umane, creand o semnatura unica, pentru a distinge cu usurinta diferiti utilizatori. Preluarea imaginii fetei se va face prin intermediul unui flux video in diferite pozitii spatiale.

Componenta trebuie sa indeplineasca urmatoarele cerinte tehnice:
- Sa functioneze pe urmatoarele platforme: Android si IOS;
- Sa analizeze diferite posturi ale user-ului in cadrul unui video live si sa returneze veridicitatea persoanei.

Componenta de face comparison

Componenta de face comparison este destinata compararii pozelor preluate pentru un utilizator: cea din documentul de identitate cu cea preluata din fluxul video al testului liveness.

Componenta trebuie sa indeplineasca urmatoarele cerinte tehnice:
- Sa functioneze pe urmatoarele platforme: Linux si Windows Server;

- Sa returneze veridicitatea persoanei comparand cele 2 poze preluate prin cadrul **Componentei de preluare date din documentele de identitate** si **Componentei de liveness test**, conform datelor biometrice;
- Sa returneze un scor pentru copararea celor 2 poze.

3.8.11. Platforma de virtualizare

Platforma de procesare aplicații va integra o platforma de virtualizare a resurselor logice de procesare aplicații (procesoare, memorie, sub-sistem I/O), exclusiv prin hipervizor dedicat instalat in fiecare tip de nod.
In stransa legatura si prin integrarea cu celelalte elementele de infrastructura de procesare aplicații, platforma de virtualizare trebuie sa permita obtinerea urmatoarelor obiective functionale si operationale:

- Complexitate redusa a platformei, in scopul integrarii cu usurinta in mediul existent, atat din punct de vedere operational cat si functional;
- Platforma ce include mecanisme de redundanta locala si la distanta, integrate cu restul elementelor de infrastructura, pentru protectia continua si completa a aplicatiilor deservite si a datelor stocate in masini virtuale si platforme, in eventualitatea unor defectiuni majore;
- Platforma scalabila in mod transparent pentru aplicatiile deservite si datele stocate in masini virtuale, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate, conectivitate si performanta;
- Platforma bazata pe componente standard, in scopul integrarii facile cu setul de aplicatii si cerinte existente in infrastructura, precum si cu orice alte noi cerinte viitoare, fara costuri aditionale datorate investitiilor in alte platforme de unica functionalitate;
- Unelte de administrare integrate si facil de folosit, ce acopera intreaga functionalitate, independente de anumite elemente de infrastructura (sistem de operare, tehnologie de aplicatie, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;
- Functionalitati integrate de securitate si protectie criptografica a datelor stocate, integrate cu restul elementelor de infrastructura, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
- Mecanisme integrate de optimizare transparenta a aplicatiilor deservite si a datelor stocate in masini virtuale, in scopul folosirii eficiente a resurselor de procesare, comunicatie si a spatiului de stocare disponibil, asigurand in acelasi timp costuri operationale minime si posibilitatea de a preveni suplimentarea respectivelor platforme;
- Platforma integrata ce va permite reducere semnificativa a timpilor de nefunctionare a aplicatiilor si serviciilor, reducerea proceselor operationale, respectiv a timpilor de solutionare a incidentelor, distribuirea uniforma a capacitatilor de procesare si stocare cu imbunatatirea semnificativa a gradului de utilizare relativ la fiecare resursa fizica, diminuarea costurilor operationale;
- Mecanisme integrate de recuperare in caz de dezastru si continuitate operationala, in scopul reducerii complexitatii asociate scenariilor de protectie si redundanta multi-site, indiferent de aplicatiile si serviciile deservite de platforma de virtualizare;

Platforma de virtualizare dedicata, va fi bazata pe Hypervizor propriu, fara dependenta de un sistem de operare anume.Aceasta va fi instalata direct in platforma de procesare aplicații si va

beneficia de suportul acestei platforme atat la nivelul capacitatii de procesare cat si la nivelul optiunilor de conectica si integrare cu restul elementelor fizice de infrastructura.

In cadrul proiectului, ofertantii vor livra elementele de infrastructura folosind mecanismele de IaC (Infrastructure as Code) - resurse definite descriptiv, procese automatizate (folosind script-uri).

Platforma de virtualizare trebuie sa indeplineasca urmatoarele **cerinte functionale specifice:**

Caracteristica	**Cerinta tehnica minimala**
Descriere	Platforma consolidata de virtualizare;
Functionalitati	▪ Hypervizorul trebuie sa fie matur, testat si implementat in infrastructuri de productie complexe si sa ofere performanta maxima pentru aplicatiile si serviciile instalate in masini virtuale indiferent de complexitatea si natura acestora.Nivelul de abstractizare a componentelor fizice din platformele de procesare, stocare si comunicatie nu trebuie sa adauge complexitate si/sau penalizari de performanta sesizabile in functionarea aplicatiilor si serviciilor deservite; ▪ Platforma de virtualizare trebuie sa fie compatibila cu toti producatorii hardware recunoscuti: Dell, HPE, Lenovo, iar hypervizorul pe care aceasta plaforma se bazeaza trebuie sa fie independent de producatorul sau de metoda de stocare interna/externa disponibila in platforma de procesare si/sau stocare pe care ruleaza; ▪ Platforma de virtualizare trebuie sa ofere suport pentru urmatoarele sisteme de operare instalabile in masina virtuala: Windows, Linux Suse/Red Hat/CentOS, FreeBSD, Solaris si sa permita adaugarea de spatiu de stocare pentru masinile virtuale prin folosirea urmatoarelor protocoale: NAS – NFS/CIFS; SAN – iSCSI/FC/FCoE si prin folosirea urmatoarelor sisteme de fisiere: FAT32, NTFS, EXT2, EXT3, asigurand astfel compatibilitate cu majoritatea tehnologiilor implementate in mod uzual atat in platformele de procesare cat si in platformele de stocare; ▪ Platforma de virtualizare nu trebuie să depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea şi funcţionalitatea echipamentelor din platforma de procesare, respectiv a maşinilor virtuale care rulează pe aceste echipamente; ▪ Amprenta pe disc a hypervisor-ului trebuie sa aiba dimensiuni reduse astfel incât instalarea hypervisor-ului să poata fi realizata foarte rapid chiar şi prin intermediul retelei de comunicatie, oferind totodată posibilitatea de rulare integrala din mediu de tip USB; ▪ Platforma de virtualizare trebuie sa ofere suport pentru USB 3.0 şi rularea de aplicaţii grafice (DirectX sau OpenGL2) in masinile virtuale rezidente, respectiv suport pentru accelerarea video in hardware pentru respectivele masini virtuale (suport pentru tehnologia de accelerare video oferita de NVIDIA GRID sau echivalent); ▪ Platforma de virtualizare trebuie sa ofere suport pentru conectarea

Caracteristica	Cerinta tehnica minimala
	pe port serial in orice masina virtuala, prin folosirea unui concentrator serial de retea; ▪ Componentele virtuale ale platformei sa poata fi modificate cu usurinta permitand astfel crearea de configuratii diferite pentru seturi comune de masini virtuale, precum si crearea de configuratii unitare la nivelul intregii infrastructure virtuale, atat din prisma elementelor virtuale de procesare si stocare (integrate in platforma sau prin integrarea cu componente terte ale respectivelor platforme de proceare si stocare), cat si din prisma elementelor de comunicatie (posibilitatea integrarii directe cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea si asigurarea crearii unei retele virtuale unificate la nivelul intregii infrastructuri virtuale); ▪ Platforma de virtualizare trebuie sa ofere mecanisme integrate pentru adaugarea de resurse de procesare si memorie fara restartarea sistemului de operare din masina virtuala, (in masura in care sistemul de operare suporta aceste facilitati), mecanisme ce pot fi independente de platformele de procesare/stocare/comunicatie sau prin intermediul unor conectori/componente comune respectivelor platforme; ▪ Prin integrarea cu platformele de procesare aplicații, masinile virtuale definite in platforma de virtualizare trebuie sa beneficieze concomitent de suport de multiprocesare simetrica si acces la totalitatea porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile in infrastructura; ▪ Resursele virtuale (resurse de procesare, stocare si comunicatie) disponibile la nivelul intregii platforme de virtualizare (prin integrarea cu platformele fizice de procesare, stocare si comunicatie) trebuie sa fie adresabile si configurabile in totalitatea lor prin intermediul unei singure interfete de management si nu prin configurarea separata pentru fiecare echipament disponibil in respectivele platforme; ▪ Platforma de virtualizare trebuie sa permita agregarea tuturor resurselor fizice (placi de retea, switch-uri de comunicatie integrate in platformele de procesare) si virtuale de comunicatie (switch-uri virtuale) intr-un singur nivel unitar de comunicatie, adresabil la nivelul intregii infrastructuri virtuale indiferent de complexitatea acesteia sau a platformelor de procesare si comunicatie ce se integreaza prin intermediul ei.Deasemenea trebuie sa ofere mecanisme automate de evaluare si prioritizare continua a accesului masinilor virtuale si aplicatiilor rezidente la resursele de comunicatie disponibile, permitand alocarea si realocarea dinamica a acestor resurse in functie de cerintele de moment sau conform unor politici prestabilite; ▪ Platforma trebuie sa permita gruparea si organizarea logica a resurselor de procesare aplicații in functie de necesitati, precum si izolarea acestor grupari de resurse, respectiv sa asigure flexibilitatea

Caracteristica	Cerinta tehnica minimala
	necesara maririi cantitatii de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari.Accesul masinilor virtuale si apartenenta la aceste grupari de resurse trebuie sa se faca atat in mod manual prin interventia unui operator cat si pe baza unor politici dinamice de acces; ▪ Platforma trebuie sa ofere functionalitati integrate de pornire/repornire a oricarei masini virtuale (indiferent de aplicatiile si serviciile ce ruleaza pe respectivele masini virtuale), in cadrul aceluiasi server sau pe servere diferite, in cazul detectarii nemijlocite a unei probleme de functionare a masinii virtuale au a aplicatiilor si serviciilor ce ruleaza pe aceste masini virtuale. Scenarii posibile ce necesita implementarea a unui astfel de mecanism de recuperare ar putea fi: blocarea sistemului de operare ce ruleaza in masina virtuala, intreruperea cailor de comunicatie catre platformele de stocare, intreruperea cailor de comunicatie catre platforma comuna de management, etc; ▪ Platforma trebuie sa ofere mecanisme integrate de balansare a incarcarii resurselor fizice si virtuale disponibile in infrastructura si redistribuire a sarcinilor generate de utilizatori, servicii si aplicatii, prin integrarea cu platformele hardware, indiferent de producatorul respectivelor elemente de infrastructura. Aceste mecanisme trebuie sa fie disponibile atat la comanda prin interventia unui operator cat si prin operatiuni automate definite in functie de necesitati, gradul de ocupare al resurselor si/sau pe baza unor reguli/politici prestabilite; ▪ Platforma de virtualizare trebuie sa ofere redundanta completa a arhitecturii, atat la nivelul elementelor virtuale distincte (procesoare, memorie, elemente de comunicatie, masini virtuale, etc) cat si la nivelul unor seturi intregi de echipamente de infrastructura (platforma de procesare, platforma de stocare, platform de comunicatie, etc) prin integrarea cu mecanismele redundante existente in aceste platforme si prin folosirea unor tehnologii de redundanta, balansare si fail-over aplicabile intregului spectru de functionalitate asigurata (masini virtuale, servcii, aplicatii, platforme de procesare, platforme de stocare, platforme de comunicatie); ▪ Platforma de virtualizare trebuie sa permita configurarea spatiului de stocare virtual prin integrarea directa cu platforma de stocare aleasa prin intermediul unor conectori/componente sau de la producatorul platformei de stocare, mecansim ce va permite extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri. Deasemenea prin integrare directa cu platforma de stocare, trebuie sa ofere mecanisme automate de monitorizare a incarcarii I/O si de alocare/realocare dinamica a resurselor I/O catre masinile virtuale in functie de cerintele acestora (ad-hoc sau conform unei politici prestabilite), realizand astfel o prioritizare inteligenta a accesului aplicatiilor la

Caracteristica	Cerinta tehnica minimala
	resursele de stocare; ▪ Prin aceleasi mecanisme de integrare (inclusiv la nivelul componentelor apelabile si programabile din cadrul altor platforme, componente de tip API) cu platformele de stocare ofertate, trebuie sa permita identificarea si folosirea optima a mecanismelor de asigurare a cailor redundante de acces in platformele de stocare si a mecanismelor terte de protectie a datelor stocate, incluzand volumele adresate direct de platforma de virtualizare, respectiv volumele de date folosite de aplicatii, servicii si utilizatori; ▪ Integrarea cu platformele de stocare alese trebuie sa permita alocarea dinamica de spatiu catre masinile virtuale, chiar daca acel spatiu nu este fizic disponibil in aceste platforme, permitand functionarea corecta a aplicatiilor si serviciilor ce necesita resurse stricte de spatiu de stocare, respectiv cresterea transparenta a volumelor de date prin adaugarea de resurse fizice de stocare (discuri) doar in momentul cand acestea devin necesare; ▪ Platforma trebuie sa includa mecanisme de catalogare si grupare a resurselor disponibile in platformele de stocare, indiferent de tipul, producatorul si numarul acestora (tipuri de discuri, latenta, tipul volumelor si metoda de export aplicata asupra lor), permitand astfel crearea de profile de stocare si asocierea acestor profile cu distribuirea/redistribuirea masinilor virtuale in functie de cereri temporare ale aplicatiilor sau in baza unor politici predefinite; ▪ Deasemenea trebuie sa includa atat mecanisme automate de evaluare continua a necesarului de resurse I/O cat si mecanisme de pozitionare si repozitionare a masinilor virtuale in gruparile de resurse de stocare in functie de cerintele initiale ale aplicatiilor, respectiv in functie de cerintele evaluate in mod continuu. Astfel se obtine o balansare permanenta a distributiei masinilor virtuale proportional cu gruparile de resurse de stocare, indiferent de cerintele de performanta si capacitate de stocare ale respectivelor masini virtuale; ▪ Trebuie sa integreze mecanisme de agregare a conexiunilor fizice de retea disponibile in platformele de procesare, astfel incat sa poata oferi un sigur nivel virtual si unificat de comunicatie, nivel ce va fi disponibil pentru intregul set de aplicatii si servicii gazduite in platforma de virtualizare.Mecanismele vor fi independente de platformele de procesare si de cele de comunicatii, permitand adaugarea transparenta de functionalitati specifice de comunicatie (management, control si tipuri de protocol suportate) de la producatori terti.Se va obtine astfel implementarea unui set comun de functionalitati, unitar la nivelul arhitecturii de retea (fizica si virtuala), set ce va permite distribuirea inteligenta, dinamica a incarcarii pe aceste conexiuni, respectiv redundanta atat la nivelul conexiunilor de retea fizice/virtuale, cat si la nivelul strict al setului de functionalitati implementate, indiferent de producatorul platformelor de procesare si de comunicatie folosite;

Caracteristica	Cerinta tehnica minimala
	▪ Platforma trebuie sa implementeze mecanisme de asigurare dinamica a prioritizarii accesului la aplicatii si servicii, prin integrarea directa cu platformele de stocare si de comunicatie ofertate, respectiv prin aplicarea de politici si profile asupra accesarii datelor ce constituie masinile virtuale respective si/sau sunt folosite de catre respectivele aplicatii, indiferent de locatia respectivelor date (rezidente in platforma de stocare sau tranzitate prin mediile de comunicatie fizice/virtuale).Se va obtine astfel garantarea accesului prioritar la aplicatiile si serviciile critice din infrastructura; ▪ Platforma va trebui sa integreze mecanisme automate de instalare/provizionare a unei intregi imagini preconfigurate de hypervizor, mecanism necesar in cazul adaugarii rapide a unui nou server in platformele de procesare virtualizata, precum si mecanisme automate de instalare/provizionare a actualizarilor software la nivelul sistemelor de operare instalate in masinile virtuale, mecanisme idependente de, dar integrate cu functionalitatile de actualizare ale respectivelor sisteme de operare; ▪ Prin integrarea cu resursele de management, platforma de virtualizare trebuie sa permita mecanisme integrate de mutare a masinilor virtuale de pe un server pe altul sau dintr-un datacenter in altul fara oprirea sistemului de operare ce ruleaza in masina virtuala si fara intreruperea serviciului oferit de aplicatia/aplicatiile din masina virtuala.Aceleasi mecanisme trebuie sa permita atat mutarea intregului harddisk virtual concomitent pentru oricare masina virtuala in cadrul aceluiasi datacenter sau intre datacenter-e diferite, independent de platforma de stocare folosita si de mecanismele de replicare ale acesteia, precum si extinderea automata a harddisk-urilor virtuale pe masura ce sistemul de operare si aplicatiile din masinile virtuale o cer.In acest fel vor deveni posibile scenarii automate, prin politici pre-definite/definibile, de consolidare a masinilor virtuale pe un numar prestabilit de servere si oprirea automata a serverelor fara activitate sau cu subutilizare a resurselor de procesare; ▪ Tot prin integrarea cu resursele de management, platforma de virtualizare trebuie sa permita operatiuni automate, bazate pe politici pre-definite/definibile, de repornire (pe o alta platforma de procesare) a masinilor virtuale individuale, precum si a seturilor de masini virtuale ce au fost definite ca deservind o singura aplicatie/serviciu sau un sub-set al unei aplicatii/serviciu, in eventualitatea unei defectiuni hardware majore la nivelul platformelor de procesare; ▪ Platforma trebuie sa includa functionalitate de rulare in paralel a unei masini virtuale sau a unui set de masini virtuale ce deservesc o singura aplicatie/serviciu, pe un numar de minim doua echipamente distincte din platformele de procesare.Mecanismul trebuie sa foloseasca tehnologii independente dar integrate cu platformele de

Caracteristica	Cerinta tehnica minimala
	procesare si de stocare, asigurand replicarea transparenta si sincrona a continutului de memorie si a continutului de disc asociat unei masini virtuale, respectiv unui set de masini virtuale, fara introducerea de latenta in respectivele platforme sau in functionarea masinilor virtuale; ▪ Platforma trebuie sa includa o componenta de administrare si monitorizare dedicata, disponibila atat la nivelul echipamentelor fizice ce alcatuiesc platformele de procesare, stocare si comunicatie cat si la nivelul masinilor virtuale, ale resurselor virtualizate, aplicatiilor, serviciilor si protocoalelor insumate in infrastructura.In vederea accesului facil la functiile de administrare si monitorizare oferite, platforma trebuie sa permita acces atat prin consola locala/la distanta cat si prin browser web si prin platforma de management dedicata; ▪ Trebuie sa permita autentificarea utilizatorilor bazata pe roluri si privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director. Deasemenea trebuie sa permita crearea facila de politici dinamice de acces la resursele de procesare, precum si de disponibilitate ale acestora; ▪ Separarea privilegiilor administrative trebuie sa se poata face pe orice element disponibil in interfata de administrare (server, utilizator, resursa de procesare, stocare, retea, etc), permitand astfel crearea de zone/domenii de securitate in functie de aplicatii si/sau roluri functionale, nu in functie de elementele disponibile in infrastructura de procesare, stocare si comunicatie; ▪ Platforma trebuie sa asigure si mecanisme de definire si aplicare a profilelor standard de configuratie pentru serverele ce fac parte din infrastructura virtuala.Deasemenea sa permita configurarea de politici de aplicare a acestor profile in functie de necesitatile de moment sau in concordanta cu politica stabilita in prealabil; ▪ Componenta de management trebuie sa se integreze sau prin intermediul unor conectori/componente cu platforma de procesare si cu platforma de stocare in vederea realizarii operatiunilor de backup direct din aceste platforme, precum si pentru crearea rapida a unor zone izolate atat din punct de vedere al securitatii cat si al gruparilor de resurse de procesare, stocare si retea, in scopul testarii si dezvoltarii; ▪ Componenta de management trebuie sa integreze functii de monitorizare analitica a integritatii si performantei platformei de virtualizare, functii ce vor permite anticiparea proactiva a problemelor de performanta si disponibilitate. Respectivele mecanisme trebuie sa se bazeze atat pe modele de utilizare predefinite, cat si pe functii integrate de auto-invatare, astfel incat sa se asigure vizibilitate completa asupra problemelor din infrastructura; ▪ Trebuie sa integreze functii de administrare si optimizare a spatiului disponibil in platformele de stocare si a gradului de disponibilitate

Caracteristica	Cerinta tehnica minimala
	si ocupare a resurselor virtualizate din plaformele de procesare si comunicatie, astfel incat sa balanseze in permanenta nevoile curente ale masinilor virtuale (atat la nivel individual cat si la nivel global) in raport cu resursele fizice din respectivele platforme, eficientizand utilizarea respectivelor resurse fizice; ▪ Platforma trebuie sa integreze un portal de tip dashboard pentru afisarea si analizarea tuturor informatiilor legate de disponbilitate, grad de ocupare a resurselor, metrici de performanta, istoric al actiunilor administrative si corective, precum si recomandari de optimizare a intregii functionalitati puse la dispozitie de platforma de virtualizare.Portalul trebuie sa permita executarea directa de actiuni corective si administrative asupra elementelor de infrastructura vizate (masini virtuale, resurse de procesare, stocare si comunicatie), actiuni bazate pe recomandarile afisate in portal in urma analizelor efectuate asupra respectivelor elemente; ▪ Datele monitorizate trebuiesc automat analizate si exprimate sub forma de metrici de stare, risc si eficienta, permitand identificarea rapida a potentialelor probleme in infrastructura; ▪ Platforma trebuie sa ofere analize de capacitate si sa identifice explicit resursele ce sunt supra-utilizate, ajutand in procesul de redistribuire a sarcinilor de incarcare intre elementele platformei in scopul eficientizarii rularii aplicatiilor si serviciilor, respectiv sa ofere scenarii predefinite de simulare a incarcarii pentru a elimina procesele deductive de alocare a resurselor platformei; ▪ Platforma trebuie sa ofere analize automate a proceselor de instalare si configurare a mediului virtualizat, in scopul detectarii rapide a eventualelor probleme ce pot aparea datorita configurarilor defectuoase sau a elementelor noi introduse in infrastrcutura; ▪ Trebuie sa integreze functii automate de alertare in cazul depasirii pragurilor optime de functionare, atat pentru starea tuturor elementelor platformei de virtualizare, cat si pentru metrici de performanta si capacitate;
Licentiere	Solutia va fi oferita pentru un numar de cel puțin 48 procesoare fizice, cu minim un centru de management si monitorizare. Solutia va contine toate elementele de licentiere necesare pentru indeplinirea obiectivelor propuse si pentru respectarea atat a cerintelor generale de arhitectura cat si a cerintelor specifice fiecarei componente in parte;

3.8.12. Asistenta tehnica

Având in vedere numărul mare de utilizatori ai sistemului este necesara furnizarea și instalarea unei soluții de asistenta tehnica (help-desk) care sa limiteze cauzele și efectele defectelor PSCID și totodată să asigure monitorizarea SLA-ului stabilit. Sistemul va permite preluarea, înregistrarea si urmărirea sesizărilor (incidente/tickete) privind funcționarea anormală a întregului sistem informatic. Sesizările vor putea fi preluate de către personalul IT specializat, prin telefon, e-mail, web sau alte canale de comunicare și vor putea fi înregistrate în sistemul de Help-desk. Incidentele/ticketele se vor aloca personalului competent care

comunica modalitatea de rezolvare a incidentului către solicitant. Sistemul va permite ca incidentele care nu pot fi gestionate de către personalul intern sa poată fi escaladate in exterior spre rezolvare de către furnizorii de echipamente hardware, comunicaţii, software, etc, in funcţie de tipul incidentului.
Sistemul va permite ca pe parcursul derulării activităţii de Help-Desk, specialiştii IT sa poată inregistra modalităţile de rezolvare pentru incidentele frecvent întâlnite sub forma de baza de cunoştinţe, astfel incat la reapariţia unui incident similar, modalitatea de rezolvare sa fie deja înregistrata in sistem si sa permită un răspuns prompt prin evitarea paşilor de re-diagnosticare.
Numărul de utilizatori care vor opera centrul de Help Desk va fi de 20. Furnizorul va asigura implementarea şi operaţionalizarea soluţiei complet funcţionale de help-desk pentru cei 20 de operatori (din care 8 concurenţi).

Sistemul va permite:

- micsorarea timpilor de nefunctionare a diverselor componente/sisteme;
- identificarea si corectarea punctelor vulnerabile ale sistemelor supervizate;
- creşterea vitezei de intervenţie a personalului IT;
- prioritizarea corecta a activităţii de rezolvare a incidentelor;
- urmărirea timpilor de intervenţie din partea furnizorilor si a modului in care aceştia isi respecta contractele de service si suport.

Soluţia de help-desk oferita va realiza gestionarea tuturor cerinţelor de service si suport ale organizatiei. Aceasta soluţie va asigura administrarea problemelor apărute in cadrul organizaţiei, escaladarea si transferul acestora, managementul alertelor si va oferi opţiuni de căutare si raportare.

Cerinţe Generale:

- Solutia propusa trebuie sa se bazeze pe un pachet de aplicatii software care sa ofere functionalitati si procese specifice pentru managementul si administrarea incidentelor/ticketelor si a relatiilor cu solicitantii.
- Solutia propusa trebuie sa se bazeze pe un pachet de aplicatii software disponibile comercial (COTS –Commercial of the Shelf).
- Solutia trebuie sa fie conforma cu practicile ITIL v3 si sa acopere minim urmatoarele procese ITIL: Request Management, Incident Management, Problem Management
- Solutia trebuie sa contina functionalitati proprii de securitate si audit.
- Solutia trebuie sa aiba definite implicit rolurile de baza din ITIL pentru scurtarea perioadei de implementare si sa permita definirea unor alte roluri in functie de necesitati.
- Utilizatorii sa aiba posibilitatea sa isi aleaga din interfata aplicatiei rolul in care activeaza in solutie fara a fi nevoie sa iasa si sa reintre in sistem (conform ITIL, o persoana poate indeplini mai multe roluri). Rolurile pe care o anumita persoana poate sa le indeplineasca trebuie sa fie definibile doar de administratorul solutiei.
- Functionalitatile solutiei trebuie sa fie adaptate rolurilor pe care utilizatorii le indeplinesc, schimbarea rolului sa duca la schimbarea tipului de interfeta in care activeaza.
- Solutia trebuie sa dispune de mecanisme de securizare a accesului utilizatorilor la datele din aplicatie prin definirea de roluri cu nivele de acces diferite. Solutia trebuie sa permita definirea unui numar nelimitat de roluri in aplicatie. Solutia trebuie sa perminta atasarea unuia sau mai multor roluri pentru un utilizator.

- Soluţia trebuie să poată funcţiona pe oricare dintre platformele software următoare: Windows, UNIX şi distribuţii majore Linux.
- Soluţia trebuie să poata utiliza sisteme de gestiune a bazelor de date ca: SQL Server, Oracle.
- Accesul la aplicaţie trebuie sa se realizeze în intregime prin intermediul unei interfete WEB, accesibilă printr-un browser consacrat. Nu se admit soluţii tip client-server.
- Soluţia trebuie să suporte reguli de business flexibile care pot varia conform unor factori multipli.
- Soluţia va oferi suport complet pentru orchestrarea de procese (workflow).
- Solutia propusa trebuie sa permita integrarea folosind servicii si adaptori in conformitate cu standardele deschise, cum ar fi WSDL, XML/JSON.

Cerinte specifice

- Aplicaţia trebuie sa fie accesibila prin interfaţa web securizata;
- Sa dispună de mecanisme predefinite pentru implementarea functionalitatilor de Incident management, Problem management, Change management;
- Sa fie uşor de exploatat astfel incat sa fie minimizata posibilitatea de apariţie a erorilor umane. Astfel:
  - Trebuie sa asigure o interfaţa prietenoasa utilizatorului, facilitaţi de navigare confortabila utilizând mijloace naturale de căutare (meniuri bara, pop-up pull-down) si sa permită navigarea in toate modulele la care utilizatorul are acces fara deconectarea si reconectarea utilizatorului;
  - Sa permită introducerea incidentelor/ticketelor de către utilizatori prin interfaţa web de către operatorul serviciului de asistenta;
  - Sa permită ataşarea la incidentul introdus a documentelor electronice (de diverse formate);
  - Sa permită configurarea unor fluxuri de operaţiuni pentru rezolvarea incidentelor/ticketelor in funcţie de tipologia acestora.
  - Sa poată fi configurata astfel incat sa escaladeze automat incidentele/ticketele in funcţie de prioritatea lor sau in situaţia in care acestea nu respecta condiţiile de calitate (timpul maxim admisibil pentru rezolvare);
  - Sa permită monitorizarea timpilor de rezolvare;
  - Solutia trebuie sa permita identificarea la nivelul interfetei aplicatiei a solicitarilor pentru care nivelul de SLA (Service Level Agreement) definit a fost incalcat.
  - Solutia trebuie sa permita configurarea de reguli automate de escaladare a cererilor si de notificare pentru a se asigura incadrarea in nivelul de SLA definit.
  - Solutia trebuie sa permita afisarea la nivelul fiecareri solicitari a mometului in care SLA-ul agreat pentru rezolvarea acelei solicitari va fi depasit.
  - Solutia trebuie sa permita oprirea contorului de timp la schimbarea status-ului in care se afla solicitarea (Hold).
  - In definriea SLA-urilor timpul de rezolvare trebuie sa fie calculat tinand cont de un program de lucru care se poate defini (workshift).
  - In cazul incidentelor trebuie sa permita definirea unei matrici flexibile de calcul a Prioritatii incidentelor in functie de nivelul de Urgenta si Impact conform specificatiilor ITIL.
  - Solutia trebuie sa permita inregistrarea de relatii de tip Parinte-Copil intre incidente sau Probleme. Deasemenea trebuie sa permita propagarea automata catre solicitarile copil a rezolutiei sau a altor informatii completate in solicitarea parinte.

- Solutia trebuie sa ofere posibilitatea deschiderea unei Probleme dintr-un Incident si relationarea Problemei cu unul sau mai multe Incidente.Analiştii sa poată salva soluţiile propuse intr-o baza de cunoştinţe cu arborescenta pe subiecte, puncte de interes etc;
- Baza de cunoştinţe trebuie sa dispună de facilitati de căutare după cele mai frecvente întrebări si Sa ofere metoda de căutare a informaţiei de tip „arbore de decizie" in baza de cunoştinţe;
- Baza de cunoştinţe sa permită definirea de drepturi diferite de acces la documentele publicate in funcţie de grupul de utilizatori;
- Trebuie sa permita introducerea de feedback-uri din partea utilizatorilor, pentru evaluarea si notarea calitatii raspunsurilor primite in urma interogarilor efectuate.
- La deschiderea unei solicitari de catre utilizatori trebuie sa se poata face mai intai o cautare in baza de cunostinte a unor posibile solutii astfel incat sa se reduca numarul de solicitari pentru care s-a dat deja o rezolvare.
- Toate activitatile de cautarile efectuate de utilizatori trebuie sa poata fie inregistrate si disponibile pentru analiza si determinarea graduli de utilitate al documentelor publicate.
- Solutia trebuie sa dispuna de raporate detaliate despre gradul de accesare al documentelor publicate precum si alti parametri
- Un solicitant trebuie sa poatea avea multiple incidente/tickete deschise simultan.
- Solutia propusa trebuie sa ofere suport complet integrat pentru toate canalele de contact, e-mail, portal web.
- Solutia propusa trebuie sa ofere capabilitati de a alocare a incidentelor/ticketelor bazata pe capabilitatile angajatilor.
- Solutia propusa trebuie sa permita inregistrarea si regasirea istoriei complete de comunicare (mesaje receptionate si emise) a solicitantului, de pe toate canalele de interactiune si zonele de cereri, informari si servicii.
- Solutia propuse trebuie sa ofere capabilitati de parsing pentru email-urile inbound pentru diverse campuri cum ar fi expeditorul, corpul e-mailului, in scopul procesarii acestora.
- Trebuie oferita posibilitatea utilizarii de sabloane pentru raspunsurile la emailuri.
- Solutia trebuie sa puna la dispozitie un instrument vizual care sa permita modificarea interfetei si a paginilor prezentate utilizatorilor, extinderea functionalitatilor si a fluxurilor de lucru, extinderea schemei bazei de date
- Solutia trebuie sa aiba incluse capabilitati de suport remote si capabilitati de self-service;
- Solutia trebuie sa dispuna de un instrument care sa permita analistilor sa se conecteze la distanta pe statia utilizatorilor, fara a necesita instalarea unor agenti pe acea statie, sa poata rula scripturi de reparare sau sa poata extrage date relevante despre starea sistemului (procese care ruleaza, loguri, servicii). Toate aceste activitati realizate de catre analist pentru rezolvarea problemei sa fie inregistrare si sa se salveze in logurile solicitarii.
- Solutia trebuie sa aiba un modul de "live chat" care sa permita un dialog direct intre utilizator si analist iar conversatia dintre acestia sa fie automat salvata ca si istoric al solicitarii
- Functionalitati de Raportare. Solutia trebuie sa aiba un modul dedicat de raportare (Business Objects sau echivalent) care sa includa un set predefinit de raporte dar sa permita si dezvoltarea de rapoarte noi.
- Solutia trebuie sa permita rularea rapoartelor in functie de cerintele utilizatorilor si in contextul de lucru al fiecarui analist.
- Solutia trebuie sa pemita programarea rularii de rapoarte si expedierea acestora pe email.
- Solutia trebuie sa pemita exportul de rapoarte in format EXCEL si PDF.

- Modulul de raportare trebuie sa fie integrat cu solutia de Helpdesk permitand autentificarea o singura data a utilizatorilor in aplicatie fara a mai cere o autentificare suplimentara atunci cand aceseaza un raport.
- Regulile de securitate aplicate asupra datelor din aplicatia Helpdesk trebuie sa se aplice automat si asupra rapoartelor.

3.9. *AMENAJARE CENTRU DE DATE*

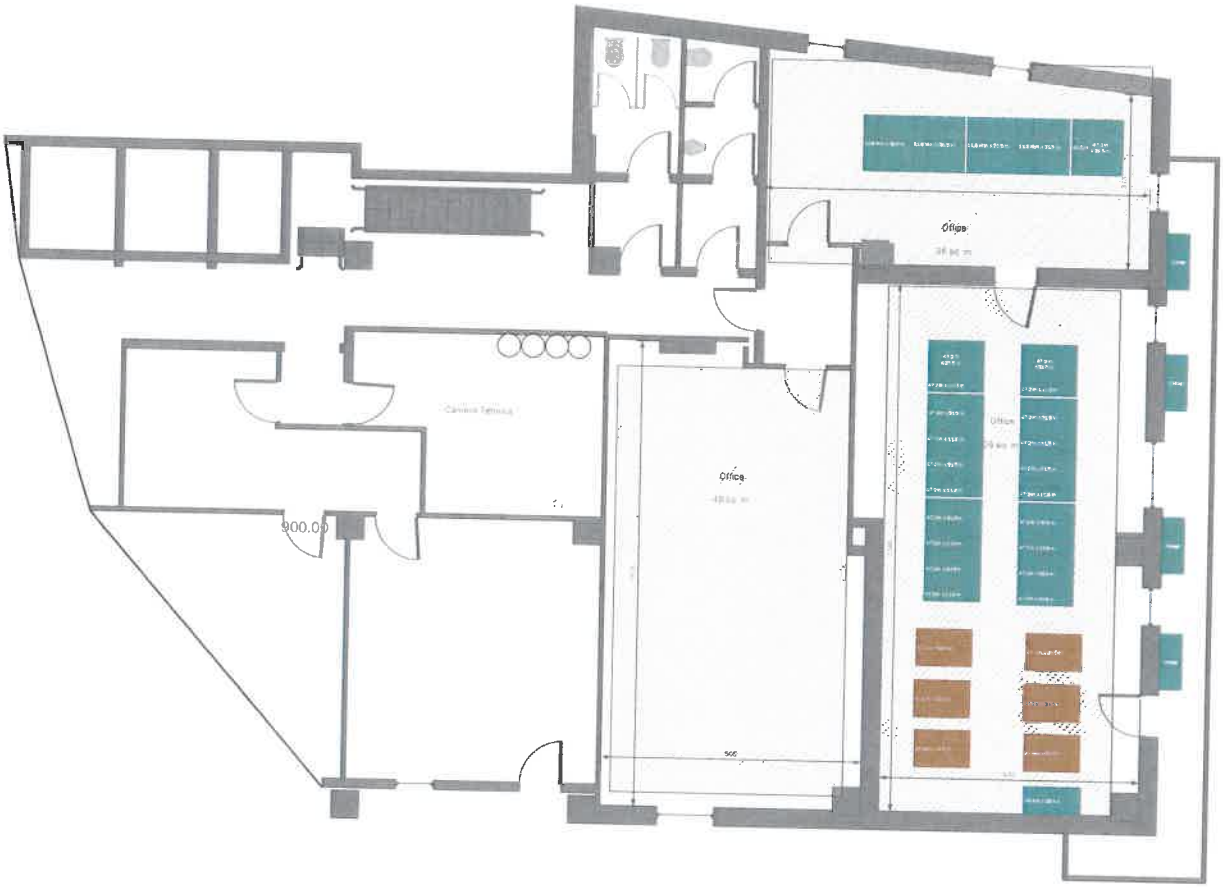
3.9.1. Locaţii

Locatia propuse este localizata in str. Italiană nr. 22. Locul de amplasare este prezentat in imaginea urmatoare:

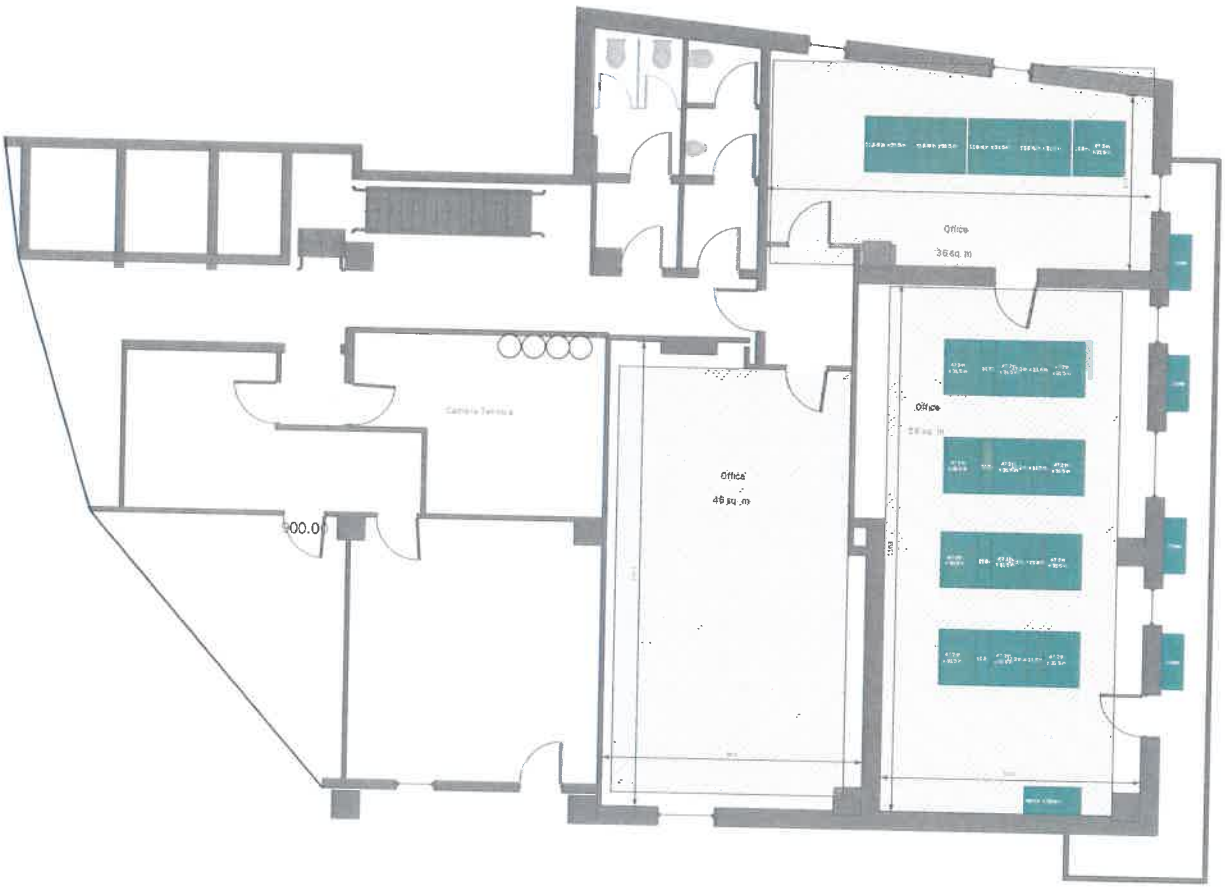
Echipamentele furnizate pentru proiect vor fi conforme cu normele europene. Pentru echipamentele exterioare se va ţine seama de normele naţionale şi europene privind acustica urbană şi limitele admisibile ale nivelului de zgomot.

Pentru sistemele să poata functiona în conditii de siguranţa este propusă amenajarea/reamenajarea a două săli in cadrul ADR.

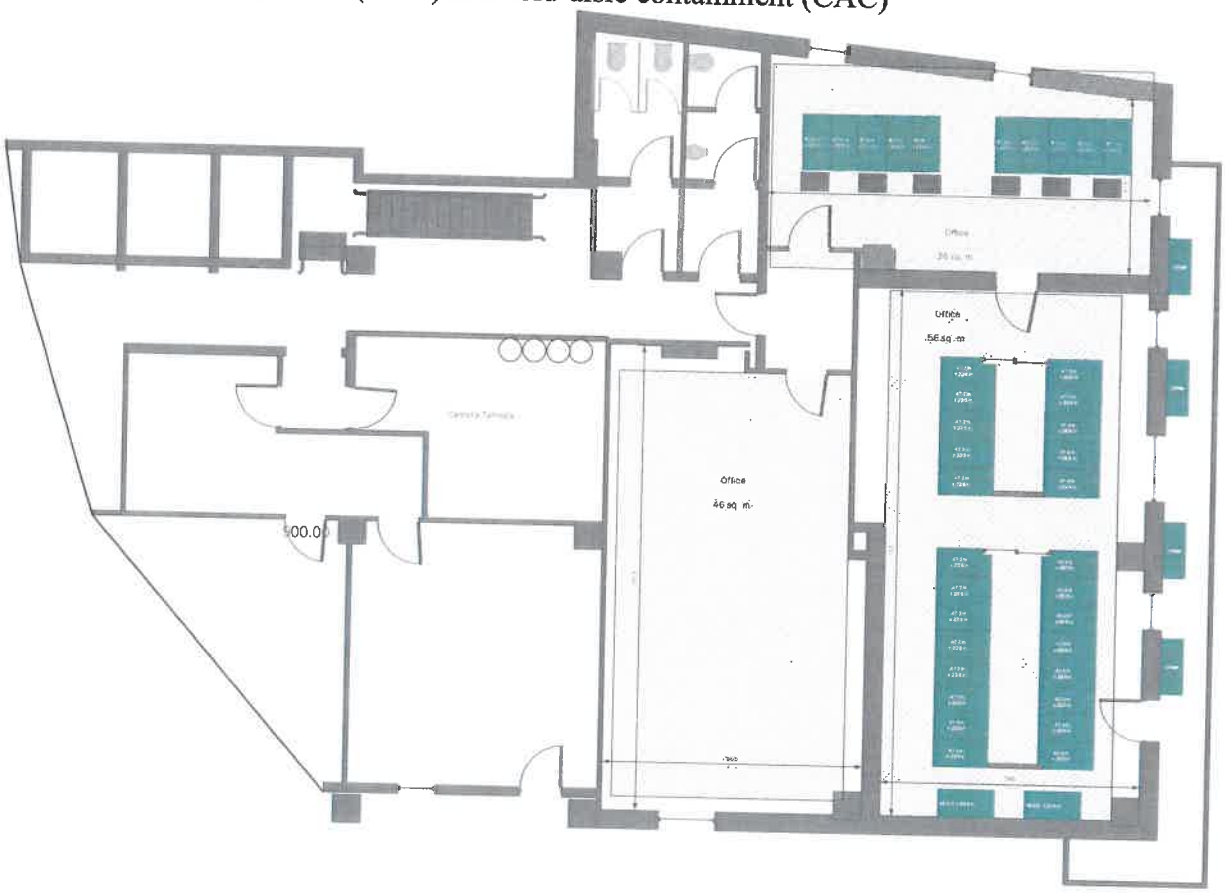
Variante de amenajare
V1 - Densitate mare Liquid cooling


Office
Office
900.00

V2 - densitate mare Liquid Cooling



V4 - hot-aisle containment (HAC) and cold-aisle containment (CAC)



3.9.2. Protecție fizică

Pentru camerele propuse este necesară realizarea unor sisteme de protecție antiefracție, protecție mecanică adecvată, detecție efracție, control acces.

Solutia pentru amplasarea serverelor, echipamentelor IT si echipamentelor de comunicatie

Pentru gazduirea serverelor, echipamentelor IT si echipamentelor de comunicatie camera de date, se propune utilizarea de rack-uri metalice (5 buc) care sa asigure cel putin urmatoarele:

- sa asigure amplasarea echipamentelor cu latimea standartizata ETSI de19"
- sa fie de tipul 42 U care se incadreaza intr-un gabarit vertical normal (2,6m) de incapere
- sa fie echipate cu console KVM
- sa fie structurate, conform figurii 5, cu minimul de componente indicate
- sa poata fi reglate la nivel si fixate antiseismic
- sa permita accesul cablurilor de electroalimentare si telecomunicatii prin partea inferioara, superioara si laterala (daca nu se instaleaza capacele laterale)
- sa aiba dispozitiv marcat de impamantare (surub)
- sa fie asigurate prin incuierea usilor de acces
- sa poata fi asezate in randuri cu posibilitate de fixare a rack-urilor intre ele
- sa asigure minimul de conditii tehnice si dimensiuni solicitate

Pentru amplasarea serverelor de aplicatie se vor utiliza dulapuri (rackuri) cu latimea de 0,75m, adecvate pentru instalarea de servere de 19" sau de servere rackabile la 19".
Pentru echipamentele de comunicatii se vor utiliza dulapuri cu latimea de 0,75m care asigura un spatiu lateral sporit pentru amplasarea unui numar mai mare de cabluri si patchcorduri de interconexiuni.
Dulapurile metalice pentru amplasarea echipamentelor se asambleaza pe randuri, conform planurilor de amplasament ale infrastructurii in incintele Centrului de date.
In vederea electroalimentarii echipamentelor instalate, fiecare rack va fi prevazut cu doua seturi de distribuitoare de electroalimentare (rack PDU) dimensionate conform consumului estimat si numarului de echipamente per rack din tema proiect.
Conectorul cordonului fiecarui rack PDU se conecteaza (pe gratarul de curenti tari amplasat in lungul randului de rackuri) cu cablul prevazut cu conector mama care este legat pe iesirea corespunzatoare alimentata dintr-un UPS.
Se vor pune la dispozitie cablurile necesare pentru realizarea interconectărilor (la nivelul rețelei de alimentare, LAN, SAN)

Pregătirea instalării echipamentelor

Pereții interiori si exteriori ai salii de echipamentelor trebuie finisați, finisarea lor asigurând:

- protectia antiincendiu (F90 minimum)
- izolarea termica (cu vata minerala)
- bariera antivapori
- acoperire cu vopsea antistatica.

Ferestrele exterioare vor fi blocate si vor asigura izolația termica necesara pentru a minimiza schimbul de caldura cu exteriorul.
Ușa prin care se delimitează perimetrul camerei de date va fi metalică, antifoc, cu acelasi grad de protectie ca si a peretilor. cu deschidere spre sensul de evacuare in caz de incendiu. In interior usile vor fi dotate cu bara antipanica, pentru deschiderea lor. Ușa va fi prevazută cu dispozitiv de deblocare conectat la sistemul de control de acces si detectie/stingere incendii.

Pardosela tehnologica din sala de calculatoare

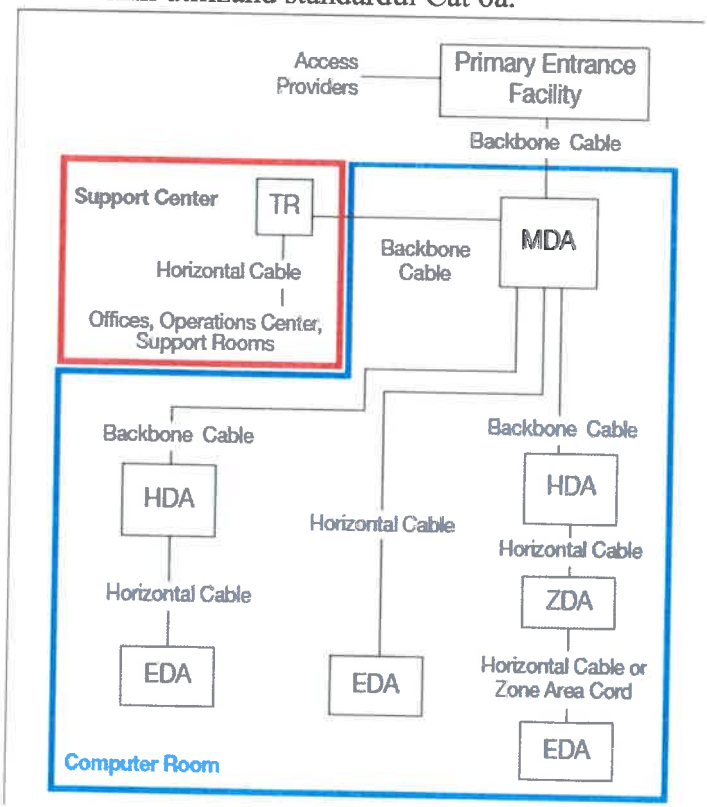
Se va instala un dispersor de greutate şi o podea tehnică.
Se va reface tavanul fals şi se vor instala corpuri de iluminat (led).
Pardoseala suprainaltata va fi realizata pe o structura de suport, metalica si va suporta minimum 1200 kg/mp. Inainte de instalarea pardoselii suprainaltate planseul va fi acoperit cu vopsea antistatica. Aceasta vopsea va fi compatibila cu rasina epoxidica utilizata pentru lipirea suportilor verticali ai structurii pardoselii suprainaltate.
Structura portanta de suport va fi formata din:

- coloane verticale reglabile cu cap profilat pentru a fixa traversele orizontale cu suruburi si picior profilat pentru fixare in planseu cu suruburi, din otel ambutisat, protejat anticoroziv,
- traverse orizontale, realizate din otel profilat, protejat anticoroziv care se fixeaza cu suruburi de capul profilat al coloanei reglabile.

Panourile pardodelii suprainaltate vor fi cu dimensiuni standard de 600x600 mm, realizate din conglomerat, ignifuge si antistatice.
Podeaua va fi prevazuta cu sistem echipotential.

Amenajare curenti slabi

Cablarea in camerele puse la dispozitie se vor realiza intr-o topologie centralizata. În această topologie, cablarea de la panoul principal de distributie (MDA) se conectează la panourile orizontale de distributie (HDA). Toata cablarea este centralizată într-un singur panoul orizontal de distributie (HDA) și comunicatiile vor fi distribuite de la HDA la echipamentele de distributie din rack-uri EDA (e). Acest scenariu utilizează un canal fizic cu trei conexiuni în cazul în care este cablarea orizontala este realizata de la panourile de patch-uri pentu echipamente EDA la panourile de distributie orizontale patch-uri HDA. Toate cablurile si conectica vor fi livrate de furnizor. Toate cablare se va realiza minim utilizând standardul Cat 6a.



Executantul de instalatii desemnat va prevedea toate materialele, echipamentele si forta de munca necesare pentru montarea si punerea în functiune a lucrarilor de instalatii de cablare structurata, asa cum rezulta din desenele si documentatia tehnica a proiectului realizata de furnizor cu accptul beneficiarului si memoriul tehnic.

Cerințe instalație de climatizare

Echipamentele IT trebuie mentinute la o temperatura medie recomandata de producator si care asigura o functionare corecta si cea mai lunga durata de viata. Pentru aceasta, centrele de date trebuie obligatoriu prevazute cu instalatii de climatizare care sa mentina aceasta temperatura, indiferent de temperatura mediului ambiant sau de caldura disipata de echipamente.
Dimensionarea instalatiei de climatizare rezulta din cerintele referitoare la puterea electrica necesara pe fiecare rack, anume 10 kW, iar numarul total de rack-uri ce va echipa camera tehnica este de 10 bucati. La aceasta se mai adauga necesarul de racire pentru unitatile de tip UPS.
UPS-ul va fi instalat la subsolu cladirii pentru toate rack-urile ce urmeaza a fi livrate.

Climatizarea trebuie prevazuta in camerele unde urmeaza a fi instalate echipamentele cu un nivel de protectie 2N. Chillerul va fi instalat in exteriorul camerelor.
Din punct de vedere constructiv, instalatia trebuie sa aiba unitati de distributie a aerului rece amplasate in rackuri metalice de 42U (2m) si trebuie sa includa o instalatie automata de umidificare, dezumidificare a aerului din incinta.

Cerințe sistem electric de alimentare a centrului de date

Sursa primara trifazica de energie electrica pentru centrul de date va fi amplasata fie in camera echipamentelor fie intr-o incapere separata va avea urmatoarele specificatii pentru site-ul principal:

- 2 surse trifazice diferite, una principala si una rezerva cu comutare automata in caz de avarie de pe una pe alta
- 1 grupul electrogen cu pornire automata care dubleaza una din sursa primara
- Sistem de automatizare pentru racordurile trifazice
- Sistem de distributie automatizat
- Tabloul general de distributie a sursei primare trifazice de joasa tensiune si a impamantarii, numai pentru consumatorii Centrului de date, amplasat in spatiul special amenajat.

Pentru redundanta, se vor folosi sisteme UPS, cu dubla conversie non stop (online), si generator de curent dimensionate corespunzator.
Dimensionarea instalatiei de alimentare redundanta rezulta din cerintele referitoare la puterea electrica necesara pe fiecare rack, anume 10 kW.
Furnizorul va evalua solutia existenta si va propune o solutie de back-up de alimentare, capabila sa asigure functionarea pe o perioada lunga de timp, cu capaciate de acoperire a tuturor consumatorilor, inclusiv incarcarea acumulatorilor aferenti UPS-urilor.
Generatorul electric va avea capacitatea de pornire automata atunci când se intrerupe alimentarea cu energie electrica pentru o perioada de timp mai lunga decat un interval de siguranta prestabilit (programabil, intre 10 sec si 30 min) sau cand cel putin una din staţiile de alimentare neintreruptibila (UPS) epuizează rezerva energetica din bateria de acumulatoare.
Împământarea tuturor barelor de pământ ale tablourilor aferente surselor primare se va realiza prin conectarea acestora la bara de împământare din tabloul general al clădirii prin cablu multifilar de cupru de secțiune adecvata. Valoarea prizei de pământ nu trebuie sa fie mai mare de 0,5 - 1 ohmi.

Cerinte sisteme de detectie, alarmare si stingere in caz de incendiu

Sistemul de stingere cu gaz inert trebuie sa fie compus din 2 parti independente:

- Sistemul de detectie, semnalizare si comanda stingere incendiu;
- Instalatia de stocare si deversare gaz;

In functionare normala sistemul de detectie, semnalizare si comanda stingere incendiu trebuie sa asigure urmatoarele functii:

- Detectia automata a incendiului; (in acest caz detectia punctiforma va fi preluata pe una din liniile centralei de stingere)
- Comanda automata de stingere;
- Comanda manual-electrica de semnalizare incendiu si de stingere;
- Blocarea stingerii in cazul in care nu sunt indeplinite conditiile de stingere;
- Confirmarea efectuarii comenzii finale de stingere;

- Comutarea in regim de mentenanta a instalatiei;
- Monitorizarea fiecarui circuit electric si semnalizarea defectelor de sistem;
- Monitorizarea indeplinirii conditiilor de asigurare a stingerii prin deversarea gazului (cilindri incarcati la presiunea prescrisa);
- Oprirea ventilatiei/climatizarii in zonele protejate prin contacte NI dedicate, libere de potential;

Sistemul va respecta normele EN12094 si EN54.

Monitorizarea instalaţiilor auxiliare

Instalatiile auxiliare (UPS, climatizare) trebuie sa fie dotate fiecare cu sisteme individuale de monitorizare a parametrilor de functionare avand posibilitatea de a semnaliza optic si acustic iesirea din parametrii normali si monitorizarea acestora de la distanta prin unitatea de management Web/SNMP prevazuta cu port Ethernet conectata la instalatia manager de infrastructura.

Monitorizare mediu rack

Pentru monitorizarea mediului incintelor in care sunt amplasate rackurile cu servere si echipamente de telecomunicatii trebuie prevazut un sistem de monitorizare a mediului prevazut cu senzori pentru monitorizarea temperaturii aerului, umiditatii, prezentei fumului, stare usa, vibratii. Senzorii se vor amplasa in punctele critice ale incintei si se conecteaza fiecare la porturile aferente unitatii inteligente a sistemului de monitorizare, amplasata intr-unul dintre rackuri. Insumarea senzorilor se va face prin Swich-uri. Unitatea inteligenta va fi prevazuta cu agent SNMP si port Ethernet pentru monitorizare la distanta, cu posibilitate de declansare de alarma optica si acustica si va fi interconectata la managementul de infrastructura.

Monitorizare acces rack-uri

Monitorizarea accesului se va realiza in fiecare incinta cu o instalatie speciala de monitorizare a accesului in incinte care contine:

- serverul de monitorizare cu posibilitate de monitorizare de la distanta prin portul Ethernet, interconectat la LAN-ul de management al centrului de date si comunicatii
- video camere color IP
- senzori magnetici de controlul deschiderii usilor de acces a usilor de la rackuri.

Activitati:

- Asigurarea de către furnizor a amenajărilor de arhitectură şi construcţii, pereţii, uşile şi celelalte lucrări de pregătire ale spaţiului, precum şi pardoseala supraînălţată şi demararea serviciilor de instalare a echipamentelor infrastructurii de suport în Centrul de date.
- Se vor instala sistemul de suport cabluri, cablurile şi circuitele electrice din sala de calculatoare pentru a suporta necesarul de putere a Centrului de date, asigurându-se integrarea în sistemele electrice existente ale facilităţii.
- Se vor instala echipamentele externe ale sistemului de răcire, sistemul de conducte al circuitului hidraulic şi sistemul de control al mediului din Centrul de date.
- Se vor instala rack-urile pentru echipamente, echipamentele interioare ale sistemului de răcire, sistemul UPS şi distribuţia electrică protejată la rack-urile de echipamente, livrate în cadrul

proiectului, şi se testează infrastructura de suport, se instalează şi testează soluţiile de monitorizare.

- Se vor realiza toate lucrările necesare privind branşarea electrica a tabloului general daca solutia propusa impune acest lucru.
- Bransamentul electric este instalatia de distributie a energiei electrice care face legatura intre reteaua de distributie a furnizorului si tabloul general al abonatului. Punctul de delimitare a instalatiilor electrice dintre furnizor si abonat este la bornele de iesire din contorul de masurare a energiei electrice monofazat sau trifazat (dupa caz). Deci instalatia electrica dintre contor si tabloul general al abonatului reprezinta instalatia electrica de utilizare a abonatului.
- In functie de solutia propusa daca este necesara realizarea unei solutii care presupune spor de putere furnizorul va sprijini beneficiarul pentru realizarea lucrarilor de bransament si modernizare a tabloului electric general.

3.10. *SERVICII DE DEZVOLTARE SI IMPLEMENTARE PROIECT*

3.10.1. Serviciile de livrare si instalare software

Pentru asigurarea livrarii cu succes a infrastructurii software ale sistemului, trebuie sa fie pusa la dispozitie infrastructura hardware corespunzatoare si apoi finalizata arhitectura fizica a sistemului. Pentru fiecare mediu in parte vor trebui sa fie instalate conform arhitecturii produsele furnizate, in modul de disponibilitate solicitat.
Vor trebui astfel asigurate urmatoarele activitati:

- Finalizarea arhitecturii componentelor software-ului de baza;
- Instalarea componentelor software de baza;
- Configurarea sistemului software de baza;
- Integrarea componentelor software de baza;
- Testarea soluţiei.

3.10.2. Serviciile de dezvoltare

Pentru asigurarea dezvoltarii sistemului vor trebui asigurate cel putin urmatoarele categorii mari de activitati:

- Servicii de analiză a sistemului
- Servicii de modelare / proiectare a sistemului
  - Proiectarea modelului sistemului de date;
  - Definirea serviciilor aferente noului flux funcţional de sistem;
  - Definirea principalele funcţionalităţi de sistem folosind modele entitate-asociere sau UML2.0;
  - Proiectarea componentelor şi arhitectura de sistem;
- Dezvoltarea softului de aplicaţie
  - Instalarea si configurarea produselor COTS;
  - Dezvoltarea componentelor de software;
  - Integrarea componentelor software;
  - Testarea soluţiei software;
  - Configurarea sistemului software;
  - Obţinerea acordului final din partea beneficiarului proiectului.

Componentele software ce vor fi dezvoltate in cadrul proiectului vor avea la baza principiul de CI / CD pipeline (continuous integration / continuos deployment) astfel incat sa fie permise dezvolarea continua, testarea continua, integrarea continua, implementarea continua si monitorizarea continua a aplicatiilor pe parcursul ciclului de viata al acestora.

Se vor avea in vedere minim servicii pentru interconectarea PSCID cu nodul eIDAS, cu furnizorii de semnatura electronica (in calitate de furnizori de identitate si atribute), cu DEPABD din MAI (ca furnizor de servicii de identitate si atribute, sursa autoritara si de incredere) si cu minim 5 furnizori de servicii de e-guvernare (ex: MAI, MMJS, CNAS, ADR, ANAF).

Pentru integrarea PSCID cu solutiile de tip managementul identitatii ale furnizorilor de servicii de e-guvernare se vor avea in vedere urmatoarele solutii tehnologice:

- **Consolidare in cadrul PSCID**
- **Consolidarea tuturor identitatilor electronice ale cetatenilor regasite in serviciile electronice existente.**
- **Partajarea informatiilor aferente identitatilor electronice cu furnizorii de servicii**
- **Federalizare**
- **Asigurarea accesului federalizat la serviciile de eGuvernare utilizand solutiile deja implementate de furnizorii de servicii**
- **Provizionare**
- **Provizionarea identitatilor electronice ale consumatorilor in cadrul sistemelor tinta care furnizeaza servicii electronice;**
- **Provizionarea drepturilor de acces corespunzatoare serviciilor solicitate;**
- **Sincronizarea modificarilor asupra identitatilor electronice in sistemele tinta.**

Componentele software vor fi dezvoltate conform metodologiei Agile centrate in jurul ideii de dezvoltare iterativa, cerintele si solutiile fiind stabilite de comun acord intre Autoritatea Contractanta si Ofertantul declarat castigator. Dezvoltarile iterative, respectiv livrarile si acceptantele partiale (atat functionale, cat si non-functionale) pentru zona de dezvoltare software vor fi evidentiate in cadrul planului de proiect propus de catre ofertanti.

3.10.3. Serviciile de livrare si instalare hardware

Pentru livrarea si implementarea infrastructurii hardware solicitate vor trebui asigurate urmatoarele activitati:

- Livrarea echipamentelor necesare funcţionării soluţiei informatice
- Servicii de livrare, instalare si punere in functiune echipamente HW
- Respectarea graficului de livrare a echipamentelor ce urmează a fi recepţionate
- Derularea activitatilor corespunzatoare recepţiei cantitative a echipamentelor
- Livrarea documentaţiei tehnice a echipamentelor recepţionate

1. Realizarea Documentaţiei de instalare

Impreuna cu Beneficiarul se va agrea de comun acord formatul documentului si procedurile de etichetare a echipamentelor in cadrul unor discutii tehnico-procedurale preliminare.

Conform cerintelor initiale documentatia de instalare asociata site-ului va contine obligatoriu informatii privind:

- Numele şi codul locaţiei;
- Persoane de contact, atat din partea Beneficiarului, cat si din partea Furnizorului;
- Tipul şi codul echipamentelor ce vor fi instalate în site, conform cu propunerea tehnica detaliata anterior;
- Diagrama conexiunilor fizice între echipamente şi poziţia acestora în rack-ul/urile existent/e la beneficiar;
- Tabele cu informaţii privind conexiunile dintre echipamente (va conţine tipul de cablu folosit, etichetarea, ce echipamente conectează, etc.) ;
- Conexiunile acestora la prizele de electroalimentare în rack-ul/urile ofertat/e sau existent/e la beneficiar.

Procedurile de etichetare care vor fi elaborate de comun acord cu Beneficiarul si vor contine obligatoriu informatii privind:

- Procedura de etichetare fizică a echipamentelor hardware, a cablurilor de interconectare şi a cablurilor de electroalimentare;
- Proceduri de etichetare electronică la conectarea remote pe echipamente pentru adminstrare (prompt echipamente, banere de login, descriere interfete, etc), daca este cazul.

2. Instalarea echipamentelor în site.

Instalarea şi punerea în funcţiune a echipamentelor vor respecta cerinţele standardului EIA/TIA 568 folosind o echipa de specialisti certificati in instalarea si configurarea echipamentelor ofertate de catre producatorii acestor echipamente sau de catre centre de training autorizate de catre producator in acest sens.
Pentru fiecare site se vor efectua următoarele operaţii:

- Transportul echipamentelor de către Furnizor la sediul Beneficiarului în vederea instalării şi punerii în funcţiune, respectand normele de transport impuse de catre producator si de ambalare (in cazul in care echipamentele livrate nu sunt ambalate in ambalajul original);
- Instalarea fizică a fiecărui echipament în rack;
- Interconectarea echipamentelor (folosind cabluri UTP cat.5/6, Fibră optică etc.) furnizate de catre ofertant;
- Interconectarea noilor echipamente cu sistemul de comunicaţii existent, daca este cazul;
- Initializarea echipamentelor;
- Teste de interconectare pentru fiecare legătură;
- Refacerea conexiunilor eronate, in cazul in care unele teste de interconectare dau erori de comunicatie;
- Marcarea cu etichete a fiecărui echipament şi conexiune conform cu procedura de etichetare agreata.

3. Configurarea echipamentelor

Toate echipamentele vor fi configurate de către Furnizor conform soluţiei tehnice agreate cu Beneficiarul în urma workshop-urilor comune.

Planul de adresare IP pentru testarea echipamentelor instalate va fi pus la dispozitia Furnizorului de către Beneficiar, iar acesta din urmă va configura adresele IP de productie pe echipamentele respective, după efectuarea tuturor testelor de verificare.
Responsabilitatea Furnizorului se va rasfrange doar asupra echipamentelor livrate de acesta si va presupune activitati legate de integrarea acestor echipamente in sistemul informatic existent.
Toate echipamentele vor fi instalate si configurate în conformitate cu cerintele Beneficiarului, ce vor fi aduse la cunostinta Furnizorului si agreate de acesta in urma discutiilor tehnice preliminare.
Instalarea si configurarea sistemului informatic de virtualizare se va face conform cerintelor Beneficiarului stabilite in perioada de acceptanta.

3.10.4. Testarea si asigurarea calitatii sistemului

Este necesar ca Furnizorul să planifice în detaliu, să pregătească şi să efectueze o serie de teste care să confirme că sunt asigurate cerinţele funcţionale şi nonfuncţionale ale sistemului, compatibilitatea sistemului cu specificaţiile de interfaţare ale sistemului cu sistemele externe.
Testarea
Pentru nodul central, Beneficiarul se va asigura că Furnizorul a efectuat cu succes următoarele activităţi cu rezultatele lor respective:

- toate componentele software de bază necesar au fost livrate corespunzător şi instalate;
- toate elementele de nodul central sunt pe deplin functionale;
- aplicatia a fost livrată şi instalată;
- sistemul functionează fără incidente majore pentru o durată de 4 săptămâni;
- sesiunile de instruire au fost livrate;
- toate documentele necesare, manuale, kit-urile de instalare şi licenţele legate de acest proiect au fost livrate;
- testatrea proceselor interne: jurnalizare, arhivare, auditare, raportare ştergeri, managementul notificărilor;
- generarea de raportări statistice care vor fi identificate în procesul de implementarea sistemului.

Testele non-funcţionale trebuie să acopere cerinţele de disponibilitate, scalabilitate, fiabilitate, robusteţe, salvare şi restaurare, recuperarea în caz de dezastru, estimări capacitate şi planificare, performanţa, managementul configuraţiilor, extensibilitate/flexibilitate, siguranţă în funcţionare, securitate, managementul şi monitorizarea sistemului, managementul căderilor în sistem, contingenţa, operarea, conectivitatea şi calitatea serviciilor.
Planurile de testare trebuie să includă cel puţin următoarele elemente:

- descrierea componentei de sistem testat
- obiectivele de testare
- descrierea mediului de testare
- rezultatele aşteptate ale testului
- test de abordare
- datele de test
- descrierea procedurilor de test
- cazuri de testare
- instrumente folosite de testare
- persoanele responsabile
- cerinte de intrare / ieşire

Instrumente de testare

Furnizorul trebuie să precizeze toate instrumentele de testare (aplicaţii, scripturi, etc), destinate a fi utilizate în timpul procedurilor de testare. Furnizorul trebuie să furnizeze instrumentele de testare.
Toate rezultatele testelor trebuie înregistrate şi furnizate Beneficiarului după fiecare test.
Toate componentele HW/SW necesare testarii vor fi descrise de furnizor şi vor fi disponibile pentru toată perioada întregului contract (inclusiv pentru actualizari / testare pentru modificări).
Acelaşi mediu de testare se va utilizeaza pentru a testa toate modificările cerute de şi derivate din modificări legislative.
Mediul de testare nu trebuie să fie reutilizat sau integrat în alt mod în mediul de producţie.

Dezvoltarea şi punerea în aplicare de testare

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

Coordonarea testelor

Testele vor fi coordonate de catre Beneficiar/Utilizatori, care vor revizui şi aproba planul şi specificaţiile de testare înainte de execuţia efectivă a testelor, vor controla că mediul de testare e conform cu cerinţele, vor monitoriza efectuarea testelor şi se vor asigura de aplicarea procedurilor de management ale testării.

Asigurarea Calitatii

- Furnizorul trebuie să prezinte un plan pentru Asigurarea Calităţii acceptabil pentru Beneficiar, ca parte a planului de proiect. Acest plan trebuie sa includa, dar nu se limiteaza la, tipurile de testare folosite, atat manule, cat si automate (ex: unit testing, integration testing, UI testing etc), si la nivelul asumat de acoperire al testelor (minim 70% pentru unit testing).
- Activităţile furnizorului pentru asigurarea a calităţii vor fi asistate de către soluţia informatică integrată pentru managementul calităţii serviciilor
- Furnizorul trebuie să aloce timp suficient, în cadrul planului de proiect, pentru verificare şi validare în termeni de calitate, pentru serviciile prestate în cadrul contractului şi pentru livrabilele / documentele / rapoartele rezultate.
- Furnizorul va elabora procedurile standard de operare pentru toate aplicaţiile livrate, cu instructiuni detaliate pentru a ajuta angajaţii în procesele de lucru diferite.
- Furnizorul va pune la dispozitie manuale, documentatii, proceduri complete privind conceptia, implementarea si administrarea in integralitate a sistemului informatic.
- Furnizorul va prezenta, la nivelul fiecarei iteratii, progresul in baza planului de asigurare a calitatii.
- Furnizorul va oferi, pe durata proiectului, trimestrial, un raport intermediar de audit intern privind modul în care activităţile au avut loc în cursul perioadei de raportare, calitatea rezultatelor obţinute în cursul perioadei de raportare şi propunerile de acţiuni corective şi preventive menite să îmbunătăţească calitatea rezultatelor. Rapoartele trimestriale vor prezinta valorile măsurate pentru o serie de indicatori de performanţa

4. RESURSE

4.1. *PERSONAL ŞI INSTRUIRE*

4.1.1. Personal

Având în vedere complexitatea, dimensiunea şi importanţa acestui proiect, se consideră necesară solicitarea următoarele cerinţe minime obligatorii privind experienţa şi competentele personalului din cadrul **echipei de implementare a furnizorului**:

ECHIPA DE EXPERŢI:

EXPERT	Responsabilitati
Expert nr. 1 - Manager de Proiect – 1 persoana	• Activităţi specifice de management de proiect (legat de obiectul contractului) • Punct principal de contact în relaţia cu beneficiarul • Managementul proiectului în ansamblul sau, managementul ariei de cuprindere, managementul schimbărilor, planificarea generala a proiectului, managementul riscurilor, managementul problemelor, managementul comunicării • Asigurarea resurselor proiectului • Managementul, organizarea, alocarea şi planificarea echipei de proiect • Urmărirea respectării tuturor termenelor conform planului de proiect • Realizarea rapoartelor periodice/ad-hoc ale proiectului. • Elaborarea planurilor de calitate • Verificarea şi asigurarea calităţii livrabilelor
Expert nr. 2 - Arhitect sisteme informatice coordonator – 1 persoana	• Coordoneaza echipa tehnica formata din expertul arhitect sisteme informatice, expertii analisti de business, expertii dezvoltare software, expertul securitate cibernetica si expertul testare securitate • Asigura suport managerului de proiect pentru urmarirea respectarii termenelor din punct de vedere tehnic • Definirea soluţiilor detaliate pentru noile subsisteme • Definirea arhitecturii de integrare a componentelor sistemului • Activităţi de implementare, asistenta şi suport tehnic • Identificarea riscurilor şi problemelor tehnice şi a soluţiilor de rezolvare
Expert nr. 3 – Expert Identitate Electronica – 1 persoana	• Activităţi specifice de implementare si configurare a solutiilor de gestiune a identitailor electronice; • Configurarea din punct de vedere securitate a solutiilor de gestiune a identitatilor electronice;

	• Consultanta de specialitate pentru echipa de proiect pentru activitatile si etapele de integrare cu solutiile de gestiune si securitate a identitatilor electronice; • Asigurarea suportului tehnic in perioada de garantie; • Instructaj pentru administratorii sistemului informatic şi pentru utilizatorii sistemului informatic
Expert nr. 4 – Expert securitate cibernetica – 1 persoana	• Realizarea soluției de securitate în etapa de analiza; • Configurarea din punct de vedere al securității a sistemelor informatice; • Consultanta de specialitate pentru echipa de proiect în timpul derulării proiectului; • Realizarea planului de securitate a sistemului informatic; • Instructaj pentru administratorii sistemului informatic şi pentru utilizatorii sistemului informatic;
Expert nr. 5 – Expert testare securitate – 1 persoana	• Consultanta de specialitate pentru echipa de proiect în timpul derulării proiectului; • Verificarea planului de securitate a sistemului informatic; • Realizarea de teste de penetrare pentru verificarea securitatii sistemului informatic; • Instructaj pentru administratorii sistemului informatic şi pentru utilizatorii sistemului informatic;
Expert nr. 6 - Analist de business – 2 persoane	• Analiza cerințelor de business • Realizarea documentelor de specificații funcționale şi a scenariilor de testare • Activități de implementare, asistenta şi suport tehnic • Suport acordat utilizatorilor cheie pentru testarea de acceptanță a sistemului
Expert nr. 7 - Arhitect sisteme informatice – 1 persoana	• Definirea soluțiilor detaliate pentru noile subsisteme • Definirea arhitecturii de integrare a componentelor sistemului • Activități de implementare, asistenta şi suport tehnic • Identificarea riscurilor şi problemelor tehnice şi a soluțiilor de rezolvare
Expert nr. 8 – Expert dezvoltare aplicatii software – 5 persoane	• Activități specifice de dezvoltare de aplicații software, pe baza documentelor de analiza, specificații funcționale, specificații tehnice, arhitectura sistem • Testare unitara (interna) • Suport în activitățile de implementare • Rezolvare disfuncționalități software (bug-uri) • Asigurare suport tehnic în perioada de garanție • Crearea/ actualizarea documentațiilor
Expert nr. 9 – Expert Management organizational – 1 persoana	• Activitati specifice de analiza si implementare procese de business in cadrul sistemului informatic; • Activitati specifice de optimizare a proceselor de

	business in perioada de analiza a specificatiilor functionale; • Colaboreaza cu expertul analist de business pentru definirea si implementarea corecta a fluxurilor de business; • Instructaj pentru administratorii sistemului informatic si pentru utilizatorii sistemului informatic din punct de vedere al definirii de noi fluxuri de business sau pentru modificarea celor existente
Expert nr.10 – Expert Data Center - 1 persoana	• Activităţi specifice de amenajare/ instalare a centrelor de date • Consultanta de specialitate pentru echipa de proiect în timpul derulării proiectului • Testarea echipamentelor de protecţie specifice centrului de date • Realizarea documentelor specifice centrului de date, inclusiv pentru operaţiile de întreţinere si mentenanţă • Instructaj pentru responsabilii centrului de date

1. Expert nr. 1: Manager de Proiect – 1 persoana

Cerinţe minime şi obligatorii:

- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţa generală: minim 5 ani experienţă generală;
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect similar (implementare sistem informatic integrat) la nivelul căruia să fi deţinut poziţia de manager de proiect;
- Deţinerea de cunoştinţe în domeniul managementului de proiecte dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel naţional/ internaţional.

2. Expert nr. 2: Arhitect sisteme informatice coordonator – 1 persoana

Cerinţe minime şi obligatorii:

- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţă generală: minim 5 ani experienţă generală;
- Experienţa specifica demonstrata prin participarea în cel puţin un proiect/contract, pe o poziţie similară la nivelul căruia să fi desfăşurat activităţi similare cu responsabilităţile din acest contract;
- Deţinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international în domeniul arhitecturii de sisteme enterprise;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind managementul serviciilor IT si alinierea acestora cu nevoile de business;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind framework-ul de business care adreseaza guvernanta si managementul IT;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international in domeniul securitatii sistemelor IT.

3. Expert nr. 3: Expert Identitate Electronica - 1 persoana

Cerințe minime și obligatorii:

- Studii superioare finalizate cu diploma de licență sau echivalent;
- Experiență generală: minim 5 ani experiență generală;
- Experiență specifică demonstrată prin participarea în cel puțin un proiect/contract, pe o poziție similară la nivelul căruia sa fi desfășurat activități similare cu responsabilitățile din acest contract;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind managementul serviciilor IT si alinierea acestora cu nevoile de business;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international pentru administrarea componentei de administrare unitara a conturilor de utilizator pentru solutia ofertata;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international pentru administrarea componentei de control al accesului la componentele de aplicatii web si portal si Single Sign On pentru solutia ofertata.

4. Expert nr. 4: Expert Securitate Cibernetica – 1 persoana

Cerințe minime și obligatorii:

- Studii superioare finalizate cu diploma de licență sau echivalent;
- Experiență generală: minim 5 ani experiență generală;
- Experiența specifica demonstrata prin participarea în cel puțin un proiect/contract, pe o poziție similară la nivelul căruia să fi desfășurat activități similare cu responsabilitățile din acest contract;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind implementarea componentei de securizare a accesului privilegiat pentru echipamentele de tip comunicatii si servere;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind gestiunea incidentelor de securitate prin intelegerea mecanismelor de atac, precum si privind contracararea atacurilor cibernetice;
- Detinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind protejarea activa a sistemelor informatice si a retelelor si verificarea sistemelor informatice impotriva vulnerabilitatilor.

5. Expert nr. 5: Expert testare securitate - 1 persoana

Cerințe minime și obligatorii:

- Studii superioare finalizate cu diploma de licență sau echivalent;
- Experiență generală: minim 5 ani experiență generală;
- Experiență specifică demonstrată prin participarea în cel puțin un proiect/contract, la nivelul căruia să fi desfășurat activități de management organizațional;
- Detinerea de cunostinte privind testarea de penetrare a sistemelor informatice din punct de vedere al securitatii informatiei, dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international care probeaza in mod concludent indeplinirea cerintei si obtinute in urma promovarii unui examen practic ce a presupus:
  - Tehnici de colectare a datelor in scopul identificarii sistemului vulnerabil;
  - Teste de penetrare cu ajutorul script-urilor sau instrumente specializate;

- Analiza, corectarea si modificarea codului malitios in scopul simularii atacului informatic;
- Tehnici de evitare a protectiei de tip firewall

- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international privind identificarea vulnerabilitatilor existente si contracararea atacurilor cibernetice prin modificarea codului malitios si pivotarea retelei in vederea exfiltrarii datelor.

6. **Expert nr. 6: Analist de Business – 2 persoane**
- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţă generală: minim 5 ani experienţă generală;
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect/contract, pe o poziţie similară la nivelul căruia să fi desfăşurat activităţi similare cu responsabilităţile din acest contract
- Deţinerea de cunoştinţe în domeniul analizei de business dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel naţional/internaţional;

7. **Expert nr. 7: Arhitect Sisteme Informatice – 1 persoana**

Cerinţe minime şi obligatorii:
- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţă generală: minim 5 ani experienţă generală;
- Experienţa specifica demonstrata prin participarea în cel puţin un proiect/contract, pe o poziţie similară la nivelul căruia să fi desfăşurat activităţi similare cu responsabilităţile din acest contract;
- Deţinerea de cunostinte dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international în domeniul arhitecturii de sisteme enterprise;

8. **Expert nr. 8: Dezvoltator aplicatii software – 5 persoane**

Cerinţe minime şi obligatorii:
- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţă generală: minim 5 ani experienţă generală;
- Experienţa specifica demonstrata prin participarea în cel puţin un proiect/contract, pe o poziţie similară la nivelul căruia să fi desfăşurat activităţi similare cu responsabilităţile din acest contract;
- Deţinerea de competenţe privind dezvoltarea de software dovedite prin certificare în domeniu recunoscută la nivel naţional sau internaţional;

9. **Expert nr. 9: Expert management organizaţional - 1 persoana**

Cerinţe minime şi obligatorii:
- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţă generală: minim 5 ani experienţă generală;
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect/contract, la nivelul căruia să fi desfăşurat activităţi de management organizaţional;
- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international in domeniul managementului de proiecte;
- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international in management prin obiective;

- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international in rezolvarea problemelor.

10. Expert nr. 10: Expert Data Center - 1 persoana

Cerinţe minime şi obligatorii:

- Studii superioare finalizate cu diploma de licenţă sau echivalent;
- Experienţă generală: minim 5 ani experienţă generală;
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect/contract, la nivelul căruia să fi desfăşurat activităţi de amenajare, instalare si operare centru de date;
- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international in specialitatea ATD (Accredited Tier Designer) in domeniul amenajarii/instalarii centrelor de date;
- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome / certificari recunoscute la nivel national / international in domeniul instalarii rack-urilor IT, obtinuta in urma promovarii unui examen practic.

Ofertanţii trebuie să prezinte în oferta tehnică, pentru fiecare expert solicitat următoarele informaţii/documente:

• numele persoanei propuse pentru fiecare poziţie (de exemplu pentru dezvoltator software sunt cerute minim 5 poziţii şi pentru fiecare dintre acestea trebuie nominalizată câte o persoana);

• declaraţia de disponibilitate semnata de persoana propusa (în cazul în care aceasta nu este angajat al Prestatorului);

• Curriculum Vitae (CV), aferent fiecărei persoane propuse în cadrul echipei, semnat de către fiecare titular în parte şi datat;

• Copiile documentelor justificative relevante care demonstrează îndeplinirea cerinţelor referitoare la studiile, expertiza şi experienţa specifică relevantă solicitată şi prezentată în CV, cum ar fi:

o Diplome de studii, certificări, alte diplome relevante;

o Recomandări sau alte documente edificatoare din care să reiasă activităţile desfăşurate şi care să evidenţieze experienţa profesională specifică similară.

Copiile documentelor trebuie să fie confirmate pentru conformitate cu originalul documentelor respective. Certificatele/ diplomele/ documentele justificative emise în alta limba decât limba română vor fi prezentate în limba de origine, însoţite de traducerea autorizată în limba română.

Autoritatea Contractantă are dreptul de a verifica exactitatea informaţiilor şi a dovezilor furnizate de ofertanţi şi de a solicită şi alte documente/ informaţii care să clarifice experienţa similara respectivă.

În urma verificării exactităţii informaţiilor şi a dovezilor furnizate de către ofertanţi, Autoritatea Contractantă poate solicita şi alte documente/informaţii care să clarifice experienţa profesionala solicitată. De asemenea, Autoritatea Contractantă îşi rezervă dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experienţa profesională, în vederea confirmării celor prezentate de către ofertanţi.

Pentru persoanele propuse care au calitatea de salariaţi ai ofertantului, se va prezenta în mod obligatoriu orice document prin care să se demonstreze relaţia contractuală dintre persoanele nominalizate şi ofertant (extras Revisal/ contract de muncă, etc.). În cazul în care se propune personal care nu este salariat al Prestatorului, fiecare astfel de personal va completa şi va semna o declaraţie de disponibilitate semnată de titular, cu referire strictă la obiectul contractului ce face obiectul prezentei proceduri.

Pe parcursul derulării contactului de achiziție publică, modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează conform prevederilor art. 162 din Anexa 1 (Normele metodologice) la HG nr. 395/2016.
Astfel, înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează numai cu acceptul autorității contractante, și nu reprezintă o modificare substanțială, așa cum este aceasta definită în art. 221 din Lege, decât în următoarele situații:
a) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin criteriile de calificare/selecție prevăzute în cadrul documentației de atribuire;
b) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu obține cel puțin același punctaj ca personalul propus la momentul aplicării factorilor de evaluare.
În situațiile prevăzute anterior, contractantul are obligația de a transmite pentru noul personal documentele solicitate prin documentația de atribuire fie în vederea demonstrării îndeplinirii criteriilor de calificare/selecție stabilite, fie în vederea calculării punctajului aferent factorilor de evaluare.

4.1.2. Instruire utilizatori

În cadrul proiectului se va asigura instruirea diferențiată a următoarelor categorii de beneficiari in vederea operationalizarii sistemului la parametrii proiectati, astfel:

- administratorii și personalul de întreținere a sistemului informatic. Pentru această categorie proiectul va asigura instruirea a **5 persoane de la ADR**;
- personalul ADR, cu accent pe modalitățile de răspuns la solicitările și sesizările furnizorilor, precum și pe valorificarea potențialului datelor colectate. De asemenea, personalul ADR va fi instruit privind modificările și suplimentărilor de funcționalități determinate de implementarea sistemului propus. O echipa desemnată de ADR va fi instruită de furnizorul soluției informatice pentru asigurarea Nivelului 1 de suport pentru utilizatorii sistemului propus (15 utilizatori).
    - cursul va avea o durată de minim 10 zile lucratoare (8 ore /zi)
    - cursul va fi dimensionat pentru **10 utilizatori**
    - cursul va fi susținut în limba română. mai a
    - curicula va acoperi toate aspectele necesare utilizării în bune condiții a sistemului.

Prin instruire se va asigura realizarea cel puțin a următoarelor obiective:

- cunoașterea sistemului integrat în ansamblul său;
- învățarea modului de operare a funcționalităților sistemului propus;
- învățarea modului de rezolvare a problemelor curente de folosire a componentelor sistemului;
- înțelegerea implicațiilor sistemului propus și a avantajelor acestuia.

Sesiunile de instruire vor fi realizate de furnizorul soluției informatice. De asemenea, furnizorul soluției informatice va elabora și pune la dispoziția beneficiarului manuale de utilizare și suport de curs în limba română, pentru toate categoriile de utilizatori ai sistemului.
La terminarea cursului, cursanții din categoriile administrator de sistem și personal ADR vor primi de la furnizor certificate de instruire individuale. Certificarea se va face diferențiat pentru cele două categorii.
Toate categoriile de utilizatori vor beneficia doar de materiale de prezentare și de instruire individuală (*self-trainig*).

Furnizorul soluţiei va face instruirea utilizatorilor sistemului prin livrarea de documentaţie şi organizarea de cursuri de instruire la nivelul ADR.
Instruirea utilizatorilor sistemului se va efectua la finalizarea implementării proiectului pe baza manualelor/ghidurilor de utilizare în limba română, care vor fi disponibile în format fizic şi electronic. Se vor realiza ghiduri distincte în funcţie de tipurile de utilizatori ai sistemului. Aceste materiale vor fi puse la dispoziţia beneficiarului înainte de punerea în producţie a sistemului informatic propus.
Furnizorul soluţiei informatice va pune la dispoziţia Beneficiarului un Ghid de operare pentru persoanele care vor administra şi opera sistemul, în format fizic şi electronic.
Pentru desfăşurarea în bune condiţii a activităţii necesare utilizării sistemului este foarte important ca personalul care va opera sistemul să fie instruit corespunzător. Furnizorul trebuie să organizeze sesiuni de instruire şi să realizeze activităţi de instruire a personalului ce va utiliza noul sistem în vederea familiarizării corespunzătoare cu elementele de noutate ale aplicaţiei şi cu modul de operare a acesteia.
Se solicita servicii de instruire pe următoarele categorii de administratori:

- **Administratori infrastructura software** – cursuri specifice infrastructurii software ofertata.
  - cursul va avea o durată de minim 5 zile lucratoare (8 ore /zi)
  - cursul va fi dimensionat pentru **10 utilizatori**
  - cursul va fi susţinut în limba română.
  - curicula va acoperi toate aspectele necesare utilizării în bune condiţii a sistemului.
- **Administratori sistem integrat** – cursuri specifice solutiei integrate oferite.
  - cursul va avea o durată de minim 5 zile lucratoare (8 ore /zi)
  - cursul va fi dimensionat pentru **10 utilizatori**
  - cursul va fi susţinut în limba română.
  - curicula va acoperi toate aspectele necesare utilizării în bune condiţii a sistemului.
- **Administratori securitate sistem** - cursuri specifice de cybersecurity
  - cursul va avea o durată de minim 5 zile lucratoare (8 ore /zi)
  - cursul va fi dimensionat pentru **10 utilizatori**
  - cursul va fi susţinut în limba română.
  - curicula va acoperi toate aspectele de securitate cibernetica a sistemului informatic
  - după încheierea cursului participanţii vor beneficia de un stagiu de pregătire aplicat în centrul de tip SOC în care se vor realiza activităţile descrise la capitolul Servicii dedicate asigurarii securitatii cibernetice a sistemului informatic. Stagiul de pregătire va avea o durată minimă de 5 zile, va fi realizat împreună cu instructorul cursului şi va fi de tipul hands-on.

Furnizorul va asigura toate resursele necesare desfăşurarii serviciilor de instruire, va elabora şi susţine cursurile si va tipări materiale de curs pentru toţi participanţii.
Toate cursurile in format electronic – insotite de documente suport – vor fi publicate in solutia de knowledge management (KM) inclusiv pentru Operatorii de date.

Soluţie software de knowledge management
Această soluţie trebuie să permită următoarele:

- Definirea drepturilor de acces diferenţiate; politica legată de drepturile de acces va fi furnizată de către Autoritatea Contractantă;
- Introducerea tuturor documentelor elaborate / generate pe parcursul contractului, în formate digitale vizuale;

- Accesarea de pe dispozitive mobile;
- Facilități de căutare;
- Organizarea conținutului pe categorii; categoriile vor fi sincronizate cu politica de acces;
- Accesul în aplicație via web;
- Solutia va fi disponibila tuturor tipurilor de utilizatori;
- Emiterea de notificări către utilizatorii cu drepturi de acces pe fiecare categorie de conținut definită.

Solutie pentru documentare procese si generare continut instruire pentru aplicatiile software dezvoltate in cadrul proiectului.

Scopul si cerintele generale ale aplicatiei:

- Scaderea timpului necesar pentru documentarea proceselor si a instruirii;
- Cresterea calitatii operatiilor efectuate de utilizatorii finali ai sistemului integrat;
- Scaderea riscului implementarii in fiecare faza a ciclului de implementare a solutiei;
- Maximizarea investitiei in sistemul integrat;
- Suport pentru procesele de documentare.

Solutia trebuie sa asigure minim urmatoarele functionalitati:

- Documentarea si generarea continutului de instruire: sa produca automat materialele de instruire si documentele aferente procesului de implementare (manualul utilizatorului, documente de test) si manualul de ajutor al utilizatorului;
- Generarea de continut de instruire a utilizatorilor sistemului integrat pentru fiecare tranzactie sau functionalitate;
- Continutul generat va trebui sa poata fi incarcat intr-un sistem de instruire de tip e-learning si sa fie conform cu standardele de industrie, minim SCORM 1.2;
- Inregistrarea de capturi de ecran pe baza carora sa se poata adauga comentarii si sa permita publicarea a diferite documente: manualul instructorului, manual pentru utilizator, scenarii de testare;
- Suport utilizatorilor sistemului pentru fiecare tranzactie sau functionalitate pentru care s-a definit continut anterior, punand la dispozitia acestora mai multe moduri de accesare a continutului;
- Accesarea continutul ajutorului (Help) fara a parasi tranzactia in curs de efectuare;
- Editarea ulterioara a continutului, avand incorporate instrumente de editare fara a modifica componentele sistemului;
- Suport utilizatorilor sistemului pentru a trece pas cu pas printr-un proces sau procedura in aplicatie;
- Urmarirea progresului utilizatorilor in cadrul materialelor oferite web-based;
- Accesul simultan al mai multor utilizatori concurenti peste o retea de tip WAN;
- Inregistrarea, stocarea, modificarea si accesarea documentelor intr-o singura baza de date sursa;
- Integrarea de documente din alte surse (voce, film, ppt, html, pdf, etc.);
- Sa sustina procese complexe (de ex. cai de lucru alter in cadrul unui anumit flux de lucru);
- Sa suporte managementul structurat al continutului;
- Sa suporte versionarea continutului;
- Sa aiba capabilitatea de recunoastere a obiectelor (recunoasterea automata a obiectelor, butoanelor, campurilor, textelor sistemului integrat);

- Sa permita crearea automata de pachete de documentatie si materiale de instruire bazate pe roluri, care sa poata fii publicate si transferate catre alti utilizatori doar cu acordarea permisiunii.

Aplicatia trebuie sa raspunda minim urmatoarele cerinte tehnologice:
- Sa suporte multiple browsere de Internet (ex: Mozilla Firefox, Safari);
- Sa suporte documente Microsoft Office (word, excel, powerpoint) si Adobe PDF;
- Sa permita integrarea cu meniul de Ajutor al sistemului integrat (bazat pe text sau bazat pe simularile proceselor);
- Simularile proceselor sa poata fi publicate in diferite moduri (internet, LMCSI, document).

Ghidul de operare va cuprinde cel puţin:
- procedurile de administrare şi operare a sistemului: administrarea utilizatorilor, salvarea şi restaurarea datelor, optimizarea timpului de răspuns şi a perioadelor de maximă încărcare a cererilor de la utilizatori
- opţiunile şi procedurile de configurare a sistemului propus
- descrierea completă a arhitecturii cuprinzând:
  - componentele hardware, caracteristicile şi configuraţia principala a acestora
  - componentele software, versiunile, configuraţiile şi maparea componentelor software pe componente hardware
  - configurarea securităţii şi descrierea arhitecturii de securitate a soluţiei
- Instruirea personalului care va utiliza/administra sistemul propus va fi realizată în cadrul a două categorii de cursuri specifice organizate, în funcţie de tipul de utilizatori şi se va face pe modelul de tipul "train the trainers" astfel încât să poată instrui un număr corespunzător de reprezentanţi.
- Limba folosită în activităţile de instruire este limba româna.

La sfârşitul fiecărei sesiuni de instruire se vor elabora documentele:
- Prezenţa la curs
- Raport de şcolarizare realizat de către instructor
- Evaluare curs (se va completa de către cursanţi)

4.2. *RESURSE MATERIALE*

În calitate de solicitant al investiţiei ADR înţelege că pentru bunul mers al proiectului ce face obiectul investiţiei trebuie să pună la dispoziţie toate resursele necesare îndeplinirii cu succes a proiectului.
Întregul proiect se va realiza şi implementa la sediul ADR sau într-o locaţie desemnată de ADR.
În acelaşi timp, beneficiarul va pune la dispoziţie pentru buna desfăşurare a fazelor proiectului, dar şi pentru exploatarea curentă a acestuia după implementare, dotări şi resurse materiale existente.

Dintre aceste resurse disponibile, enumeram:

Instituţia	**Adresa de implementare**	**Resurse materiale puse la dispoziţie de către instituţie**
ADR	Sediul ADR sau locaţia desemnată de ADR	• Sediul propriu • Calculatoarele personalului tehnic implicat, împreună cu echipamentele periferice alocate fiecărui calculator în parte (imprimante, scanere, etc.) • Dotările permanente ale ADR – mobilier, linii de comunicaţii, etc.

4.3. *GRAFICUL DE IMPLEMENTARE*

Nr. crt.	Activitati\Luna	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2	**Achiziție implementare sistem informatic**																																				
2.1	Pregatirea documentatiei de atribuire																																				
2.2	Derulare procedura de achiziție																																				
2.3	Notificare castigator si semnarea contractului																																				
3	**Implementare sistem informatic**																																				
3.1	Analiza necesitatilor																																				
3.2	Proiectarea solutiei informatice																																				
3.3	Servicii de livrare, instalare si punere in functiune infrastructura hardware si software																																				
3.4	Dezvoltarea, configurarea si instalarea aplicatiei informatice																																				
3.5	Testarea aplicatiei și operaționalizarea sistemului IT																																				
4	**Instruire utilizatori**																																				

5. GARANȚIE SI SUPORT TEHNIC

Pentru toate echipamentele şi pentru produsele software de bază se va acorda suport tehnic până la finalizarea implementării proiectului, conform contractului încheiat de instituţia beneficiară cu furnizorul soluţiei informatice.
Pentru întregul sistem integrat se va acorda o garanţie de 3 ani. Prin garanţie în acest context se înţelege asigurarea funcţionalităţilor existente la data finalizării implementării sistemului informatic.
Pentru componentele licenţiate ale software-ului de aplicaţii se va asigura suport tehnic pe perioada garanţiei de 3 ani, începând cu data livrării sistemului informatic final.
Intervenţiile vor fi realizate cu tehnicieni autorizaţi de producator.
Costurile de depanare defecte aplicative şi realizare de versiuni noi ale aplicaţiilor informatice vor face obiectul unui contract de service şi suport tehnic.
Pe întreaga perioadă de garanţie furnizorul soluţiei informatice va asigura obligativitatea funcţionării sistemului în perioada de post-implementare, va presta servicii de suport pentru toate sistemele software furnizate, iar această activitate va fi monitorizată de către Responsabilul de proiect.
Activităţile de mentenanţă şi suport din aceasta perioadă vor realiza prevenirea şi remedierea defecţiunilor şi anomaliilor apărute la produsele software din cadrul soluţiei informatice.
Serviciul de suport tehnic va avea scopul de a oferi utilizatorilor finali un Punct Unic de Contact pentru toate solicitările de intervenţii asupra componentelor software, pentru suport operativ şi pentru semnalările unor funcţionari defectuoase a soluţiei furnizate.
Remedierea defecţiunilor pe perioada garanţiei se va face la sediul beneficiarului proiectului sau prin intervenţie de la distanţă (*remote maintenance*), iar în cazul unor defecte mai grave, echipamentele se vor transporta la sediul furnizorului de către acesta.
Fiecare intervenţie în perioada de garanţie va fi documentată cu ajutorul unei fişe de intervenţie care va conţine următoarele detalii: data intervenţiei, descrierea intervenţiei, modalitatea de rezolvare a intervenţiei (reparaţie/înlocuire), durata de intervenţie şi confirmarea recepţiei prin semnăturile furnizorului şi beneficiarului.
Controlul intervenţiilor
Pentru înregistrarea tuturor tipurilor de intervenţii (preventive, corective, actualizări etc) si pentru asigurarea bunei funcţionări a produselor ofertate, se va propune daca este cazul, un model de registru pentru controlul intervenţiilor, care va fi validat de comun acord in urma workshop-urilor comune avute cu beneficiarul. Beneficiarul va actualiza acest registru cu toate informaţiile care descriu intervenţiile respective.

Prin garanţie se va asigura faptul că produsele sunt conforme cu specificaţiile tehnice, fără costuri suplimentare, pe toată durata garanţiei.
Ofertantul va da o declaraţie scrisă din care să rezulte garantarea produselor furnizate în conformitate cu cerinţa stabilită.
Ofertantul va da o declaraţie scrisă prin care să ateste că piesele de schimb, inclusiv bateriile reîncărcabile, dacă este cazul, vor fi puse la dispoziţia autorităţii/entităţii contractante de catre el sau printr-un prestator de servicii şi că acestea (piesele de schimb) sunt conforme cu standardele europene.

Disponibilitatea sistemului trebuie sa fie garantata de catre ofertanti la un nivel de minim 99,95% pentru intreaga perioada de garantie.

Timpii de rezolvare sunt definiţi mai jos în funcţie de gravitatea incidentului apărut:

Nivel Criticitate	Timp de răspuns	Timp soluționare temporară	Timp soluționare finală
Critic	1 oră	6 ore	12 ore
Mediu	6 ore	12 ore	36 ore
Minor	12 ore	36	72 ore

Tipurile incidentelor:

1. **Critic**: una sau mai multe resurse din mediul productiv sunt nefuncţionale sau profund degradate, iar impactul acestui incident duce la imposibilitatea utilizării sistemului.
2. **Mediu**: impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanţei sau afectarea parţială a unor funcţionalităţi ale sistemului. Sistemul este funcţional pentru cea mai mare parte a scenariilor de utilizare.
3. **Minor**: impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluţie temporară.

6. MODALITATEA DE ELABORARE A OFERTELOR

În cadrul ofertei tehnice, Ofertantul va prezenta:

6.1. *METODOLOGIA ŞI PLANUL DE LUCRU*

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

a) metodologia pentru realizarea serviciilor;
b) planul de lucru pentru realizarea serviciilor;
c) personalul utilizat pentru realizarea serviciilor şi organizarea acestuia.

6.1.1. Metodologia

În această secţiune trebuie să prezentaţi modul în care dumneavoastră, în calitate de ofertant, înţelegeţi:

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

Cel puţin următoarele informaţii trebuie prezentate aici:

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

- descrierea soluţiei propriu-zise propuse pentru îndeplinirea obiectivelor stabilite prin caietul de sarcini.

6.1.2. Planul de lucru

Cel puţin următoarele informaţii trebuie prezentate aici:
- denumirea şi durata activităţilor şi pachetelor de activităţi din cadrul contractului, aşa cum sunt acestea prezentate la capitolul "Metodologie";
- succesiunea şi interrelaţionarea acestor activităţi;
- punctele-cheie de control - "jaloanele" proiectului.

Planul de lucru propus trebuie să fie:
1. conform cu abordarea şi metodologia propusă;
2. să demonstreze:

- înţelegerea prevederilor din caietul de sarcini;
- abilitatea de a transpune prevederile într-un plan de lucru fezabil;
- încadrarea activităţilor în timp de aşa manieră încât să se asigure finalizarea serviciilor în termenul specificat în caietul de sarcini;

3. realizat utilizând un software de planificare a timpului.

6.1.3. Organizarea şi personalul

Cel puţin următoarele informaţii trebuie prezentate aici:
- structura echipei propuse pentru managementul contractului;
- modul de abordare a activităţii de raportare cu privire la progresul serviciilor, inclusiv documentele finale în raport cu prevederile caietului de sarcini;
- descrierea infrastructurii pe care contractorul o utilizează pentru realizarea activităţilor propuse pentru îndeplinirea obiectului contractului. Această infrastructură trebuie să fie corespunzătoare scopului contractului şi să îndeplinească toate cerinţele solicitate de legislaţia în vigoare.

Se va prezenta doar echipamentul necesar şi propus pentru desfăşurarea contractului şi nu tot echipamentul deţinut de către ofertant.

Descriere (tip / provenienta / model)	Caracteristici	Nr. de unitati	Vechime (ani)	Autorizatii, agremente, licente etc., cf. legislatiei in vigoare	Localizarea echipamentului (adresa)	Momentul din executarea serviciilor in care se utilizeaza

Ofertantul va prezenta informaţii referitoare la momentele din derularea serviciilor când va intenţiona să utilizeze aceste echipamente şi va justifica propunerea sa ţinând cont de echipamentele necesare pentru realizarea corespunzătoare a serviciilor şi obţinerea rezultatelor dorite.

- modul de abordare a activităţii de identificare a riscurilor ce pot apărea pe parcursul derulării contractului şi măsuri de diminuare a riscurilor în raport cu prevederile caietului de sarcini;
- modul de abordare a activităţii de prevenire/atenuare/eliminare sau minimizare a efectelor, dupăcaz, a riscurilor identificate în caietul de sarcini;
- modul de abordare a activităţilor corespunzătoare îndeplinirii cerinţelor privind sănătatea şi securitatea în muncă, inclusiv modul în care ofertantul devenit contractor se va asigura că pe parcursul executării contractului obligaţiile legale referitoare la condiţiile de muncă şi protecţia muncii sunt respectate (dacă este cazul);
- modul de abordare şi gestionare a relaţiei cu subcontractorii, în raport cu activităţile subcontractate (dacă este cazul);
- evaluarea utilizării resurselor în termeni om-zile de lucru, deplasările personalului şi utilizarea echipamentelor alocate tuturor organizaţiilor (inclusiv autoritatea/entitatea contractantă) implicate în realizarea contractului.

6.2. *TABELUL DE CORESPONDENȚĂ*

Ofertantul va elabora un tabel de corespondență – in format editabil, în cadrul căruia va preciza în ce capitole ale ofertei tehnice sunt descrise punctual cerințele din Caietul de Sarcini, ținând cont de structura capitolelor celui din urmă.
Ofertantul va prezenta răspunsuri detaliate la toate cerințele Caietului de Sarcini prin care să arate modul concret în care acesta va realiza toate activitățile solicitate prin Caietul de Sarcini. Oferta tehnică va fi elaborată cu respectarea structurii Caietului de Sarcini. Ofertele care se vor limita la a confirma faptul că se vor presta toate activitățile solicitate, fără să prezinte concret modul în care vor realiza acest lucru, vor fi considerate neconforme.
Lipsa din ofertă a oricăror informații dintre cele solicitate anterior în acest capitol sau prezentarea unor descrieri nerelevante sau care nu demonstrează înțelegerea proiectului va conduce la declararea ofertei ca fiind neconformă și, implicit, la descalificarea Ofertantului.

6.3. *PROTECȚIA MUNCII*

În baza prevederilor art.51 alin.2) din Legea nr.98/2016, Ofertantii sunt obligati sa indice in cadrul ofertei faptul ca la elaborarea acesteia au tinut cont de obligatiile referitoare la conditiile de munca si protectia muncii.
Informatii privind reglementarile in vigoare la nivel national in acest domeniu se pot obtine de la Inspectia Muncii sau de pe site-ul http://www.inspectmun.ro/Legislatie/legislatie.html http://www.inspectmun.ro/site/Legislatie/legislatie.html
Conform prevederilor art.37 alin.2) lit.d) din H.G. nr.395/2016 in cazul in care nu se asigura respectarea reglementarilor obligatorii referitoare la conditiile specifice de munca si de protectie a muncii, Oferta va fi considerata inacceptabila.

7. MANAGEMENTUL CONTRACTULUI

7.1. *ASPECTE ORGANIZATORICE*

Autoritatea contractantă

ADR va indeplini rolul de Autoritate contractanta in prezenta procedura de achizitie publica si va fi responsabil cu organizarea acestei proceduri. Totodata, **ADR** indeplineste si rolul de Beneficiar al serviciilor ce urmeaza a fi contractate.
Managementul Contractului, inclusiv implementarea administrativa şi procedurala aferente Contractului, va fi asigurat de catre o echipa de implementare din partea **ADR** (Echipa de implementare a Proiectului), care va gestiona totodata si documentele elaborate de furnizor (analize, rapoarte de progres, rapoarte, facturi, alte documente justificative etc.).

Autoritatea Contractantă este responsabilă pentru:
a. punerea la dispoziţia Contractantului a tuturor informaţiilor disponibile pentru obţinerea rezultatelor aşteptate, cum ar fi: date de intrare, raportări, situaţii specifice;
b. punerea la dispoziţia Contractantului, dacă este cazul, a unui spaţiu de lucru mobilat;
c. desemnarea echipei implicate şi responsabile cu interacţiunea şi suportul oferit Contractantului;
d. asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului.

Atribuţiile şi responsabilităţile **ADR**:
- Implementarea soluţiei informatice:
  - Analiza necesităţilor;
  - Proiectarea soluţiei informatice;
  - Servicii de livrare, instalare şi punere în funcţiune echipamente HW şi licenţe software;
  - Dezvoltarea aplicaţiei informatice;
  - Testarea aplicaţiei;
  - Pilotare la nivel naţional;
- Instruirea echipei de proiect.

Furnizorul

Furnizorul serviciilor este responsabil pentru executia conforma si la timp a tuturor activitatilor si pentru furnizarea livrabilelor prevazute in prezentul Caiet de sarcini, corespunzatoare Proiectului.
Furnizorul va raspunde intocmai tuturor cerintelor prevazute in prezentul Caiet de sarcini, respectand si aplicand cele mai bune practici in domeniu.
Furnizorul este direct si integral responsabil pentru activitatea expertilor săi si pentru indeplinirea scopului Contractului si obtinerea rezultatelor Proiectului.

Contractantul este pe deplin responsabil pentru:
a. asigurarea planificării resurselor în raport cu graficul estimat pentru derularea contractului şi prezentat în cadrul acestui document;

b. îndeplinirea obligațiilor sale, cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale relevante precum și cu deplina înțelegere a complexității legate de derularea cu succes a Contractului, astfel încât să se asigure îndeplinirea obiectivelor stabilite, inclusiv prin furnizarea – prin intermediul Planului de management al calității – a asigurării că activitățile și rezultatele sunt realizate la parametrii calitativi solicitați;
c. asigurarea valabilității tuturor autorizațiilor și certificatelor (atât pentru organizația sa, cât și pentru personalul/echipamentul propus pentru realizarea serviciilor), care sunt necesare (conform legislației în vigoare) pentru prestarea serviciilor;
d. asigurarea unui anumit grad de flexibilitate în prestarea serviciilor în funcție de necesitățile obiective ale Autorității Contractante la orice moment în derularea contractului (acest grad de flexibilitate trebuie definit în Caietul de Sarcini și în nici un caz nu trebuie definit astfel încât să poată fi asociat unei modificări la Contract;
e. prestarea serviciilor în conformitate cu cerințele Caietului de Sarcini;
f. prezentarea rezultatelor în formatul/formatele care să respecte cerințele Autorității Contractante;
g. colaborarea cu personalul Autorității Contractante alocat pentru serviciile desfășurate conform Contractului (monitorizarea progresului activităților în cadrul Contractului, coordonarea activităților în cadrul Contractului, feedback).

7.2. *FACILITATI OFERITE DE FURNIZOR*

Furnizorul va asigura expertilor sai sprijin administrativ, de secretariat si traducere, dupa caz, care sa le permita expertilor desfasurarea in bune conditii a activitatilor din acest contract.
Printre altele, **Furnizorul** va fi responsabil pentru (si va suporta costurile):

- Asigurarea cazarii, serviciilor de masa, si transportului (local si international) pentru personalul său;
- Cheltuieli de relocare, asigurari de sanatate, dupa caz;
- Asigurarea spatiului necesar pentru desfasurarea activitatilor expertilor (suplimentar fata de cel pus la dispozitie de autoritatea contractanta), dotat cu mobilier si toate echipamentele si materialele necesare;
- Cheltuieli de comunicare;
- Serviciile de secretariat;
- Orice cost legat de interpretare si traduceri, imprimarea sau multiplicarea rapoartelor;
- Costurile pentru angajarea expertilor;
- Costurile elaborarii si transmiterii rapoartelor;
- Orice alte cheltuieli legate de activitatea Furnizorul.

Echipamente
Furnizorul va fi responsabil si va suporta costurile pentru toate echipamentele necesare in executarea obligatiilor asumate prin Contractul de prestari servicii.
Niciun fel de echipamente nu vor fi achizitionate in numele Autoritatii Contractante/beneficiar ca parte a serviciilor din cadrul Contractului sau transferate Autoritatii Contractante/ beneficiarului la finalizarea Contractului.

7.3. *RAPORTARE*

7.3.1. Cerințe privind raportarea

Furnizorul este responsabil de elaborarea si transmiterea urmatoarelor rapoarte catre Autoritatea Contractanta:

Raportul Inițial
Va fi intocmit in maxim 2 saptamani de la data inceperii executarii Contractului. Acest document trebuie sa aiba in vedere precizarile din Caietul de sarcini si Propunerea tehnica si sa aduca detalierile necesare, structurari sau clarificari unde este cazul. Raportul va cuprinde planificarea activitatilor, metodologia utilizata si indicatorii planificati pentru fiecare etapa. Raportul initial va constitui principalul instrument de lucru si se va face referire la el pe toata perioada de executare a Contractului. Raportul initial va fi inaintat spre aprobare Autoritatii Contractante.

Rapoarte lunare
Furnizorul va elabora un raport lunar prin care sa prezinte evolutia lunara a activitatilor si intarzierile, daca acestea sunt semnificative. Rapoartele lunare vor detalia:

- Progresele inregistrate;
- Activitati aflate in derulare cu data estimativa a finalizarii acestora si cu rezultatele anticipate;
- Dificultatile intampinate in cursul implementarii proiectului si solutiile propuse pentru a depasi respectivele dificultati;
- Rezultatele realizate in cursul perioadei de raportare, resursele utilizate, precum si recomandarile sau solicitarile aferente, si planificarea activitatilor pentru perioada urmatoare.

Rapoartele lunare vor fi transmise pana in data de 5 a urmatoarei luni pentru care se face raportarea (de ex. Raportul aferent activitatii din luna ianuarie se va transmite pana pe data de 5 februarie). În cazul în care data de 5 a lunii respective este o zi nelucrătoare, furnizorul va anticipa transmiterea raportului lunar.

Raportul final
Varianta preliminara a Raportului final trebuie sa fie transmisa Echipei de implementare a Proiectului cu cel putin o luna inainte de sfarsitul perioadei de executie a Contractului pentru a fi analizata. Acest raport trebuie sa descrie intreg procesul de executie si va inlesni evaluarea rezultatelor obtinute atat in termeni calitativi, cat si cantitativi.
Raportul va cuprinde:

- evaluarea succesului si constrangerilor majore pentru fiecare activitate;
- realizarile generale ale Contractului;
- recomandari pentru actiuni viitoare cu scopul asigurarii durabilitatii activitatilor, rezultatele asteptate dupa finalizarea Contractului, precum si masurile ce trebuie intreprinse in acest sens.

Varianta preliminara a acestui raport va fi revizuita cu observațiile/comentariile primite din partea Autoritatii Contractante, în termen de 5 zile lucrătoare de la data primirii observațiilor/comentariilor. Autoritatea Contractantă va transmite observațiile/comentariile în termen de 15 zile lucrătoare de la data primirii variantei preliminare a Raportului final.
Alte rapoarte: Autoritatea Contractanta poate cere Furnizorului sa elaboreze pe parcursul derulării Contractului si alte rapoarte, in masura in care acestea sunt legate de buna desfasurare a Contractului.

7.3.2. Transmiterea și aprobarea rapoartelor

Raportul initial, Rapoartele lunare si Raportul final trebuie transmise, in trei exemplare, spre aprobare, in atentia Managerului de Proiect al Echipei de implementare a proiectului din partea Autoritatii Contractante.
Toate rapoartele vor fi redactate in limba romana. Variantele intermediare, de lucru, pot fi transmise Autoritatii Contractante doar in format electronic editabil. Variantele finale vor fi transmise, atat in format electronic editabil, cat si pe hartie. Aprobarea rapoartelor se face de catre Comisia de receptie desemnata de Autoritatea Contractanta.
Autoritatea Contractanta, în urma recepției, va aproba rapoartele sau va prezenta observatiile sale in termen de maxim 10 zile lucratoare de la data depunerii rapoartelor initial, lunare, respectiv 15 zile lucratoare pentru raportul final.
In cazul unor modificari, Furnizorul are obligatia de a raspunde pozitiv solicitarilor Autoritatii Contractante de modificare/ completare a rapoartelor, corespunzator cu observatiile Autoritatii Contractante, in termen de maxim 5 zile lucratoare de la data primirii acestora. Autoritatea Contractanta, prin recepție, va proceda la aprobarea sau respingerea rapoartelor, dupa caz, in termen de 15 zile lucratoare de la data primirii acestora in forma revizuita, termen care poate fi prelungit in functie de situatiile specifice.

7.3.3. Indicatori de performanță

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

Indicator privind calitatea livrabilelor proiectului

- **Categorie indicator**: Nivelul de calitate; -
- **Indicator de performanță al contractului:** Livrabil adecvat pentru scopul utilizării;
- **Nivelul de performanță așteptat conform Caiet de sarcini:** Documentele elaborate sunt conforme cerințelor stabilite în Caietul de Sarcini;
- **Ce se măsoară:** Nivelul de acuratețe al livrabilelor după "peer review" (sub nivelul de calitate, agreat conform cerințelor stabilite în Caietul de Sarcini și/sau prezentat în oferta tehnică).
- **Modalitatea de evaluare:**
  - **Foarte satisfăcător (5 puncte)** – Livrabilele includ îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini și prezentate în oferta tehnică.
  - **Satisfăcător (4 puncte)** – Livrabilele includ unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreat. Au fost necesare doar ajustări nemateriale.
  - **Acceptabil (3 puncte)** - Livrabilele nu includ neconformități/inexactități față de nivelul agreat însă nu include nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului. Nu au existat întârzieri semnificative ca urmare a efctuarii eventualelor remedieri.
  - **Nesatisfăcător (2 puncte)** - Livrabilele prezintă neconformități / inexactități față de nivelul agreat iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă

rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost remediate de către Furnizor.

- **Foarte nesatisfăcător (1 punct)** – Livrabilele prezintă neconformități / inexactități majore față de nivelul agreat iar aceste aspecte nu au putut fi corectate de către Furnizor. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului.

Indicator privind termenele de predare a livrabilelor proiectului

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

7.4. *CONFLICTUL DE INTERESE*

Se aplica prevederile legii nr. 98/2016 privind achizitiile publice, cu completarile și modificările ulterioare.
Pentru a se asigura independenta Ofertantului, acesta va semna o declaratie prin care certifica faptul ca nu se afla in conflict de interese in momentul depunerii ofertei si ca va informa Autoritatea Contractantă in cazul in care se va afla la un moment dat in situatia de conflict de interese, chiar potential, in timpul indeplinirii sarcinilor pentru care a fost contractat.

7.5. *DREPTURI DE PROPRIETATE INTELECTUALĂ*

Toate documentele ce vor fi elaborate in executarea Contractului (Livrabile, studii, analize, rapoarte, planuri, proceduri, metodologii, materiale de instruire si prezentare etc) vor face obiectul dreptului exclusiv de proprietate (inclusiv, dar fara a se limita la drepturi de autor si/sau orice alte drepturi de proprietate intelectuala) al Autoritatii Contractante, care le poate utiliza, publica sau transfera dupa cum considera necesar, fara nicio limitare geografica sau de alta natura.

Drepturile patrimoniale de autor asupra solutiei tehnice create de către Furnizor (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, ADR (cf. art. 12, alin. (1) din Ordonanţa de urgenţă nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administraţiei publice centrale şi pentru modificarea şi completarea unor acte normative: *"Instituţiile publice şi organele de specialitate ale administraţiei publice centrale au obligaţia de a prevedea explicit în caietele de sarcini şi în contractele aferente procedurilor de achiziţie publică demarate de la data intrării în vigoare a prezentei ordonanţe de urgenţă, care includ dezvoltări de programe informatice la solicitarea instituţiei sau autorităţii, faptul că toate drepturile patrimoniale de autor asupra tuturor operelor create de către contractant sau membrii asocierii, aferente produsului sau serviciului livrat, se transferă către autoritatea contractantă".*

Înainte de plata facturii finale, Furnizorul va preda Autorității Contractante:

- **codul sursă al aplicației informatice dezvoltate documentat si versionat intr-un repository specific;**
- **documentația aferentă intregului sistem informatic;**
- **kit-urile de instalare pentru ultima versiune a aplicatiilor informatice comerciale, impreuna cu documentatiile aferente.**

7.6. *ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI*

7.6.1. Propunerea tehnica

Ofertantul va descrie în detaliu modul de îndeplinire a cerinţelor de realizare a activităţilor. Metodologia de prestare a serviciilor constituie acea parte a propunerii tehnice care prezintă strategia propusă de ofertant pentru prestarea serviciilor solicitate prin specificaţiile tehnice incluse în documentaţia de atribuire.
Metodologia trebuie să cuprindă minimum următoarele informaţii:

- descrierea de ansamblu a abordării propuse de ofertant pentru prestarea serviciilor, precum şi a riscurilor aferente implementării proiectului;
- descrierea cât mai detaliată a activităţilor propuse de ofertant pentru prestarea serviciilor solicitate, cu indicarea oricăror etape / stadii considerate ca esenţiale, a rezultatelor şi efectelor aşteptate şi estimate ale fiecărei activităţi, precum şi a riscurilor specifice fiecărei activităţi;
- descrierea contribuţiei ofertantului, în termeni de resurse umane specializate, cunoştinţe etc., necesare pentru ducerea la îndeplinire în cele mai bune condiţii a activităţilor respective şi obţinerea rezultatelor;
- în cazul în care oferta este depusă de o asociere, o descriere a implicării fiecărui asociat în prestarea serviciilor solicitate, a modului de colaborare între asociaţi în vederea executării contractului, inclusiv prin delimitarea sarcinilor şi responsabilităţilor individuale în prestarea serviciilor;
- descrierea oricăror aranjamente de subcontractare a unei părţi a serviciilor solicitate, a interacţiunii dintre ofertant şi subcontractor/i, precum şi o descriere detaliată a serviciilor ce vor fi subcontractate.

Graficul de prestare a serviciilor constituie acea parte a propunerii tehnice care prezintă calendarul propus de ofertant pentru prestarea serviciilor solicitate prin specificaţiile tehnice incluse în documentaţia de atribuire.
Graficul trebuie să includă un calendar al activităţilor ce vor fi derulate în cadrul contractului, conform metodologiei de prestare a serviciilor, a modului în care activităţile respective sunt reflectate în rapoarte, a legăturilor şi relaţiilor dintre activităţi şi secvenţialitatea acestora. Etapele de raportare pe fiecare activitate vor fi evidenţiate ca activităţi separate.
Calendarul propus trebuie să se încadreze în termenele indicate în caietul de sarcini. Beneficiarul a indicat pentru fiecare activitate şi rezultat aşteptat termenul maxim la care acestea trebuie realizate, fiind în sarcina Prestatorului să propună termenele de execuţie, în funcţie de legăturile şi condiţionalităţile existente între etape şi să asigure corelarea acestora din punct de vedere al secvenţialităţii şi resurselor implicate.
Ofertantul are obligaţia să respecte toate cerinţele prezentate în caietul de sarcini şi să dezvolte într-o manieră proprie şi originală punctele prezentate. Neregăsirea cerinţelor minime prezentate în caietul de sarcini va presupune declararea ofertei ca fiind neconformă.
Propunerea tehnică va fi astfel prezentată încât să asigure posibilitatea verificării conformităţii acesteia cu cerinţele minime obligatorii prevăzute în caietul de sarcini. Propunerea tehnică trebuie să reflecte modul în care Ofertantul înţelege să îndeplinească în integralitatea lor, cerinţele prevăzute în Caietul de sarcini.

7.6.2. Propunerea financiară

Propunerea financiară va fi prezentată în lei, atât în sumă globală, cu evidenţierea separată a TVA, pe fiecare activitate/subactivitate, cu evidenţierea unităţilor de măsură şi a valorilor unitare, conform anexei la formularul de ofertă financiară ce se regăseşte şi mai jos:

Nr. crt.	Livrabile	Preţ unitar fără TVA (lei)	Valoare totală fără TVA (lei)	Valoare TVA (lei)	Valoare totală maximă cu TVA (lei)
1	Platforma Software Centralizata pt. Identificare Digitala – PSCID **AMENAJARE CETRU DE DATE**				
2	Platforma Software Centralizata pt. Identificare Digitala – PSCID **HARDWARE**				
3	Platforma Software Centralizata pt. Identificare Digitala – PSCID **SOFTWARE DE BAZA**				
4	Platforma Software Centralizata pt. Identificare Digitala – PSCID **SERVICII DE PROIECTARE, INSTALARE SI CONFIGURARE, DEZVOLTARE, IMPLEMENTARE SI TESTARE**				

5	Platforma Software Centralizata pt. Identificare Digitala – PSCID **SERVICII DE INSTRUIRE**				
TOTAL OFERTA FINANCIARA					

Bugetul de cheltuieli incidentale nu va fi inclus în propunerea financiară.
Nu există suprapuneri între costurile logistice / cheltuieli incidentale şi categoriile de cheltuieli directe (precum onorariile expertilor).

7.7. *MODALITATEA DE PLATĂ ŞI TERMENE*

Autoritatea Contractantă va efectua 5 (cinci) plati către Furnizor, în baza facturilor emise de către acesta din urmă şi în baza proceselor verbale de recepţie semnate de comisia de recepţie din partea Beneficiarului pentru fiecare livrabil din oferta financiara.
Platile se vor efectua pentru realizarea şi finalizarea sub-activităţilor (conform Gantt al proiectului si livrabilelor):

- Analiza necesităţilor;
- Proiectarea soluţiei informatice;
- Servicii de livrare, instalare şi punere în funcţiune echipamente HW şi licenţe software;
- Dezvoltarea aplicaţiei informatice;
- Testarea aplicaţiei;
- Pilotare la nivel national;
- Instruirea echipei de proiect.

Modalitatea de plată şi termenele sunt prevăzute în Contract, anexa la prezenta documentaţie de atribuire.

Documentele tip, necesare pentru efectuarea plăţii din cadrul contractului de către Prestator, sunt prezentate mai jos:

1. Aviz de însoţire a mărfii (dacă este cazul);
2. Certificate de garanţie şi declaraţie conformitate (dacă este cazul);
3. Set de proceduri şi mecanisme pentru coordonare şi consultare factori interesaţi;
4. Manuale de utilizare a aplicaţiei;
5. Suport de curs, în format electronic;
6. Liste de prezenţă;
7. Chestionare evaluare instruire;
8. Certificate de participare;
9. Raport al activităţii;
10. Proces verbal de recepţie calitativ si cantitativ al produselor/serviciilor cat şi a raportului aferent activitatii;
11. Factura fiscală.

Orice obiecţiune de natură financiară sau privind calitatea rezultatelor atinse poate determina diminuarea valorii de plată.
Decizia Beneficiarului de diminuare a sumei de plată va fi motivată şi comunicată în scris Prestatorului.
Factura se va emite de către Prestator după recepţionarea echipamentelor/serviciilor de către Autoritatea Contractantă.

7.8. *IPOTEZE ȘI RISCURI*

Riscurile contractului au fost definite prin cererea de finanțare a proiectului din care face parte prezentul contract.

7.8.1. Riscurile

Riscurile avute în vedere sunt:

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
1.	Prelungirea termenelor procedurilor de achiziție publica	- realizarea si actualizarea permanenta a unui plan de achizitii - analiza permanenta a legislatiei referitoare la achizitiile publice - un membru al echipei de proiect are rolul de a coordona si realiza derularea achizitiilor publice
2.	Începerea activitaților cu întârziere	- realizarea si actualizarea permanenta a unui plan de management - monitorizarea permanenta a respectarii termenelor
3	Depunerea cu întârziere a documentelor aferente Cererilor de rambursare sau a altor documente cerute de proiect sau de Autoritatea de Management	- organizarea riguroasa a documentelor justificative ale proiectului - achiziție soluție de document management pentru proiect - realizarea corecta si la timp a raportarilor - urmarirea atenta a programarii cheltuielilor, în strânsa corelare cu bugetul aprobat si programul de activitați
4	Fluctuații de personal	- selectarea atenta a persoanelor din echipa de proiect - selectarea unei echipe de formate din persoane externe, care vor fi angajate pe toata durata proiectului
5	Modificari legislative care influențeaza implementarea proiectului	- monitorizarea permanenta a modificarilor legislative - respectarea Contractului de finantare - Comunicare permanenta cu Autoritatea de management
6	Indisponibilitatea unor produse/servicii prevazute în proiect	- plan de achizitii realist, care corespunde ofertei de pe piata - informarea prealabila privind disponibilitatea de oferte si livrare de servicii si bunuri
7	Calitate necorespunzătoare a produselor/serviciilor	-selecția atentă a furnizorilor de bunuri și servicii, inclusiv pe baza performanțelor dovedite anterior -întocmirea unor documentații de atribuire acoperitoare elaborarea unor clauze stricte în contracte referitor la neîndeplinirea obiectivelor la nivelul de calitate solicitat
8	Modificări in structura organizatorica a implementatorului	-flexibilității in planificarea si utilizarea resurselor umane incluse in proiect si posibilitatea suplimentarii resurselor alocate in cazul in care riscul se materializează
9	Probleme de comunicare	-stabilirea și monitorizarea respectării unui circuit de

	și coordonare între membrii echipei de proiect	comunicare între membrii echipei de proiect
10	Riscuri politice: - instabilitatea factorului politic poate duce la schimbari legislative si normative; - poate induce instabilitate la nivel administrativ si decizional prin schimbari în organizarea, functionarea si/sau conducerea institutiilor	-atenuarea efectelor acestui risc se va efectua asigurând o echipa dedicata implementarii acestui proiect, astfel încât deciziile politice sa nu influenţeze realizarea investiţiei.

Riscuri care pot fi identificate la momentul elaborării Caietului de Sarcini şi riscuri care pot apărea în derularea contractului sunt următoarele:

a. dificultăţi de colaborare şi comunicare între factorii interesaţi implicaţi;
b. datele şi informaţiile necesare desfăşurării serviciilor comunicate de către Autoritatea Contractantă nu sunt suficiente pentru îndeplinirea cerinţelor solicitate prin Caietul de Sarcini;
c. adăugarea de activităţi/ solicitări de informaţii noi, în funcţie de progresul activităţilor.

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

Ofertantul va introduce în propunerea tehnică:

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

7.8.2. Ipotezele

Ipoteze avute în vedere sunt:

a. conţinutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
b. corelaţia dintre resursele necesare şi rezultatele aşteptate este realistă;
c. începerea serviciilor se va realiza în perioada preconizată;
d. nu se prevăd schimbări ale cadrului instituţional şi legal care să afecteze major implementarea şi desfăşurarea în bune condiţii a Contractului;
e. toate informaţiile relevante şi disponibile la nivelul Autorităţii Contractante pentru realizarea serviciilor vor fi puse la dispoziţia Contractantului;
f. Contractantul va semna un acord de confidenţialitate la momentul semnării Contractului şi va respecta toate instrucţiunile privind utilizarea informaţiilor confidenţiale.

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