CAIET DE SARCINI

pentru

SERVICII DE DEZVOLTARE ȘI IMPLEMENTARE SISTEM INFORMATIC, INCLUSIV SERVICII DE INSTRUIRE

în cadrul proiectului

Sistem informatic pentru registrele de sănătate – RegInterMed

1. INFORMAȚII GENERALE. OBIECTIVELE PROIECTULUI

1.1. *INFORMAȚII GENERALE*

Autoritatea Contractantă este **MINISTERUL SĂNĂTĂȚII** (denumit în continuare și **M.S.**).

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 servicii de instruire 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 potenţialii ofertanți să elaboreze propunerea tehnică corespunzător cu necesităţile autorităţii contractante.

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

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

Operatorii economici vor indica şi dovedi în cuprinsul ofertei care informaţii din propunerea tehnică, elemente din propunerea financiară şi/sau fundamentări/justificări de preţ/cost sunt confidenţiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Informaţiile indicate de operatorii economici din propunerea tehnică, elemente din propunerea financiară şi/sau fundamentări/justificări de preţ/cost ca fiind confidenţiale trebuie să fie însoţite de dovada care le conferă caracterul de confidenţialitate, dovadă ce devine anexă la ofertă.

1.2. *OBIECTIV GENERAL*

Proiectul propus de catre **MINISTERUL SĂNĂTĂȚII** spre finanțare prin POC are ca obiectiv general eficientizarea sistemului de sanatate prin dezvoltarea si consolidarea de sisteme informatice ale depozitelor de date, de monitorizare, documentare si suport al proceselor de decizie.

Eficientizare sistemului informatic va implica actualizarea progresiva de informatii, în functie de nevoile de informatii de sanitate identificate - diagnostic, evolutie, tratament, status vital, luarea deciziilor în situatii de urgenta respectând însa particularitatile si scopul pentru care se colecteaza aceste date (calculul indicatorilor de incidenta, prevalenta si mortalitate, cercetare medicala etc.).

Obiectivul sistemului informatic propus este de a inregistra, coerent şi la timp datele din registrele de sanatate, fapt ce va conduce la creşterea transparenţei şi la dezvoltarea unui instrument important de informare şi suport operaţional pentru utilizatori.
Sistemul informatic propus va respecta atât politicile şi reglementările interne ale instituţiei pentru tehnologia informaţiei cât şi legislaţia în vigoare privind protecţia datelor cu caracter personal, protecţia informaţiilor clasificate şi alte acte normative care referă tehnologia informaţiei.

1.3. *OBIECTIVE SPECIFICE*

Obiectivele specifice ale proiectului sunt:

- Realizarea registrelor de sanatate si interconectarea acestora cu alte platforme IT din domeniul e-sanatate.
- Cresterea utilizarii sistemelor de e-sanatate prin realizarea sistemului informatic pentru registrele de sanatate – „RegInterMed”.
- Actualizarea progresiva de informatii, în functie de nevoile de informatii de sanatate identificate - diagnostic, tratament, evolutie, luarea deciziilor în situatii de urgenta respectând însa particularitatile si scopul secundar pentru care se colecteaza aceste date (calculul indicatorilor de incidenta, prevalenta, morbiditate si mortalitate, cercetare medicala etc).
- Dezvoltarea infrastructurii informatice în domeniul e-sanatate, pentru a sprijini utilizarea TIC.
- Dezvoltarea Sistemului Informatic Integrat în domeniul sanatatii prin implementarea solutiilor sustenabile de e-sanatate.
- Integrare în platforme de e-sanatate existente la nivel european..

1.4. *CADRUL LEGAL*

Prestatorul va desfășura activitățile, va 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, enumerarea următoare nefiind limitativă:

Nr. crt.	Document
1	Strategia Europa 2020, o strategie pentru creștere inteligentă, ecologică și favorabilă incluziunii, Cadrul Strategic Comun 2014-2020
2	Strategia europeană privind Piața Unică Digitală
3	Strategia Națională privind Agenda Digitală pentru România (SNADR) 2020
4	Strategia de Securitate Cibernetică a României

Nr. crt.	Document
5	Planul Naţional de Reformă
6	POC 2014-2020
7	Legea nr. 455/2001 privind semnătura electronică
8	Hotărârea Guvernului nr. 1259/2001 pentru aprobarea Normei tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, actualizată
9	Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
10	Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare
11	Legea nr. 98/2016 privind achizițiile publice
12	HG nr. 395/2016 pentru aprobarea Normelor Metodologice de aplicare a prevederilor referitoare la atribuirea Contractului de achiziție publică /acordului-cadru din Legea nr. 98/2016 privind achizițiile publice
13	Ordonanța de urgență nr. 38/2020 privind utilizarea înscrisurilor în formă electronică la nivelul autorităților și instituțiilor publice
14	Hotărârea Guvernului nr. 285/2020 pentru modificarea și completarea Hotărârii Guvernului nr. 1.235/2010 privind aprobarea realizării Sistemului național electronic de plată online a taxelor și impozitelor utilizând cardul bancar

1.5. *VALOAREA ŞI DURATA CONTRACTULUI*

Valoarea contractului

Valoarea totală a achiziției este de **52.374.000,00** lei fără TVA, respectiv **62.325.060,00** lei cu TVA.

Durata de implementare a contractului

Durata de implementare a contractului este de **24 de luni de la semnarea contractului cu posibilitate de prelungire, dar nu mai mult de 31.10.2023**.

Activitățile aflate în responsabilitatea Prestatorului sunt prevăzute a se desfășura conform graficului de implementare a proiectului, anexă 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. CERINȚE PRIVIND SOLUȚIA TEHNICĂ

2.1. *CERINŢE GENERALE*

Sistemul informatic propus are ca scop principal furnizarea de servicii online specifice domeniului e-sanatate în beneficiul cetăţenilor şi al instituţiilor şi organizaţiilor din domeniul sanatatii. În plus, acesta este un instrument ce permite desfăşurarea în mod eficient şi în anumite cazuri automat a activităţilor specifice interfeţei dintre organismele administraţiei centrale şi cetăţeni. Activitatea specifică a instituţiei şi serviciile publice oferite de către aceasta pentru cetăţeni vor fi puse la dispoziţie prin intermediul componentei aplicative sub forma de servicii web publice online. Acest lucru va asigura apropierea instituţiei de cetăţeni şi va oferi acestora servicii moderne şi electronice.
Soluţia implementată trebuie să asigure interoperabilitatea sistemului informatic propus cu alte sisteme existente în cadrul CNAS precum si cu sistemele informatice de tip HIS ale unitatilor medicale.
Din perspectiva colaborării inter-instituţionale, comunicarea şi colaborarea joacă un rol esenţial. Sistemul informatic propus este instrumentul modern, actual, care asigură legătura directă între instituţie şi publicul larg.
Sistemul informatic propus va respecta atât politicile şi reglementările interne ale instituţiei pentru tehnologia informaţiei cât şi legislaţia în vigoare privind protecţia datelor cu caracter personal, protecţia informaţiilor clasificate şi alte acte normative care referă tehnologia informaţiei.
Interfaţa utilizator a sistemului se urmarește să fie intuitivă (facilă), informativă, fiabilă, atractivă şi stabilă, ea fiind accesibilă doar medicilor specialisti. Interfaţa utilizator va fi accesată utilizând ultimele versiuni ale browser-elor Mozilla, Firefox, Edge, Google Chrome şi va fi optimizat pentru o rezoluţie de minim 1024x768. Prin utilizarea şabloanelor de afişare se va obţine o interfaţă grafică unitară. Aceasta va fi realizată conform ultimelor versiuni ale standardelor HTML, CSS, XML.
Furnizorii de servicii vor avea la dispoziţie servicii web pentru transmiterea şi validarea documentelor medicale în format electronic care vor fi accesate prin intermediul unor aplicaţii informatice proprii.

Definiție Registru medical = un sistem organizat care colectează, analizează și difuzează datele și informațiile despre un grup de persoane definit de o anumită boală, condiție, sau serviciu de sănătate și care servește unor scopuri medicale prestabilite: științifice, clinice sau / și pentru stabilirea unei politici publice.

Clasificare registre:

Categorie	**Boli și condiții**	**Produse/dispozitive medicale**	**Servicii, Medicale**
Tipul obiectului	boli cronice, acute transmisibile, boli rare, handicap, cauză de deces	medicamente, dispozitive, echipamente	diagnostic, curativ, preventiv, evacuări, nașteri, avorturi
	rezultatele sănătate (obiectiv, raportat de pacient)		
	eficiență (clinică, comparativă, financiară)		
	siguranța și incidente		
	intervenție (planificare, ghiduri, memouri)		
Acoperire (geografică și organizațională)	local (județe, districte, asigurători, asociații profesionale, ONG-uri)		
	național (SM, non-SM)		
	internațional (regional, european, european, global)		
	unitatea de îngrijire a sănătății (GP, spital)		
	populație (pe bază geografică)		

Categorie	Boli și condiții	Produse/dispozitive medicale	Servicii, Medicale
Definirea populației	populație (dependentă de expunere)		
Unitate de observare	pacient (utilizator, client, asigurător)		
	persoană cu o caracteristică de observație	dispozitiv de persoană, echipament	eveniment legat de persoană (naștere, moarte, serviciu)

Observații legate de dezvoltarea registrelor:

- Un format unitar al registrelor nu este aplicabil la maladii foarte diferite (acute vs cronice, temporare vs permanente, afectand organe diferite). Fiecare boala are cerinte proprii privind parametrii care trebuie inregistrati, fara de care simpla numarare a cazurilor ramane fara beneficiu.
- Incarcarea datelor pacientilor in registru este o activitate care necesita personal dedicat. Experienta tuturor registrelor din domeniul pneumologiei care au functionat pana in prezent arata ca fara registratori dedicati doar o minoritate din cazuri ajung sa fie inregistrate, ceea ce duce la esuarea obiectivelor oricarui registru (epidemiologice, bugetare sau de cercetare). Exemplul pozitiv al registrului cazurilor de tuberculoza arata ca acesta este complet deoarece a existat de la bun inceput personal dedicat includerii cazurilor in baza de date.

În accepțiunea europeană registrele de boli sunt registrele pentru pacienți care au același diagnostic (de exemplu: fibroza cistică sau infarct sau fac parte din același grup - de exemplu persoane cu dizabilități).

Principii cheie de constituire a registrelor de boli**:**

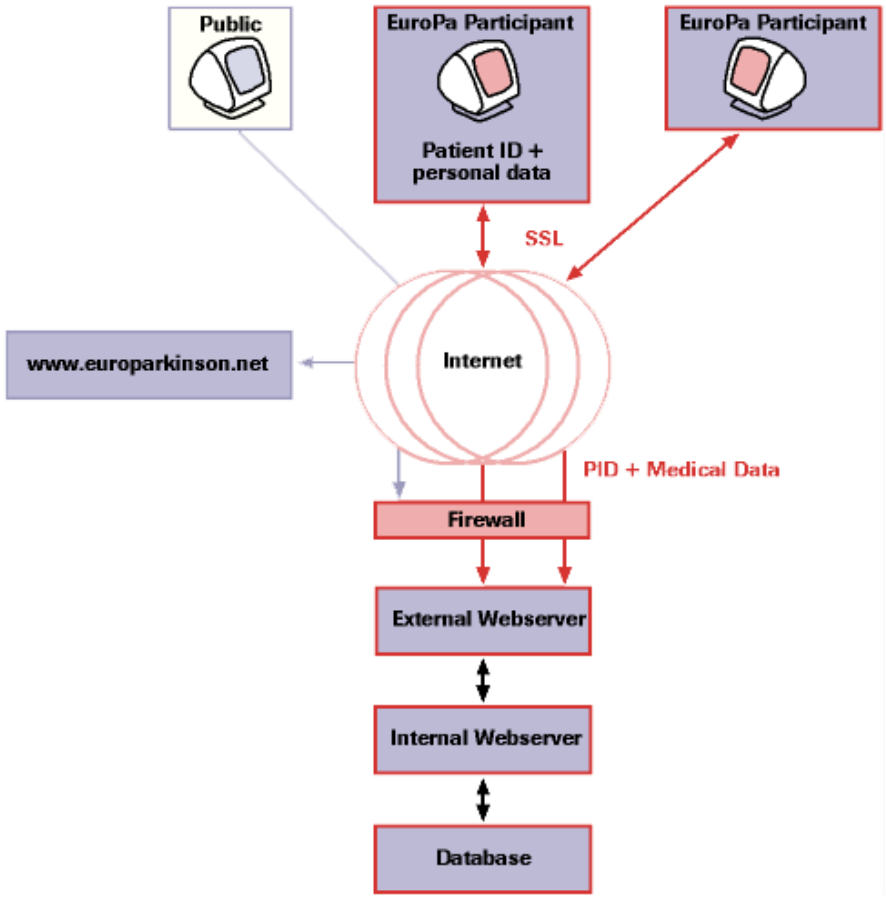
- Scopul, obiectivele și rezultatele registrului trebuie să fie definite în mod clar și succint, într-o manieră susținută de cele mai bune dovezi și orientări, și care să fie conștient de existența unei suprapuneri cu alte proiecte la nivel național și internațional.
- Menținerea unei abordări concentrate, deschise și transparente a dezvoltării registrelor este vitală.
- Pentru fiecare registru din domeniul sănătății se va analiza dacă registrul este interoperabil și că respectă standardele, seturile de date și terminologia relevante.
- Pentru fiecare registru se vor publica orientări clare cu privire la obligațiile legale. Aceasta vor include evaluarea impactului asupra vieții private, politicile de protecție a datelor, proprietatea asupra datelor, accesul la date și proprietatea intelectuală.
- Domeniul de aplicare al registrului va trebui să fie menținut pe măsura dezvoltării proiectului.
- Plan de guvernare al registrelor. Va fi susținut de echipele pentru fiecare de registru care includ, cel puțin, o echipă de management de proiect, un comitet științific și un comitet de asigurare a calității. Printre altele, aceste grupuri pot identifica seturi de date necesare pentru a asigura că registrul își îndeplinește rezultatele predefinite, pe lângă crearea unor politici clare privind accesul la date și asigurarea menținerii asigurării calității.

Pe lângă proiectele naționale funcționale menționate mai jos, la nivel European există câteva exemple de bune practici:

- EUBIROD (“European Best Information through Regional Outcomes in Diabetes”) registrele regionale pentru diabet. (partener din Romania: Simion Pruna Board Directors, Secretary for Medical Technology & IT at Romanian Association of Medicine)
  - Initiativa venita in sprijinul European Parliament resolution of 14 March 2012 on addressing the EU diabetes epidemic (2011/2911(RSP))

  - Institute of Diabetes, Nutrition and Metabolic Diseases “Prof. N. Paulescu”, Bucharest, Romania **Contact person:** Simion Pruna www.paulescu.ro
- BRidging Information and Data Generation for Evidence-based Health policy and research.
- European Academy of Allergy and Clinical Immunology (EAACI) avand ca rezultat: Registrul EAACI Allergy Registry Task Force (A-reg)
  - Romanian Society of Allergology and Clinical Immunology (RSACI)
    President
    Roxana Bumbacea
    Email: roxana.bumbacea@gmail.com
    Representative
    Florin-Dan Popescu
    Email: florindanpopescu@allergist.com Official website: www.sraic.eu
  - Romanian Society of Pneumology
    President
    Ruxandra Ulmeanu
    Email: r_ulmeanu@yahoo.com
    Representative
    Florin Mihaltan
    Email: mihaltan@starnets.ro
  - Registre relevante alergii:
    https://www.anaphylaxie.net/index.php?L=1
- EuroPa Rețeaua europeană de cooperare pentru cercetarea, diagnosticarea și terapia bolii Parkinson urmărește îmbunătățirea cercetării clinice și a tratamentului bolii Parkinson în Europa, prin crearea de rețele de expertiză și resurse de centre clinice de înaltă calificare în diferite țări europene. Proiectul este coordonat de Prof. Wolfgang Oertel de la Philipps-University Marburg (Germania). Inițial, rețeaua EuroPa va asocia centrele clinice din 11 țări. Rețeaua va fi apoi transformată într-o organizație independentă și durabilă, care va urmări misiunea EuroPa dincolo de perioada de finanțare a UE. Specialiștii din centrele clinice din alte țări europene vor putea apoi să se alăture rețelei. EuroPa va colabora, de asemenea, cu alte rețele de cercetare, cum ar fi Grupul european de studiu MSA, care este finanțat și de UE și se concentrează asupra Atrofiei multisistem (MSA), o boala neurodegenerativă distinctă din aceeași familie neuropatologică cu boala Parkinson, care afectează mai multe sisteme neurale din SNC, și care clinic se manifestă cu parkinsonism și alte tulburări motorii și vegetative progresive, invalidante și cu risc vital, însă neresponsivă la terapiile caracteristice bolii Parkinson.

  Vizualizare schematică a infrastructurii IT a registrului pacientului EuroPa:



Participarea la registrul EuroPa este voluntară și fiecare pacient semnează un formular de consimțământ înainte de introducerea datelor. În prezent, numai pacienții din centrele clinice participante vor fi incluși în registru. Un chestionar uniform - setul minim de date - va fi folosit pentru a colecta date clinice comparabile de la toți pacienții. Datele clinice ale tuturor pacienților sunt păstrate pseudonime. Doar personalul responsabil din centrul clinic de tratament este capabil să re-identifică un anumit pacient. Re-identificarea va fi necesară pentru vizitele de urmărire în vederea actualizării datelor clinice și a informării pacienților cu privire la orice studiu sau studiu planificat.
În afară de un browser web obișnuit, nu este necesar un software suplimentar la site-ul utilizatorului. Participanții EuroPa care sunt autorizați vor accesa serverul web extern pentru a trimite informații către baza de date centrală. Informațiile sunt schimbate prin intermediul unei aplicații web, furnizând chestionarul și diverse opțiuni pentru introducerea datelor. Serverul extern web solicită apoi informațiile necesare din baza de date și transmite informațiile înapoi participantului EuroPa. Transferul de date va fi criptat. Baza de date de pe serverul central comunică numai cu serverul web intern.
Registrul de pacienți este protejat împotriva utilizării abuzive prin diferite măsuri de securitate.

- European Partnership for Action Against Cancer (**EPAAC**)

Rețeaua europeană a registrelor de cancer (ENCR) are ca obiectiv îmbunătățirea comparabilității datelor privind incidența cancerului, promovarea înregistrării cancerului Europa precum și promovarea utilizării informațiilor privind cancerul pentru cercetare și stabilire politici publice. În prezent, există peste 200 de registre de cancer active în cadrul ENCR în Europa. Sistemele de colectare a datelor din UE reflectă organizarea specifică a sistemelor naționale de sănătate, iar barierele privind accesul la date sunt persistente. Trecerea de la scară națională la cea europeană este încă dificilă, deoarece nu toți indicatorii sunt comparabili în întreaga UE. Registrele furnizează în prezent cele mai multe date epidemiologice privind cancerul, dar sunt subfinanțate, în cea mai mare parte sub personal, luptând cu legile naționale și europene privind datele de protecție sau sunt lansate fără o planificare adecvată.

Un exemplu de buna practică este sprijinul acordat Republicii Moldovei in 2016 de către ENCR și JRC pentru registrul national.
Există in momentul actual initiative europenne privind calitatea softului si a colectării datelor, initiativa concretizata prin documentul programatic "One common procedure for data quality checks for European cancer registries" publicat in 2014.
Cea mai recentă versiune a JRC-ENCR QCS a fost lansată la 24 noiembrie 2016 și include:

- verificarea formatului de fișiere (pentru incidență, mortalitate, populatie) și a variabilelor - nume și ordine conform ghidului de depunere a datelor;
- verificarea consecvenței interne a variabilelor;
- controale încrucișate între variabile;
- verificări tumori primare.

Orice propunere de registru național va trebui sa îndeplinească criteriile de calitate stabilite de JRC-ENCR QCS.
O propunere nefinalizata inca este propunerea pentru European Cancer Information System (ECIS)

- Orphanet (http://www.orpha.net/consor/cgi-bin/index.php) este o altă inițiativă legată de bolile rare și este considerată aici o bună practică. Este un portal de referință și o bază de date pentru informații privind bolile rare și medicamentele orfane, conduse de un consorțiu de parteneri europeni, cu scopul de a contribui la îmbunătățirea diagnosticării, îngrijirii și tratamentului pacienților cu boli rare. Serviciile Orphanet includ: un inventar al bolilor rare și clasificarea acestora; o enciclopedie a bolilor rare; o listă a registrelor europene privind bolile rare. Unul dintre beneficiile serviciilor enumerate este asistența în identificarea potențialelor surse de date și a colaboratorilor.
- **EPIRARE** (http://www.epirare.eu) (The European Platform for Rare Disease Registries) este o alta initiativa europeana privind bolile rare.
- The European Register for Multiple Sclerosis (**EUReMS**) Registrul pentru scleroza multiplă.
- EU-ADR (http://www.euadr-project.org) a fost un proiect finanțat de CE (Programul PC7), cu obiectivul de a proiecta, dezvolta și valida un sistem computerizat care exploatează date din înregistrările medicale electronice și bazele de date biomedicale pentru detectarea reacțiilor adverse la medicament (ADR). În acest proiect, au fost disponibile înregistrări electronice de sănătate (EHR) care includ date demografice, consumul de droguri și date clinice de peste 30 de milioane de pacienți din mai multe țări europene. Bazele de date ale EHR formează, de asemenea, fundamentul proiectului, în măsura în care acestea furnizează datele pacientului pe lângă care este construit sistemul. Sistemul UE-ADR a urmărit atunci să genereze semnale (perechi de droguri-evenimente de interes de farmacovigilență) prin utilizarea tehnicilor de extragere a datelor și a tehnicilor epidemiologice, computaționale și text mining . În final, obiectivul final al proiectului a fost acela de a demonstra că o detectare mai rapida a reactiilor adverse(ADR-urilor) este posibilă prin utilizarea EHR.
- Un alt exemplu de initiativa a CE fiind HoNCAB (http://honcab.eu) - o rețea pilot de spitale referitoare la plata pentru îngrijirea pacienților transfrontalieri, cu obiectivele principale de stabilire a drepturilor pacienților în condițiile de acces la asistență medicală transfrontalieră și dreptul la rambursarea unui astfel de tratament, pentru a asigura accesul și furnizarea unei asistențe medicale sigure, de înaltă calitate, eficiente și cantitative corespunzătoare în străinătate, pentru a sprijini colaborarea dintre statele membre în ceea ce privește asistența medicală și, înțelegerea cerințelor financiare și organizatorice care pot apărea ca urmare a unui pacient care primește asistență medicală în afara afilierii SM. Rețeaua de spitale are o structură organizațională funcțională și mijloace de comunicare stabilite, susținute de o bază de date bazată pe web pentru colectarea și schimbul de informații, toate cu scopul de a împărtăși experiențele practice ale statelor membre, problemele și soluțiile legate de îngrijirile transfrontaliere.

Lista de standarde minime aplicabile:

Metadate
- ISO/CEN Metadata standard 11179
- Dublin Core MetadataSt

Structura de date/Schimb de date
- OpenEHR
- HL7 RIM CDA, C-CDA
- HL7 FHIR
- I2b2
- ISO/CEN 13606
- IHE
- Clinical information modelling initiative

Terminologie
- CTS2 standard
- IHTSDO SNOMED-CT
- ICD10
- LOINC
- ATC
- ICPC-2
- ICF
- ICHI
- DRG

Ontologie
- OWL

Pharma si cercetare
- C-DISC
- BRIDG

Integrare cu DES

a. Sumar pentru situații de urgență, cu date medicale vitale
   - alergii si intoleranțe
   - proteze și alte dispozitive medicale interne
   - transplanturi
   - proceduri medicale relevante pentru urgență
   - fistula arterio-venoasa (existența acesteia)
   - boli cronice
   - boli hematologice relevante pentru urgență
   - boli transmisibile relevante pentru urgență
   - tratamente curente
   - internări recente

b. Istoricul medical complet
   - alergii si intolerante diagnosticate
   - boli cronice diagnosticate
   - istoricul de boli/diagnostice (altele decât alergii si cronice)
   - intervenții si proceduri efectuate
   - servicii medicale
   - imunizări
   - tratament medicamentos acordat în cadrul unor studii clinice

c. Antecedente declarate medicului de pacient
   - Antecedente heredo - colaterale
   - Antecedente fiziologice

- Antecedente patologice
- Mod de viață

d. Documente medicale primite
- Fișa de observație clinică generală pentru spitalizare continuă
- Fișa de observație clinică generală pentru spitalizare de zi - prezentare vizită
- Fișa consultație medic specialist
- Fișă de consultație medicină de familie
- Trimiteri pentru investigații clinice
- Trimiteri pentru investigații paraclinice
- Recomandări pentru îngrijiri la domiciliu
- Recomandări pentru dispozitive medicale
- Rețete prescrise de medici
- Rețete eliberate de farmacii

Date ce pot fi transmise in DES:

DATE
1. Prezentare la internare - spitalizare continuă (non urgenţă)
Datele/Informaţiile sunt transmise în DES în ziua internării din foaia de observaţie clinică generală şi sunt:
a) date de identificare pacient*;
b) date privind internarea*;
c) trimitere spre internare.
2. Extras fişă de spitalizare continuă
Datele/Informaţiile sunt transmise în DES la data externării din foile de observaţie clinică generală/biletele de ieşire din spital şi sunt:
1. date de identificare pacient*;
2. detalii episod de spitalizare*;
3. trimitere spre internare;
4. diagnostice*;
5. stare prezentă la internare;
6. istoricul bolii actuale;
7. antecedente:
a) antecedente heredo-colaterale;
b) mod de viaţă;
c) antecedente fiziologice adult femeie;
d) antecedente fiziologice copil;
e) antecedente personale patologice;
8. proceduri medicale efectuate;
9. detalii naştere;
10. servicii şi investigaţii clinice, paraclinice şi spitaliceşti;
11. monitorizare semne vitale;
12. imunizări;

DATE
13. tratament medicamentos;
14. tratament medicamentos acordat în cadrul unor studii clinice;
15. alte probleme identificate:
a) boli cronice;
b) alergii;
16. tratament medicamentos recomandat;
17. servicii şi investigaţii recomandate:
a) trimitere clinică;
b) trimitere paraclinică;
c) trimitere recomandare îngrijire la domiciliu;
d) trimitere recomandare dispozitive medicale;
18. bilet de externare*;
19. scrisoare medicală*.
3. Extras fişă de spitalizare de zi - prezentare vizită
Datele/Informaţiile sunt transmise în DES din fişa de spitalizare de zi, la fiecare vizită/zi, şi sunt:
1. date de identificare pacient*;
2. antecedente:
a) antecedente heredo-colaterale;
b) mod de viaţă;
c) antecedente fiziologice adulţi;
d) antecedente fiziologice copii;
e) antecedente personale patologice;
3. detalii episod de spitalizare*;
4. trimitere spre internare;
5. diagnostice*;
6. detalii vizită*;
7. proceduri medicale efectuate;
8. servicii şi investigaţii clinice, paraclinice şi spitaliceşti;
9. imunizări;
10. tratament medicamentos în cadrul vizitei;
11. alte probleme identificate:
a) boli cronice;
b) alergii;
12. tratament medicamentos recomandat;
13. tratament medicamentos acordat în cadrul unor studii clinice;
14. servicii şi investigaţii recomandate:
1. trimitere clinică;
2. trimitere paraclinică;
3. trimitere recomandare îngrijire la domiciliu;

DATE
4. trimitere recomandare dispozitive medicale;
15. bilet de externare*;
16. scrisoare medicală*.
4. Fişă consultaţie la medicii de specialitate din specialităţile clinice
Datele/Informaţiile sunt transmise în DES în ziua acordării consultaţiei şi sunt:
1. date de identificare pacient*;
2. date privind consultaţia sau investigaţia*;
3. antecedente:
a) antecedente heredo-colaterale;
b) mod de viaţă;
c) antecedente fiziologice adulţi;
d) antecedente fiziologice copil;
e) antecedente personale patologice;
4. trimitere clinică în baza căreia se face consultaţia;
5. consemnarea examenelor periodice - copii;
6. istoricul bolii curente;
7. servicii clinice şi paraclinice efectuate;
8. imunizări;
9. tratament medicamentos administrat în ambulatoriu;
10. tratament medicamentos acordat în cadrul unor studii clinice;
11. alte probleme identificate:
a) boli cronice;
b) alergii;
12. tratament medicamentos recomandat în urma consultaţiei;
13. servicii şi investigaţii recomandate în urma consultaţiei:
a) bilet de trimitere către o specialitate clinică/internare;
b) bilet de trimitere către o specialitate paraclinică;
c) bilet de trimitere îngrijire la domiciliu;
d) bilet de trimitere dispozitive medicale;
5. Fişă de consultaţie medic de familie
Datele/Informaţiile sunt transmise în DES în ziua acordării consultaţiei şi sunt:
1. date de identificare pacient*;
2. date privind consultaţia sau investigaţia*;
3. antecedente:
a) antecedente heredo-colaterale*;
b) mod de viaţă;
c) antecedente fiziologice adult femeie;
d) antecedente fiziologice copil;
e) antecedente personale patologice;
4. trimitere clinică în baza căreia se face consultaţia;
5. consemnarea examenelor periodice - copii;

DATE
6. istoricul bolii curente;
7. servicii clinice şi paraclinice efectuate;
8. imunizări;
9. tratament medicamentos administrate în ambulatoriu;
10. tratament medicamentos acordat în cadrul unor studii clinice;
11. alte probleme identificate;
a) boli cronice;
b) alergii;
12. tratament medicamentos recomandat în urma consultaţiei;
13. servicii şi investigaţii recomandate în urma consultaţiei;
a) bilet de trimitere către o specialitate clinică/internare;
b) bilet de trimitere către o specialitate paraclinică;
c) bilet de trimitere îngrijire la domiciliu;
d) bilet de trimitere dispozitive medicale.
6. Bilet de trimitere către o specialitate clinică/internare
Datele/Informaţiile sunt transmise în DES în ziua întocmirii biletului şi sunt:
1. date identificare pacient*;
2. bilet de trimitere către o specialitate clinică/internare*.
7. Bilet de trimitere către o specialitate paraclinică
Datele/Informaţiile sunt transmise în DES în ziua întocmirii biletului şi sunt:
1. date identificare pacient*;
2. bilet de trimitere către o specialitate paraclinică*.
8. Bilet de trimitere pentru îngrijiri la domiciliu
Datele/Informaţiile sunt transmise în DES în ziua întocmirii biletului şi sunt:
1. date identificare pacient*;
2. bilet de trimitere pentru îngrijiri la domiciliu*.
9. Bilet de trimitere - prescripţie pentru dispozitive medicale în ambulatoriu
Datele/Informaţiile sunt transmise în DES în ziua întocmirii biletului şi sunt:
1. date identificare pacient*;
2. bilet de trimitere - prescripţie pentru dispozitive medicale*.
10. Prescripţie medicală

Pentru interoperabilitatea registrelor se va utiliza cadrul European de Interoperabilitate pentru sănătate:
https://ec.europa.eu/digital-single-market/news/ehealth-interoperability-framework-study-0
Se vor aplica principiile stabilite de proiectul **Cross-border Patient Registries Initiative**:

La definirea registrelor se vor utiliza acele standarde care permit interoperabilitatea prescriptiei si a sumarului pacientului.

Planificarea interoperabilității

Având în vedere că "interoperabilitatea este posibilă prin punerea în aplicare a standardelor", este esențială legătura cu autoritățile naționale de reglementare / îmbunătățire a calității, care poate constitui o sursă valoroasă de consiliere cu privire la accesul și utilizarea adecvată a standardelor relevante. O relevanță deosebită din perspectiva dezvoltării registrelor este selectarea seturilor de date standard și a terminologiei pentru a facilita interoperabilitatea locală și transfrontalieră. Pentru zonele generale, cum ar fi demografia, initiativa europeana PARENT este o excelentă sursă de orientare în ceea ce privește seturile de date standard și terminologie sau pentru a facilita contactul cu un registru dintr-un alt stat, cu o structură și o compoziție care poate fi adaptată sau adoptată pentru nevoile unui nou registru. La nivel național, organismele de reglementare vor putea, în mod tipic, să consilieze utilizarea optimă a sistemelor de clasificare, cum ar fi Clasificarea Internațională a Bolilor (ICD) a Organizației Mondiale a Sănătății (OMS) sau terminologii cum ar fi Nomenclatorul Sistematizat al Organizației pentru Dezvoltarea Terminologiei Sănătății (IHTSDO) al termenilor clinici de medicină (SNOMED CT®). Pentru zone mai specifice, grupurile clinice profesionale naționale sau internaționale pot fi o sursă bogată de informații. Un scop al interoperabilității este acela de a preveni blocarea datelor potențial valoroase în "silozuri" de informație și de a facilita reprezentarea mai precisă a conceptelor și a compararii datelor la nivel transfrontalier.

2.1.1. Beneficiarii sistemului informatic

Sistemul va susține activitatea următoarelor grupuri de beneficiari/utilizatori:

- administratori procese operationale de la nivelul Ministerului Sănătăţii care vor defini si administra registrele;
- utilizatori de la nivelul Ministerului Sănătăţii care vor putea vizualiza lista de pacienţi înscrişi în registru, statistici şi rapoartele specifice;
- furnizorii de servicii medicale (medici) cu dreptul de a introduce informaţiile despre pacienţi şi de a vizualiza rapoartele specifice;
- cetateni – vor vizualiza propriile date si pot participa activ la actualizarea datelor – asa cum este definit de furnizorul de servicii.

2.1.2. Informații cantitative

Sistemul va fi dimensionat pentru a face față următoarelor caracteristici legate de volumetria grupului țintă curent:

- 55.000 medici;
- 2.000.000 de pacienti;
- 300 - administratori procese operationale.

Dinamica datelor:

- In cadrul programelor nationale de sanatate se preconizeaza a fi inregistrati 1.500.000 de pacienti, cu o crestere ulterioara de 500.000 de inregistrări pe an.
- Registrele actuale pe specialități contin in momentul actual intre: 1.000 și 15.000 de pacienți intr-un registru (de exemplu: Epidermoliza buloasa 1.080 pacienti, Registrul National de Boli Cardiace Congenitate copii si adulti 4.000, Infectii sexual transmisibile 15.000). Creșterea anuală a numărului de pacienți intr-un registru fiind intre: 1.000-15.000 pe an (de exemplu: Registrul National de Boli Cardiace Congenitate copii si adulti 1.000, Infectii sexual transmisibile 13.000)

2.2. *PREVEDERI DE SECURITATE*

Sistemul trebuie să asigure protecția datelor pe tot parcursul ciclului de viață al acestora: creare, modificare, stocare, transport și distrugere.
Componentele sistemului informatic propus trebuie să fie protejate împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le înmagazinează. Astfel, sistemul informatic trebuie să asigure:

- Securitatea datelor printr-un sistem de limitări ale accesului la aplicaţie bazat pe drepturi şi parole, defalcat pe mai multe niveluri. Drepturile de acces ale utilizatorilor vor putea fi configurate de administratorii sistemului din interfaţa aplicaţiei;
- Autentificarea utilizatorilor externi trebuie să fie permisa de la orice staţie de lucru conectata la Internet, atât timp cât aceasta nu se află într-o zonă pentru care accesul a fost restricţionat din motive de securitate;
- Împiedicarea utilizatorilor de a se conecta la sistem dacă acesta este în incapacitate temporară de a asigura securitatea datelor sau există suspiciuni că mecanismele de protecţie au fost compromise;
- Schimbul de date si atribute cu nodul national eIDAS conform regulamentului CE 910/2014;
- Închiderea automata a sesiunilor de lucru ale utilizatorilor în caz de inactivitate pe o anumita durata predeterminata de timp, pentru a proteja dezvăluirea accidentală a informaţiilor către alte persoane care nu sunt autorizate să le primească;
- Jurnalizarea operaţiilor zilnice la nivelul aplicaţiei, individual pentru fiecare utilizator cu drept de acces la modificarea înregistrărilor, cu marcarea orei la care a fost executata fiecare operaţie precum şi a identităţii utilizatorului care a iniţiat-o;
- Stabilirea unei sesiuni de lucru va consta în operaţiunea de autentificare (login) a utilizatorului curent în aplicaţie; autentificarea unică a utilizatorilor şi autorizarea acestora se vor realiza o singura data pe sesiune;
- Securitate de perimetru - prin implementarea unui sistem de tip firewall care va proteja reţeaua interna de trafic nedorit.

Soluţia de securitate proiectată trebuie să asigure confidenţialitatea transferului de informaţii. Informaţia dintr-un astfel de sistem trebuie protejată împotriva ameninţărilor în orice situaţie, fie când este stocată, fie când este transportată.
Instrumentele proiectate pentru asigurarea confidenţialităţii datelor trebuie să asigure accesul utilizatorilor sistemului prin intermediul protocolului securizat HTTPS, folosind certificate digitale calificate, pentru a elimina posibilele încercări de interceptare a datelor când sunt transmise prin mediile de comunicaţie.
La construirea soluției de securitate se va avea în vedere asigurarea conformității cu cerințele cuprinse in: Regulamentul UE 910/2014, Regulamentul UE 2015/1502, Directiva UE 2016/1148, Regulamentul UE 2016/679 (GDPR).

2.2.1. Autentificare si acces

Sistemul informatic propus trebuie să pună la dispoziţia administratorilor o componentă pentru controlul accesului utilizatorilor interni sau externi la funcţiile aplicative ale sistemului informatic, pe baza drepturilor de acces specifice pentru fiecare categorie sau grup de utilizatori.
Este necesar ca soluţia tehnică să implementeze cel puţin următoarele funcţionalităţi:

- Posibilitatea restricţionării accesului utilizatorilor privilegiaţi la datele manipulate de aplicaţiile de business, prin segregarea responsabilităţii.
- Soluţia va permite autentificarea furnizorilor de servicii medicale şi a altor persoane autorizate pe baza certificatelor digitale calificate sau a sistemului nume-parola-OTP.

Pentru orice beneficiar sistemul va permite, conform regulamentului EIDAS 910/2014, atributele specificate de acest regulament.

Pentru acces sistemul trebuie să poată opera cu următorul set minim de date pentru o persoană fizică, care conține toate atributele obligatorii de mai jos:

a) numele de familie actual(e);
b) prenumele actual(e);
c) data nașterii;
d) un identificator unic, care este alcătuit de către statul membru expeditor în conformitate cu specificațiile tehnice privind identificarea transfrontalieră și care are o durată de viață cât mai mare.

Setul minim de date pentru o persoană fizică poate conține unul sau mai multe din atributele suplimentare de mai jos:

a) prenumele și numele de familie la naștere;
b) locul nașterii;
c) adresa actuală;
d) sexul.

Pentru acces sistemul trebuie să poată opera cu următorul set minim de date pentru o persoană juridică, care conține toate atributele obligatorii de mai jos:

a) denumirea oficială actuală;
b) un identificator unic, care este alcătuit de către statul membru expeditor în conformitate cu specificațiile tehnice privind identificarea transfrontalieră și care are o durată de viață cât mai mare.

Setul minim de date pentru o persoană juridică poate conține unul sau mai multe din atributele suplimentare de mai jos:

a) adresa actuală;
b) codul de înregistrare în scopuri de TVA;
c) codul de identificare fiscală;
d) identificatorul care are legătură cu articolul 3 alineatul (1) din Directiva 2009/101/CE a Parlamentului European și a Consiliului;
e) identificatorul entității juridice (LEI) menționat în Regulamentul de punere în aplicare (UE) nr. 1247/2012 al Comisiei;
f) numărul de înregistrare și identificare a operatorilor economici (EORI) menționat în Regulamentul de punere în aplicare (UE) nr. 1352/2013 al Comisiei;
g) codul de acciză prevăzut la articolul 2 alineatul (12) din Regulamentul nr. 389/2012 al Consiliului

Specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare

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

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

4. „sistem de management al securității informațiilor” înseamnă un set de procese și proceduri menite să gestioneze la niveluri acceptabile riscurile legate de securitatea informațiilor.

Sistemul va folosi urmatoarele nivele de incredere:

- Nivelul minim de autentificare in sistem va fi: **substanțial conform Regulamentului 910/2014**

Se va introduce autentificarea cu 2 factori. Se va implementa autentificarea folosind doi factori de autentificare, respectiv nume și parolă și o modalitate suplimentară de tip one-time-password, prin SMS, mail sau folosind o aplicație mobilă. În procesul de obținere a datelor de acces se va asigura că utilizatorii sunt înscriși atât cu numele și parola dar și cu numărul de telefon mobil.

- Nivel **ridicat de autentificare in sistem conform Regulamentului 910/2014**

Pentru medici sau cetateni care au un certificat calificat valid se va introduce autentificarea folosind certificate digitale calificate astfel încât toți utilizatorii să acceseze sistemul în mod securizat corespunzător.

2.2.2. Confidențialitatea datelor

Confidențialitatea este o cerinta de bază pentru furnizarea serviciilor publice.

In cadrul proiectului se vor respecta urmatoarele principii:

- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că respectă cerințele și obligațiile juridice privind **protecția și confidențialitatea datelor** recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

De asemenea, trebuie să asigure respectarea de către operatori a legislației privind protecția datelor, prin:

- **„Planuri de gestionare a riscurilor”** pentru identificarea riscurilor, evaluarea potențialului impact al acestora și planificarea intervențiilor cu măsuri tehnice și organizatorice adecvate. Pe baza ultimelor evoluții tehnologice, aceste măsuri trebuie să asigure un nivel de securitate proporțional cu gradul de risc;
- **„Planuri de continuitate a activității”** și **„planuri de rezervă și de redresare”** pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucerea tuturor funcțiilor la situația normală cât mai curând posibil;
- Un **„plan de acces la date și autorizare”** care stabilește persoanele care au acces la date, datele care sunt accesibile și condițiile accesării datelor, pentru a asigura confidențialitatea. Accesul neautorizat și încălcarea normelor de securitate trebuie monitorizat, și măsurile corespunzătoare pentru a preveni orice repetare a încălcărilor trebuie documentate si planificate;
- Utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS[1] pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

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

- Securitate adecvată – protecția împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri tehnice sau organizatorice;
- Protecția datelor cu caracter personal care dezvăluie originea rasială sau etnică, confesiunea religioasă şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice;
- Pseudonimizare și criptare – prelucrarea datelor cu caracter personal în zona de testare într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizată, fără a se utiliza informații suplimentare;

[1] Regulamentul (UE) nr. 910/2014.

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

3. DESCRIEREA TEHNICĂ A PROIECTULUI

3.1. *CERINŢELE FUNCŢIONALE ALE SISTEMULUI*

Proiectul RegInterMed presupune implementarea unui sistem informatic nou, actualizat la nivelul de evoluție tehnologică, cu o securitate informatică sporită și pentru care, la proiectarea, realizarea și implementarea sistemului informatic, trebuie să se țină cont de următoarele principii generale:

- **Principiul legalității**: care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- **Principiul divizării arhitecturii pe nivele:** constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
- **Principiul arhitecturii bazate pe servicii:** constă în distribuirea funcționalității aplicației în unități mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic;
- **Principiul destinației strategice** - asigurat de faptul că autoritățile centrale și locale pot avea date și informații exacte și necesare pentru dezvoltarea eficientă a politicilor de asistență socială;
- **Principiul datelor sigure**: stipulează introducerea datelor în sistem doar prin canale autorizate și autentificate;
- **Principiul securității informaționale**: presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și acces nesancționat;
- **Principiul transparenței**: presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
- **Principiul expansibilității**: stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
- **Principiul scalabilității**: presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;
- **Principiul simplității și comodității utilizării**: presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor Sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
- **Principiul integrității, plenitudinii și veridicității datelor:** presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business ale sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte dintr-un sector concret al sistemului informatic.

3.1.1. Cerinte functionale

Sistemul va utiliza nomenclatoare sistematizate/standardizate pentru medicină, astfel încât să permită interoperabilitatea registrelor la nivel european.
În această secţiune sunt detaliate cerinţele funcţionale minime obligatorii pe care soluţia tehnică trebuie să le îndeplinească pentru realizarea aplicaţiei informatice, pentru ca aceasta să atingă obiectivele asumate.
Sistemul va utiliza aceleaşi categorii de date existente în sistemele informatice ale CNAS (nomenclatoare, asiguraţi, registre de servicii medicale şi farmaceutice, registre de furnizori de servicii medicale, etc) în măsura în care aceastea sunt standardizate (ex ICD, DICOM, SNOMED, LOINC etc). Accesul la aceste categorii de date se va face programatic.

Accesul la aceste categorii de date se va face programatic. Se face migrarea datelor din registrele existente deja, acolo unde este posibila această operație.

Sistemul este proiectat să funcţioneze în mod ONLINE si nu va fi proiectat pentru a memora imagistica (radiografii, RMN etc.).

Proiectele pe domeniul e-sanatate încearcă în prezent să definească funcțiile minime pe care un EHR (Electronic Health System) ar trebui să le îndeplinească pentru a ajuta medicii să practice o medicina moderna.

Unele dintre aceste funcții includ, dar nu se limitează, la urmatoarele cerințe functionale:

- Identificare pacient si datele demografice ale pacientului
- Gestionare listele de probleme de sanatate ale pacientului
- Gestionare listele de medicamente
- Gestionare istoricul pacientului
- Gestionare documente și note clinice
- Documente clinice externe
- Planuri de îngrijire actuale, orientări și protocoale
- Gestionare orientări, protocoale și planuri de îngrijire specifice pacienților
- Instrucțiuni specifice pentru pacient

Se vor dezvolta formulare electronice similare unor formularele de hârtie. Formularele vor fi salvate într-o bibliotecă și pot fi adesea folosite în mai multe protocoale. Aceasta elimină necesitatea de a recrea formularele utilizate în mod obișnuit și de a promova standardele de date. Când se creează formulare, se pot programa controale de editare pentru a preveni introducerea datelor nevalide. Acest lucru va asigura asigura că valorile introduse îndeplinesc anumite cerințe.

Introducerea datelor. Datele colectate se vor putea introduce în formularele corespunzătoare dezvoltate pentru fiecare registru.

Soluția va asigură o comunicare raționalizată in funcție de roluri pentru utilizatorii sistemului. Solutia va putea genera automat interogari și va permite realizarea manuală de interogări. Toate interogările vor trebuie să permită utilizarea de roluri înainte ca datele să poată fi deblocate.

HL7 - Lista funcțiilor EHR. Sistemul informatic va:

- Permite identificarea și actualizarea înregistrării pacienților - o singură înregistrare a pacientului pentru datele sale specifice.
- Permite prelucrarea datelor demografice ale pacientului – pentru datele care ar sunt relevante din punct de vedere clinic pentru care este necesar să fie raportabile și să poată fi urmărite în timp.
- Permite gestionarea unor liste de probleme - liste de probleme specifice fiecărui pacient.
- Permite gestionarea unor liste de medicamente - liste de medicamente specifice pacienților.
- Permite vizualizarea istoricului pacientului - istoricul medical / chirurgical, istoricul social și familial, inclusiv capturarea istoricelor pozitive și negative relevante, istoricul clinic al pacienților raportat sau extern.
- Permite gestionarea de note clinice - transcrierea sau introducerea directă a documentației și notelor clinice.
- Furnizeaza instrumentele administrative pentru pentru a construi planuri de îngrijire, orientări și protocoale pentru a fi utilizate în planificarea și îngrijirea pacientului.
- Generarea și înregistrarea instrucțiunilor specifice pacientului - Generarea și înregistrarea instrucțiunilor specifice pacientului referitoare la cerințele pre- și post-procedurale.
- Plasarea comenzilor de îngrijire a pacientului - Captură și urmărirea comenzilor pe baza datelor furnizate de furnizorii de îngrijire speciali.
- Permite gestionarea rezultatelor - Diseminarea, gestiunea și prezentarea rezultatelor/ testelor curente și istorice către personalul clinic adecvat pentru examinare, cu capacitatea de a filtra și compara rezultatele.

- Permite gestiunea automata a formularelor de consimțământ și autorizații - Crearea, mențineținera și verificarea deciziilor de tratare a pacienților sub formă de consimțământ și autorizații atunci când este necesar.
- Suport pentru serviciile medicale necesare evaluărilor pacienților - Oferă solicitări de sprijinire a aderării la planurile de îngrijire, orientări și protocoale la punctul de captare a informațiilor.

Registrele de boală

Înregistrarea furnizorilor de servicii medicale

Această funcţionalitate permite introducerea informaţiilor despre furnizorii de servicii medicale care vor avea acces la Registrele naţionale de boli pentru gestionarea acestora la nivel de categorie de boala.

Date de identificare furnizor:

a. cod şi nume unitate sanitară;
b. cod şi denumire secţie;
c. cod şi denumire judeţ;
d. cod şi denumire localitate;
e. nume şi prenume medic specialist;
f. specialitate medic;
g. cod parafă medic

Datele de mai sus vor fi definitivate în etapa de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu medicii coordonatori ai fiecărui registru de boală.

Beneficiarii acestui serviciu online vor fi în primul rând furnizorii de servicii medicale (medici specialişti), care vor avea acces la un mijloc modern şi rapid de introducere a informaţiilor referitoare la pacienţi. De asemenea, alt beneficiar este Ministerul Sănătăţii, care va avea acces la rapoarte bazate pe informaţii complete si coerente privind pacienții.

Avantajele utilizării serviciului online de înregistrare furnizori de servicii medicale:

- vor avea la dispoziţie un mijloc modern şi rapid de completare şi actualizare a datelor pentru conectare la Registrul naţional de boli

Lista pacienţilor cuprinşi în registrul naţional

Pentru a facilita accesul la informaţiile existente în baza de date, aplicaţia va permite afişarea unei liste de pacienţi.

Datorită volumului mare de informaţii lista se va afişa în urma unei operaţii de filtrare. Filtrarea se va putea face după informaţiile de identificare a pacientului, ca de exemplu: nume, prenume, CNP/CID, data naşterii, unitatea medicală, data luării în evidenţă sau alte elemente care vor fi stabilite în timpul etapei de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu medicii coordonatori ai fiecărui registru de boală.

Motorul de căutare va fi accesibil în momentul accesării opţiunii Pacienţi din meniul principal

De asemenea, pentru a uşura căutarea în interiorul listei va exista posibilitatea sortării informaţiei.

Beneficiarii acestui serviciu sunt medicii şi angajaţii MS.

Avantajele utilizării serviciului atât pentru furnizorii de servicii medicale cât şi pentru angajaţii MS:

- accesul rapid la informaţii prin intermediul rapoartelor puse la dispoziție de sistemul informatic
- imagine clară şi completă asupra datelor statistice despre pacienţinecesare elaborării politicilor publice

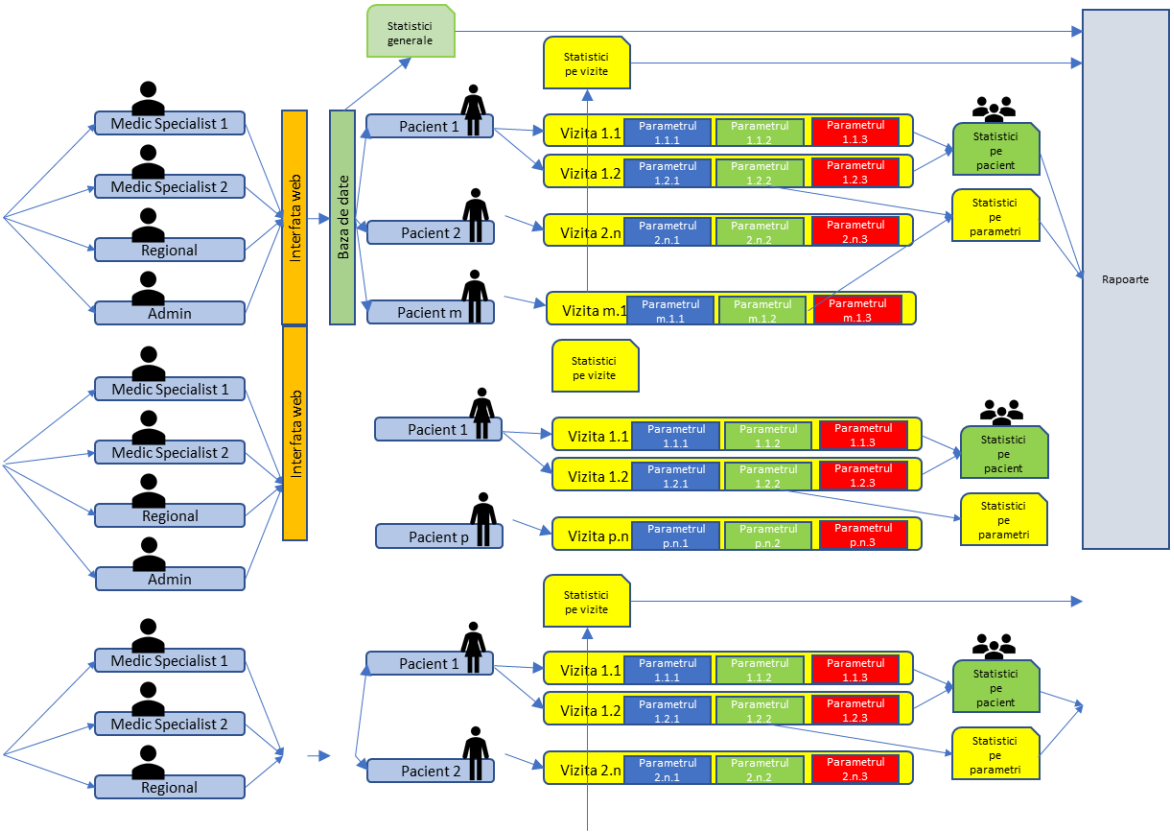
Înregistrare online a pacienţilor

Această funcţionalitate este specifică furnizorilor de servicii medicale care se află înregistraţi în lista de furnizori de servicii medicale a sistemului.

Prin înregistrarea online a pacienţilor, se va furniza medicilor specialişti un mecanism online, modern şi uşor de utilizat pentru accesul la informaţia din registrul naţional. Astfel, înregistrarea online a pacienţilor va permite introducerea informaţiilor medicale specifice registrului naţional specific.

Propunere pentru continutul registrului: registrul trebuie sa contina minim, pentru fiecare pacient, urmatoarele:

- Date de identificare pacient, diagnostice
- Evenimente - inclusiv vizite medicale
- Scrisoarea medicală: raportul vizitei, raportul de evolutie a pacientului pe parcursul tuturor vizitelor anterioare.



Informaţiile vor fi structurate pe grupe de date:

1. Date de identificare pacient:
    - CNP/CID
    - nume
    - prenume
    - sex
    - varstă
    - data naşterii,
    - locul naşterii,
    - denumire localitate de domiciliu
    - sector de domiciliu,
    - denumire judeţ de domiciliu,
    - motivul de înregistrare.
    - date antropometrice
2. Date referitoare la boală:
    - data diagnosticarii initiale
    - tipul bolii
    - Cum a debutat boala
    - Forma de boala

- Factori de risc
  - Istoric familial
  - traumatisme (de orice fel, la orice vârstă)
  - expunere toxice (de orice fel)
- statusul bolii
  - aspecte motorii
  - aspecte non-motorii
- calitatea vieții
  - scoruri / scale de evaluare

3. Date referitoare la evoluţia şi tratamentul bolii:
   - Servicii medicale acordate pe perioada internărilor
   - Tratament simptomatic motor
   - Tragtament simptomatic non-motor
   - Complicaţiile tratamentului
   - Data şi motivul de deces

Datele prezentate mai sus constituie structura setului minim de date necesar pentru înregistrarea unui pacient într-un Registrul Naţional. Acest set de date va fi definitivat în etapa de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu medicii coordonatori ai fiecărui registru de boală.

Sistemul va permite adăugarea de pacienţi noi sau modificarea datelor unui pacient existent.

Sistemul va permite implicarea pacientului de la distanță pentru a economisi timp, pentru a lucra excelent în mediile mobile și a încuraja colaborarea mai bună. Pentru un act medical bazat pe evidențe și centrat pe pacient, registrele vor conține informatii importante pentru pacienți astfel incât furnizorii de servicii medicale să poată lua decizii cât mai informate în materie de asistență medicală. Implicarea pacienților are ca scop implementarea unui intrument care asigură măsurarea rezultatelor care sunt vizibile și importante pentru pacienți si care ajută la o mai mare vizibilitate a valorii asistenței medicale.

Beneficiarii acestui serviciu online vor fi în primul rând furnizorii de servicii medicale (medici specialişti), care vor avea la dispoziţie un mijloc modern şi rapid de introducere a informaţiilor în baza de date. De asemenea, celălalt beneficiar este Ministerul Sănătăţii, care va avea acces la o informaţie completă şi coerentă referitoare la pacienţii. Pacienții sunt de asemenea beneficiarii registrelor. Prin implementarea unor instrumente adaptate dispozitivelor mobile se urmărește îmbunătățirea participării pacienților, motivarea acestora pentru utilizarea registrelor. Nu în ultimul rând pe baza evidențelor se preconizează descoperirea de noi modele care vizează mai bine populațiile și / sau se aliniază mai bine cu utilizare în lumea reală.

Statistici si rapoarte

Sistemul va permite constituirea unei baze de date completă şi coerentă ce va conţine informaţii despre pacienţii, tratamentele aplicate si evoluţia bolii, informaţii pe baza cărora se vor putea defini rapoarte si statistici referitoare la apariţia bolii, la nivelul tuturor segmentelor populaţiei.

Statisticile şi rapoartele dorite vor fi definite în cadrul etapei de analiză.

Analiza geospatiala

Se va dezvolta o platformă WEB pentru preluarea datelor din bazele de date la nivel de registru medical și transpunerea acestora în hărți tematice care să figureze geografic datele din registre. Hărțile vor reprezenta grafic cazurile pe coduri de culoare la nivel de județe și la nivel de localități (Unități Administrativ Teritoriale). Limitele Unitățile Administrativ Teritoriale vor fi delimitate pe hartă astfel încât la un nivel de zoom la nivelul unui județ, cazurile raportate să poată fi figurate foarte clar la nivelul localităților componente.

Cazurile raportate pe fiecare registru vor fi figurate geografic atât sintetic (pe coduri de culoare) cât și analitic (număr de cazuri filtrate după parametrii asociați cazului). Pentru ambele modalități de figurare, se va putea filtra după perioada de timp a raportării.

Beneficiarul prin atribuțiile sale monitorizează permanent starea de sănătate publică în ceea ce privește riscurile medicale cu potential de propagare în societate, de aceea urmărește implementarea unor mecanismle informatice pentru înregistrarea rapidă în sistem a primelor semne specifice aparițiilor acestora, monitorizarea evoluției și a caracteristicilor fenomenelor medicale infecțioase, monitorizarea măsurilor de intervenție și a rezultatelor obținute.
Monitorizarea eficientă a propagării fenomenelor medicale se poate realiza prin instalarea în cadrul sistemului informatic a unui modul geospatial care să permită următoarele fucționalități de bază:

- Fundal geografic uzual: imagini aeriene, elemente de relief, infrastructura rutieră, elemente urbane, elemente de transport;
- Reprezentarea ariei de monitorizarea și a detaliilor de bază, astfel: locațiile unităților spitalicești și a celor de natură medicală: cabinete medicale, clinici medicale, alte instituții medicale cu flux de pacienți; locațiile marilor aglomerări publice urbane: piețe publice, gări, stații de metrou, mari centre comerciale, unități de învățământ;

Modulul geospațial trebuie să înglobeze mecanisme pentru raportarea prin intermediul echipamentelor mobile de tip smarphone/tablete sau de tip PC, de către personal autorizat a apariției evenimentelor medicale cu potential de propagare – **early warning.** Deasemenea evenimentele tip early warning trebuie să fie posibile și prin integrarea cu alte sisteme medicale de specialitate (software pentru internările din spitale pentru evenimentele infecțioase-epidemiologice), prin preluarea evenimentelor de natură infecțios-epidemiologice cu potential de propagare și a caracteristicilor inițiale: localizarea apariției evenimentului, tipul sursei, dominiciul și parcursul acestuia până la depistarea evenimentului.
Prin intermediul modului geospațial Beneficiarul va avea acces la o hartă actualizată privind starea focarelor, distribuția geografică, atât din punctul de vedere al locațiilor unde au fost raportate, dar și al locurilor de provenire al surselor/pacienților. În felul acesta, în cadrul modului geospațiale vor exista suficiente date statistice și obiecte georeferențiate care să permită realizarea de analize și simulări privind propagarea pe unități de timp, zone geografice și în funcție de fluxurile uzuale de trafic (persoane). Modulul geospațial trebuie să permită definirea de scripturi pentru realizarea acestor analize și vizualizarea dinamică a rezultatelor, prin reprezentări heatmaps și comparații vizuale sincronizate pe seturile de date, la momente de timp diferite.
Modulul geospațial trebuie să permită încărcarea de hărți de bază, definerea de straturi grafice pe care să poată fi încărcate obiecte georeferențiate precum cele enumerate mai sus (evenimente epidemiologice, locații, caracteristice, algoritmi de propagare și efecte), înregistrarea de scripturi pentru obținerea analizelor și să conțină instrumente pentru vziualizarea rezultatelor într-o manieră interactivă. Deasemenea, rezultatele trebuie să fie expuse în formate și servicii web.
Folosind instrumentele puse la dispoziție în cadrul modului geospațial, Beneficiarul trebuie să fie capabil să evalueze obiectiv gradul de severitate al epidemiilor, să identifice correct comunitățile afectate și cele ce pot fi afectate în eșantioane de timp, ținând cont de viteze și modelele de propagare ale diverselor categorii de epidemii. Monitorizarea acțiunilor privind limitarea efectelor epidemiilor, dar și planurile continue sau periodice de prevenție trebuie să poată fi gestionate prin intermediul aplicației de fată.
Beneficiarii acestui serviciu sunt cetăţenii, furnizorii de servicii medicale.
Avantajele utilizării serviciului:

- pentru cetăţeni:
  - existenţa unei baze centralizatoare a tuturor pacienţilor, şi statisticile care sunt extrase de aceasta, pot furniza date concrete, şi intr-un mod eficient, în sprijinul unor decizii în beneficiul pacienţilor. Ajută în timp, la estimarea mai bună a necesităţilor reale şi reprezintă premisa unor viitoare îmbunătăţiri ale sistemului de asigurări de sănătate
- pentru medici:
  - consistenţa informaţiilor, centralizate într-o bază unică, şi păstrarea istoricului pentru fiecare pacient, asigură un plus de încredere în luarea deciziilor;
  - pot fi urmărite eventualele interferenţe ale diverselor tratamente acordate într-o anumită perioadă de timp, care ajută la luarea unei decizii medicale optime

- administrarea unitară a informaţiilor aferente centralizat, asigură o diminuare a timpului în evaluarea situaţiei pacientului
- utilizarea standardelor informatice medicale asigură interoperabilitatea şi schimbul de informaţii pentru pacienţii care solicită servicii medicale transfrontaliere
- baza de date constituită reprezintă o arhivă electronică şi un back-up al informaţiilor fiecărui pacient

- pentru angajaţii Ministerului Sănătăţii:
  - multitudinea de statistici, care pot fi oferite în baza informaţiilor deţinute într-o bază de date reală şi curentă, sunt esenţiale în stabilirea politicilor în sistemul sanitar şi de luarea deciziilor ulterioare premiţînd:
    - asigurarea mediului necesar pentru controlarea impactului bolii la nivelul unei anumite comunităţi
    - planificarea mai eficientă a metodelor de prevenire a bolii
    - monitorizarea serviciilor medicale oferite în tratamentul şi îngrijirea bolnavilor de boli cardiovasculare

Registre Specifice de sănătate

Registrul „raportare st-biocide”

În domeniul produselor biocide, în Romania, autoritatea competenta este Ministerul Sanatatii. A fost înfiintata Comisia Nationala pentru Produse Biocide, denumita în continuare CNPB, al carui principal rol este de a asigura implementarea prevederilor RPB. Pe langa CNPB functioneaza Secretariatul Tehnic al Comisiei Nationale pentru produse Biocide, denumit ST-CNPB, care este parte integranta din Institutul National de Sanatate Publica, denumit INSP, în subordinea autoritatii competente.

ST-CNPB trebuie sa asigure informarea autoritatilor implicate şi ale operatorilor economici din domeniul produselor biocide cu date privind plasarea pe piata a produselor biocide, avizate – prin Registrul National al Produselor Biocide Avizate cat şi autorizate prin Registrul National al Produselor Biocide Autorizate în Romania. Ambele registre trebuie afisate pe website-ul www.ms.ro.

Cerințe tehnice:

Aplicatia web trebuie sa aiba mai multe sectiuni si anume:

- Sectiunea publica unde se prezinta informatii de interes public, rapoarte si statistici publice, registre nationale (Registrul Naţional al Produselor Biocide, Registrul produselor biocide plasate pe piata in baza acordarii certificatelor de Recunoastere reciproca, Registrul produselor biocide plasate pe piata in baza notificarilor din R4BP,etc), tabele, etc
- Sectiunea pentru ST-CNPB in care operatorii din ST-CNPB in urma autentificarii pot introduce, importa sau exporta date sau rapoarte in sistem
- Sectiunea pentru autoritati (MS, ANPM, ICBMV, etc) de unde utilizatorii autentificati ai autoritatilor vor extrege date sau rapoarte (registre specifice) confidentiale sau alte cerinte de date sau rapoarte catre ST-CNPB sau automate din software. De exemplu se va genera automat in format Excel Registrul National de Produse Biocide si Registrul produselor biocide plasate pe piata in baza acordarii certificatelor de Recunoastere reciproca care vor fi sincronizate cu siteul Ministerului Sanatatii (http://www.ms.ro/2017/01/17/registrul-national-al-produselor-biocide/).
  Registrul va fi accesibil online pe web prin browserele uzuale de internet indiferent de dispozitiv (PC, Laptop, tableta, smartphone, smartTV, etc) si indiferent de sistemul de operare (Windows, Android, Linux, UNIX, IOS, etc) fara a necesita instalarea locala a altor software-uri sau achizitionarea de licente.
  Pentru utilizatorii CNPB client sub forma de aplicatie portabila instalata pe calculatoarele din secretariatul CNPB

Funcționalități:

- Introducerea datelor in formulare (e-forms) prevazute cu elemente grafice si scripturi de validare, formatare si corectie automata a acestora conform unor reguli precise si selectia datelor din butoane (de selectie sau radio), liste sau ComboBox-uri.
- Sortarea, indexarea si gruparea arborescenta a datelor pe categorii si subcategorii
- Butoane de cautare simpla si avansata a datelor conform unor criterii de cautare.
- Cautari interactive unde se sugereaza o lista sau cuvantul cautat in functie de tastare.
- Importul selectiv al datelor din fisiere Word, EXCEL, CSV sau XML. De exemplu importul datelor din fisierele word specifice avizelor, avizelor de prelungire si extindere precum si al certificatelor de recunoastere reciproca si anexelor la certificatele de recunoastere reciproca.
- Extragerea selectiva a datelor din aceste fisiere Word precum: Numar aviz / numar certificat, Tip documente aferente (existenta de avize de extindere, avize de prelungire, anexe certificate de recunoastere reciproca) precum si datele de identificare ale acestora (numar avize sau certificate de recunoastere reciproca), Status aviz sau certificat de recunoastre reciproca: admis, in (re)evaluare sau respins, Denumire comerciala a produsului, Denumirile comerciale sinonime (market/trade names), Data emiterii, Data expirarii, Denumire producator, Denumire detinator de aviz (legal entity), Domeniul de utilizare, Denumire substante active, Pentru fiecare substanta activa: Numarele CAS, CE, pentru fiecare substanta activa: Concentratia (in procente, etc), Frazele de pericol si de avertizare (Frazele H si P), Date de identificare in sistemul R4BP al ECHA (Case Number si Asset Number) atat pentru MSCA-Romania in calitate de cMS cat si pentru statul membru de referinta rMS. In plus trebuie sa contina numarul autorizatiei in statul membru de referinta (cMS), Denumirea produsului in statul membru de referinta, Denumirea detinatorului de autorizatie in cMS, etc., precum si alte date de interes la cerere ce pot aparea ulterior. Toate campurile enumerate trebuie sa fie referite ca si campuri de cautare in generarea de rapoarte interne sau de interes public.
- Datele introduse trebuie sa aiba mecanisme de protectie, audit si istoric. Astfel trebuie sa existe posibilitatea de „”Track Changes”, UNDO-REDO, Commit Changes-Abandon Changes, etc. Pentru un utilizator fraudulent sau eronat trebuie sa existe posibilitatea usoara de selectie a tutoror datelor introduse de acesta, de reverificare manuala sau automata a lor si de stergere partiala sau totala a lor fara a periclita functionalitatea si si integritatea bazei de date.
- Solutia trebuie sa fie capabilă sa genereze rapoarte care sa poata fi usor tiparite si exportate in format Word, Excel si PDF
- Soluția trebuie sa fie capabila sa se sincronizeze utilizand formatul de import/export modular in format XML, EXCEL si PDF cu alte aplicatii similare de la alte autoritati competente (MSCA), ECHA sau CE prin R4BP, CIRCABC, IUCLID, Portal DASHBOARD, etc

Modul 1 Registrul National al Produselor Biocide

Această funcţionalitate permite introducerea informaţiilor despre avizele de plasare pe piata in Romania a produselor biocide.
Informaţiile vor fi structurate pe tipuri de produse (22 tipuri). Date de identificare produs biocid din aviz pentru fiecare tip de de produs TP (1-22):

- Numar aviz
- Denumirea produsului biocid
- Denumire sinonim
- Numar BC extras din R4BP
- Data expirare aviz
- Denumire producator biocide
- Denumirea substantei active
- Act comunitar de aprobare/neaprobare

- Data punere in aaplicare act comunitar
- Concentratie
- Numar EC
- Numar CAS
- Tip de produs
- Forma pdf/word a avizului (minim 10 formate) – camp parolat
- Observatii

Datele de mai sus vor fi definitivate în etapa de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu personalul Secretariatului Tehnic Biocide din INSP.
Beneficiarii acestui serviciu online vor fi în primul rând detinatorii de avize, care vor avea acces la un mijloc modern şi rapid de furnizare ainformatiilor legate de valabilitatea avizelor, precum si unitatile medicale si oricare beneficiar (public) ce achizitioneaza un produs biocid. De asemenea, celălalt beneficiar este Ministerul Sănătăţii, al carui personal de control care va avea acces la informaţii complete si coerente privind actele administrative. In ceea ce priveste controlul, beneficiarii vor fi personalul Garzii de Mediu si de control al ANSVSA pentru domeniul produselor biocide
Avantajele utilizării serviciului online de înregistrare a avizelor:

- pentru personalul Secretariatului care vor avea termene de valabilitate ale avizelor calculate online si sigur
- pentru personalul de control din cadrul MS, ANSVSA si Ministerul Mediului care vor avea acces la formatul electronic al avizelor

Modul 2 Registrul produselor biocide plasate pe piata in baza acordarii certificatelor de recunoastere reciproca a diverselor autorizatii

Această funcţionalitate permite introducerea informaţiilor despre certificatele de recunoastere reciproca a autorizatiilor in vederea plasarii pe piata in Romania a produselor biocide.
Informaţiile vor fi structurate pe tipuri de produse (22 tipuri). Date de identificare produs biocid din certificat pentru fiecare tip de de produs TP (1-22):

- Numar certificat
- Numar de autorizatie – se extrage din numarul de certificat
- Denumire comerciala a produsului
- Denumirile comerciale sinonime (market/trade names)
- Data expirarii
- Denumire detinator de certificat (legal entity)
- Denumire substante active
- Pentru fiecare substanta activa: Numarele CAS, CE,
- Pentru fiecare substanta activa: Concentratia (in procente, etc)
- Simbol si frazele de pericol (GHS si Frazele H)
- Forma pdf/word a certificatului/documente insotitoare (minim 10 formate) – camp parolat
- Alte date de interes la cerere ce pot aparea ulterior – 2 subcampuri minim

Baza de date trebuie sa permita posibilitate de incarcare (import, upload) SPC produs, eticheta si/sau FDS-ul produsului in format XML sau PDF precum si posibilitatea de import campuri de interes direct din SPC-ul din format XML
Baza de date trebuie sa permita incarcarea a mai multor fisiere simultan cu aplicatii de tip file picker. De exemplu, sa incarce toate fisierele de un anumit tip (Word sau PDF sau XML) dintr-un director si/sau subdirectoarele aferente.
Baza de date trebuie sa valideze fisierele la import pentru a asigura un nivel inalt de consistenta si corectitudine a datelor si sa elimine duplicatele. Fisierele care nu se pot importa prin validare automata

trebuie stocate separat si trebuie sa existe un fisier de erori unde se va preciza motivul respingerii fisierului la import.
Beneficiarii acestui serviciu online vor fi în primul rând detinatorii de certificate, care vor avea acces la un mijloc modern şi rapid de furnizare a informatiilor legate de valabilitatea acestora, precum si unitatile medicale si oricare beneficiar (public) ce achizitioneaza un produs biocid. De asemenea, celălalt beneficiar este Ministerul Sănătăţii, al carui personal de control care va avea acces la informaţii complete si coerente privind actele administrative. In ceea ce priveste controlul, beneficiarii vor fi personalul Garzii de Mediu si de control al ANSVSA pentru domeniul produselor biocide
Avantajele utilizării serviciului online de înregistrare a avizelor:

- pentru personalul Secretariatului care vor avea certificate online
- pentru personalul de control din cadrul MS, ANSVSA si Miniterul Mediului care vor avea acces la formatul electronic al certificatelor si documentelor insotitoare

Modul 3 Registrul produselor biocide plasate pe piata in baza notificarii a diverselor autorizatii

Această funcţionalitate permite introducerea informaţiilor despre notificari ale autorizatiilor in vederea plasarii pe piata in Romania a produselor biocide.
Informaţiile vor fi structurate pe tipuri de produse (22 tipuri). Date de identificare produs biocid din certificat pentru fiecare tip de de produs TP (1-22):

- Numar de autorizatie din UE/Stat membru de Referinta
- Emitent
- Tip documente aferente (autorizatie)
- Denumire comerciala a produsului
- Denumirile comerciale sinonime (market/trade names)
- Data expirarii
- Denumire detinator de autorizatie (legal entity)
- Denumire rersponsabil de plasre pe piata in Romania
- Denumire substante active
- Pentru fiecare substanta activa: Numerele CAS, CE,
- Pentru fiecare substanta activa: Concentratia (in procente, etc)
- Simbol si frazele de pericol (GHS si Frazele H)
- Alte date de interes la cerere ce pot aparea ulterior – 2 subcampuri minim

Baza de date trebuie sa permita posibilitate de incarcare (import,upload) a autorizatiei, SPC produs, eticheta si/sau FDS-ul produsului in format XML sau PDF precum si posibilitatea de import campuri de interes direct din SPC-ul din format XML.
Baza de date trebuie sa permita incarcarea a mai multor fisiere simultan cu aplicatii de tip file picker. De exemplu sa incarce toate fisierele de un anumit tip (Word sau PDF sau XML) dintr-un director si/sau subdirectoarele aferente.
Baza de date trebuie sa valideze fisierele la import pentru a asigura un nivel inalt de consistenta si corectitudine a datelor si sa elimine duplicatele. Fisierele care nu se pot importa prin validare automata trebuie stocate separat si trebuie sa existe un fisier de erori unde se va preciza motivul respingerii fisierului a import.
Beneficiarii acestui serviciu online vor fi în primul rând detinatorii de autorizatii, care vor avea acces la un mijloc modern şi rapid de furnizare a informatiilor legate de valabilitatea acestora, precum si unitatile medicale si oricare beneficiar (public) ce achizitioneaza un produs biocid. De asemenea, celălalt beneficiar este Ministerul Sănătăţii, al carui personal de control care va avea acces la informaţii complete si coerente privind actele administrative. In ceea ce priveste controlul, beneficiarii vor fi personalul Garzii de Mediu si de control al ANSVSA pentru domeniul produselor biocide
Avantajele utilizării serviciului online de înregistrare a avizelor:

- pentru personalul Secretariatului care vor avea autorizatiile notificate online
- pentru personalul de control din cadrul MS, ANSVSA si Miniterul Mediului care vor avea acces la formatul electronic al certificatelor si documentelor insotitoare

Rapoarte
Sectiunea ST-CNPB va genera automat registre publice sau private (pentru autoritati) de produse biocide conform criteriilor de continut si campuri asociate. Aceste registre vor fi disponiblie pe siteul WEB al aplicatie in sectiunile corespunzatoare (publica, privata pentru autoritati).
Pentru sectiunea de interes public aplicatia Web/Desktop interoghează baza de date si genereaza Registrul Național al Produselor Biocide extrage informatiile de interes public. Rezultatul interogării este o pagină de tip formular care va afișa sub formă de listă tabelară informaţiile de interes public. Acest tabel trebuie sa aibă obțiunea de ordonare dupa câmpul din capul de tabel cand utilizatorul efectuează click cu mouseul pe acesta ordonarea realizându-se crescător sau descrescător în mod alternativ la fiecare click.
Pentru toate registrele specifice se vor avea in vedere si cerintele de la cap "Statistici si rapoarte" valabile pentru registrele de boala.

Registrul calitatea apei potabile (RECAP)
Registrul Electronic Calitatea Apei Potabile (RECAP) va stoca informatii referitoare la zonele de aprovizionare cu apa potabila respectiv informatii referitoare la calitatea apei potabile distribuite in sistem centralizat din Romania.
Monitorizarea de audit
Aceasta functionalitate este specifica Directiilor de Sanatate Publica (DSP) judetene, care analizeaza pentru una sau mai multe zone de aprovizionare cu apa, conformitatea parametriilor apei potabile conform legii apei potabile nr. 458/2002 (cu modificarile si completarile ulterioare), legea nr. 301/2015 pe care producatorii/distribuitorii de apa o distribuie populatiei.
Conformitatea parametriilor prevazuti la Art.5, din legea calitatii apei potabile se poate efectua numai in laboratoarele acreditate in conformitate cu ordinul nr. 764/2005 inregistrate pe site-ul MS in Registrul laboratoarelor pentru monitorizarea calitatii apei potabile.
Rezultatele analizelor sunt incarcate in sistem fie direct de catre laboratoarele unde au fost efectuate analizele, fie de catre DSP.
Informatiile vor fi grupate pe grupe de date

a) Informatii despre DSP
   - Denumire
   - Adresa
   - Judetul
   - Telefon/fax
   - E-mail
   - Persoana contact
b) Informatii despre laboratoare
   - Denumire
   - Adresa
   - Judetul
   - Telefon/fax
   - Informatii despre acreditare
   - Persoana contact
c) Informatii parametrii analizati (buletin de analiza)
   - Denumire parametru
   - Unitatea de masura
   - Valoarea obtinuta

- Valoarea maxima admisa (cf legii)
- Referential de analiza
- Analiza neconforma (Da/Nu)
- Tipul monitorizarii (audit/control)
- Locul Prelevarii
- Cauze
- Remedii
- Calendar
- Proba este prelevata direct de la robinetul folosit in mod obisnuit pentru consumul apei, fara a-l lasa sa curga anterior prelevarii (Da/Nu)
- Proba este prelevata dintr-un punct de retea in care apa a stagnat o perioada de cel putin 30 de minute inainte de prelevare (Da/Nu)
- Proba este prelevata dupa evacuarea apei cu jet puternic (Da/Nu)
- Proba este prelevata dupa dezinfectia robinetului (Da/Nu)

d) Informatii zona de aprovizionare cu apa (ZAA)

- Denumire
- Judet
- Localitate/localitatii deservite
- Populatie aprovizionata
- Populatie totala
- Volum apa furnizat (mc/zi)
- Coordinate GPS (latitudine, longitudine)
- Coordonate NUTS 2 code
- Coordonate LAU2 code
- Sursa de apa

e) Informatii Derogari (daca exista)

1. **Beneficiarii** acestui serviciu online vor fi in primul rand Directiile de Sanatate Publica (DSP) care efectueaza monitorizarea de audit pentru toate zonele de aprovizionare cu apa potabila distribuite in sistem centralizat din Romania. De asemenea celalalt beficiar este producatorul/distribuitorul de apa publica, care poate verifica si compara rezultatele obtinute in urma analizarii parametriilor monitorizati, respectiv Institutul National de Sanatate Publica (INSP) al carui personal de control obtine printre altele informatii referitoare la neconformitatea zonelor de aprovizionare cu apa.

2. **Avantajele** utilizarii serviciului online de Monitorizare deAudit
   - Pentru DSP
     - vor avea la dispoziţie un mijloc modern şi rapid de completare şi actualizare a datelor referitoare la monitorizarea de audit
   - Pentru producatorii/distribuitorii de apa
     - vor avea la dispoziţie un mijloc modern şi rapid de verificare şi comparare a datelor referitoare la monitorizarea de audit fata de monitorizarea de control
   - Pentru INSP
     - vor avea la dispoziţie un mijloc modern şi rapid de vizualizare rapida a datelor referitoare la monitorizarea de control atat pentru parametrii conformi cat si despre parametrii neconformi si/sau date referitoare la ZAA

Monitorizarea de control

Aceasta functionalitate este specifica producatorilor/distribuitorilor de apa, care analizeaza pentru una sau mai multe zone de aprovizionare cu apa cei 18 parametrii prevazuti de legea 458/2002 (cu modificarile si completarile ulterioare).

Monitorizarea celor 18 parametrii privind calitatea organoleptică și microbiologică a apei potabile este efectuata periodic (lunar), si se poate analiza atat in laboratoare private cat si in laboratoarele DSP.
Rezultatele analizelor sunt incarcate in sistem fie direct de catre laboratoarele unde au fost efectuate analizele, fie de catre producatorii/distribuitorii de apa.

1. **Informatiile** vor fi grupate pe grupe de date
    a) Informatii despre producatorii/distribuitorii de apa
        - Numele Producatorului/Distribuitorului
        - Adresa
        - Judetul
        - Telefon/fax
        - Persoana contact
    b) Informatii despre laboratoare
        - Denumire
        - Adresa
        - Judetul
        - Telefon/fax
        - Informatii despre acreditare
        - Persoana contact
    c) Informatii parametrii analizati (buletin de analiza)
        - Denumire parametru
        - Unitatea de masura
        - Valoarea obtinuta
        - Valoarea maxima admisa (cf legii)
        - Referential de analiza
        - Analiza neconforma (Da/Nu)
        - Tipul monitorizarii (audit/control)
        - Locul Prelevarii
        - Cauze
        - Remedii
        - Calendar
        - Proba este prelevata direct de la robinetul folosit in mod obisnuit pentru consumul apei, fara a-l lasa sa curga anterior prelevarii(Da/Nu)
        - Proba este prelevata dintr-un punct de retea in care apa a stagnat o perioada de cel putin 30 de minute inainte de prelevare(Da/Nu)
        - Proba este prelevata dupa evacuarea apei cu jet puternic (Da/Nu)
        - Proba este prelevata dupa dezinfectia robinetului (Da/Nu)
    d) Informatii zona de aprovizionare cu apa (ZAA)
        - Denumire
        - Judet
        - Localitate/localitatii deservite
        - Populatie aprovizionata
        - Populatie totala
        - Volum apa furnizat (mc/zi)
        - Coordinate GPS (latitudine, longitudine)
        - Coordonate NUTS 2 code
        - Coordonate LAU2 code
        - Sursa de apa

i) Informatii Derogari (daca exista)

1. **Beneficiarii** acestui serviciu online vor fi in primul rand producatorii/distribuitorii de apa potabila care efectueaza monitorizarea celor 18 parametrii privind calitatea organoleptică şi microbiologică a apei potabile din Romania. De asemenea celalalt beficiar este Directia de Sanatate Publica (DSP) care poate verifica si compara rezultatele obtinute in urma analizarii parametriilor monitorizati, respectiv Institutul National de Sanatate Publica al carui personal de control obtine printre altele informatii referitoare la neconformitatea zonelor de aprovizionare cu apa.

2. **Avantajele** utilizarii serviciului online de Monitorizare de Control
   - Pentru producatorii/distribuitorii de apa
     - vor avea la dispoziţie un mijloc modern şi rapid de completare şi actualizare a datelor referitoare la monitorizarea de control
   - Pentru DSP
     - vor avea la dispoziţie un mijloc modern şi rapid de verificare şi comparare a datelor referitoare la monitorizarea de control fata de monitorizarea de audit
   - Pentru INSP
     - vor avea la dispoziţie un mijloc modern şi rapid de vizualizare rapida a datelor referitoare la monitorizarea de control atat pentru parametrii conformi cat si despre parametrii neconformi si/sau date referitoare la ZAA

I. Zona de aprovizionare cu apa (ZAA)

Pentru a facilita accesul la informaţiile existente în baza de date, aplicaţia va permite afişarea tuturor ZAA inregistrate in aplicatie.
Aceasta sectiune va fi impartita in doua module: ZAA mari si ZAA mici.
Fiecare ZAA va avea o sectiune intitulata Parametrii.
Datorită volumului mare de informaţii sectiunea intitulata Parametrii se va afişa în urma unei operaţii de filtrare. Filtrarea se va putea face după informaţiil: Judet, denumire ZAA, populatie aprovizionata, parametrii neconformi, sau alte elemente care vor fi stabilite în timpul etapei de analiză cu ajutorul specialiştilor INSP, DSP, MS.
Motorul de căutare va fi accesibil în momentul accesării opţiunii Parametrii din meniul principal al fiecarei ZAA
De asemenea, pentru a uşura căutarea în interiorul listei va exista posibilitatea sortării informaţiei.
Beneficiarii acestui serviciu online vor fi INSP, DSP, producatorii/distribuitori de apa, MS:

- Producatorii/distribuitorii de apa vor avea o situatie per total referitoare la datele parametriilor si a ZAA care le apartin
- DSP va avea o situatie per total la toate ZAA din judetul care-l reprezinta
- INSP si MS va avea o situatie per total a tututor informatiilor privind calitatea apei potabile, la nivel national

Avantajele utilizarii acestui serviciu online de catre producatorii/distribuitori de apa, INSP, DSP, MS

- accesul rapid la informaţii
- imagine clară şi completă asupra datelor referitoare la valorile parametriilor si la zonele de aprovizionare cu apa potabila distribuita in sistem centralizat din Romania

Raportare EIONET

Aceasta functionalitate este specifica specialistiilor INSP care se ocupa de raportarea catre Comisia Europeana a raportului trianual privind zonele de aprovizionare cu apa potabila din Romania.

Toate informatiile afisate cu ajutorul acestei functionalitati vor fi extrase din modulele anterioare.
Una din obligatiile pe care Romania le are in urma aderarii la Uniunea Europeana este aceea de a raporta o data la trei ani informatii referitoare la calitatea apei potabile distribuite in sistem centralizat in Zonele Mari de Aprovizionare cu apa.
Raportul trianual este sub format excel, cate un fisier pentru fiecare an, fiecare fisier contine campuri/informatii structurate in mai multe sheet-uri excel.
Informatiile vor fi grupate pe sheet-uri excel.
1.Sheet-ul AnnualMonitoring este alcatuit din urmatoarele campuri:

- Codul tarii – 2 litere
- ID-ul ZAA – 6 cifre
- Parametrul – 48 parametrii + 13 parametrii foarte rari monit in Romania
- Anul – 4 cifre

2.Sheet-ul MemberState este alcatuit din urmatoarele campuri:

- Codul tarii - 2 litere
- Anul - 4 cifre
- Populatie totala – cifre (unit. masura milioane)
- Numar total de ZAA – cifre
- Populatie totala aprovizionata -cifre
- Volum total de apa furnizat – cifre (unit. masura m3/an)
- Sursa de profunzime – cifre (procent)
- Sursa de suprafata – cifre (procent)
- Inlandwater – cifre (procent)
- Apa costala – cifre (procent)
- Reincarcare artificiala acvifer – cifre (procent)
- Apa de ploaie – cifre (procent)
- Apa filtrata prin banc – cifre (procent)
- Alte surse – cifre (procent)
- Adresa web MS - text
- Nume MS - text
- Adresa MS - text
- Telefon MS - cifre
- Fax MS - cifre
- E-mail MS - cifre
- Rezumat raport, adresa web - text

3.Sheet-ul NationalSummary este alcatutit din urmatoarele campuri

- Codul tarii - 2 litere
- Parametrul - 48 parametrii + 13 parametrii foarte rari monit in Romania
- Numar total de ZAA - cifre
- Numar total de ZAA neconforme - cifre
- Numar total de analize efectuate (audit+control) - cifre
- Numar total de analize neconforme (audit+control) - cifre
- Procent analize conforme – cifre (procent)
- SampleLocation_Water - litera W
- SampleLocation_Network – litera N
- SampleLocation_Legal – litera L
- SampleLocation_Tap – litera T
- Anul – cifre

4.Sheet-ul NonComplianceInformation este alcatuit din urmatoarele campuri:

- Codul tarii - 2 litere
- ID-ul ZAA – 6 cifre
- Parametrul - 48 parametrii + 13 parametrii foarte rari monit in Romania
- Derogarea - text
- Numar total de analize efectuate (audit+control) - cifre
- Numar total de analize neconforme (audit+control) - cifre
- Valoarea Maxima - cifre
- Mediana analize totale - cifre
- Mediana analize neconforme - cifre
- Row_ID - cifre
- Anul – 4 cifre

5.Sheet-ul NonComplianceInformation_1 este alcatutit din urmatoarele campuri:

- Id-ul ZAA - 6 cifre
- Parametrul - 48 parametrii + 13 parametrii foarte rari monit in Romania
- Row_ID - cifre
- UseRestriction_YN – Y sau N
- UseProhibition_YN - Y sau N
- Rest_Proh_reason - text
- Restr_Proh_timeframe – 1 litera
- Anul – 4 cifre

6.Sheet-ul NCI_Cause este alcatuit din urmatoarele campuri:

- Row_ID - cifre
- Cauze - litere
- Numar de analize neconforme - cifre
- RemedialID - cifre

7.Sheet-ul Remedial este alcatuit din urmatoarele campuri:

- RemedialID - cifre
- DWD_Remedii - litere
- NumberAnalysisRemedialAction - litere
- DWD_Timeframe – 1 litera

8.Sheet-ul ProductSpecifiedParameters este alcatutit din urmatoarele campuri

- Codul tarii – 2 litere
- Acrylamide – descriere text
- Epichlorohydrin – descriere text
- Vinylchloride – descriere text
- Anul – 4 cifre

9.Sheet-ul PublicInformation este alcatuit din urmatoarele campuri

- CountryCode – 2 litere
- NationalSummary
- NationalSummaryLocation - link
- RegionalSummary
- RegionalSummaryLocation - link
- WSZSummary
- WSZSummaryLocation - link
- IndividualResults
- IndividualResultsLocation - link
- MonitoringResults5000
- MonitoringResults5000Location - link
- MonitoringResults50

- MonitoringResults50Location - link
- ComplianceStricter
- ComplianceStricterLocation - link
- ComplianceAdditional
- ComplianceAdditionalLocation - link
- NonCompliant
- NonCompliantLocation - link
- Source
- SourceLocation
- Other
- OtherLocation

10.Sheet-ul QualityInformation este alcatuit din urmatoarele campuri

- CountryCode – 2 litere
- Website
- WebsiteLocation- link
- NationalReport
- NationalReportLocation- link
- RegionalReport
- RegionalReportLocation- link
- NationalTriennialReport
- NationalTriennialReportLocation- link
- Leaflets
- LeafletsLocation
- NewsLetter
- NewsLetterLocation
- WaterBills
- WaterBillsLocation
- PublicMeetings
- PublicMeetingsLocation
- LocalNewspapers
- LocalNewspapersLocation
- PublicFiles
- PublicFilesLocation
- Other
- OtherLocation

11.Sheet-ul WaterSupplyZone (ZAA) este alcatuit din urmatoarele campuri:

- Codul tarii
- ID-ul ZAA
- Nume ZAA
- Coordonate NUTS
- Populatie aprovizionata
- Volum apa furnizat
- Anul

12.Sheet-ul WaterSupplyZone_1(ZAA) este alcatutit din urmatorele campuri:

- ID
- NUTS2_code
- LAU_2_code
- lat
- lon

- Closed
- ClosedReasons
- ClosedNewSuccessorID
- LinkToNationalFiche
- Year

13. Sheet-ul SmallWaterSupplyZone este alcatutit din urmatorele campuri:
    - CountryCode
    - Year
    - NumberWSZ
    - TotalVolume
    - TotalResidentlPopulation
14. Sheet-ul SmallWaterSupplyZone_1 este alcatutit din urmatorele campuri:
    - WSZ_ID
    - WSZ_Name
    - CountryCode
    - NUTS_2_Code
    - LAU_2_Code
    - Lat DWD_S_WSZ_Lon
    - Cat_WSZ
    - WSZ_Residents
    - WSZ_Volume
    - Derogation
    - DerogationParamConcerned
    - Year
15. Sheet-ul SmallWaterSupplyZone_2 este alcatutit din urmatorele campuri:
    - CountryCode
    - Parameter
    - WSZMonitored
    - WSZNonComplied
    - NS_Analysis
    - NS_AnalysisNonComplied
    - NS_PercComplying
    - DWD_Year

Beneficiarii acestui serviciu online vor fi specialistii INSP si MS

Avantajele utilizarii serviciului online de Raportare Eionet: pregatirea si exportarea foarte rapida a raportului privind calitatea apei, raport cerut de Comisia Europeana.

Statistici si rapoarte

Sistemul va permite constituirea unei baze de date completă şi coerentă ce va conţine informaţii despre zonele de aprovizionare cu apa potabila din Romaniai pe baza cărora se vor putea defini rapoarte si statistici referitoare la calitatea apei din Romania.

Cu ajutorul hartiilor interactive, RECAP va permite vizualizarea in timp real a informatiilor despre potabilitatea apei distribuite in sistem centralizat respectiv si se vor vizualiza ultimele valori ale parametriilor analizati conform legislatiei in vigoare.

Statisticile şi rapoartele dorite vor avea minim urmatoarea structura:

1. **Rapoarte grafice tip "Column" impartite in:**
   a) Rapoarte grafice pe **judet/an** cu urmatoarele date:
      - numar total de zone de aprovizionare cu apa in fiecare judet
      - numar total de parametrii monitorizati in fiecare judet
      - numar total de parametrii neconformi in fiecare judet

- numar total de populatie aprovizionata in fiecare jutet
- volum total de apa furnizat in m3/zi in fiecare judet

b) Rapoarte grafice pe **judet/an** cu urmatoarele date:
- procent populatie aprovizionata cu apa in fiecare judet
- procent volum apa distribuit in m3/zi din totalul anual pe tara
- procent populatie aprovizionata din totalul pe tara
- procent sursa de apa

c) Tendinte
- Numar de ZAA
- Populatie aprovizionata
- Volum apa furnizat
- Sursa de apa

2. **Rapoarte Tabelare impartite in:**

a) Rapoarte **judet/an** referitoare la zona de aprovizionare cu apa
- cap tabel:
  - Judet
  - Numar total Zone de Aprovzionare cu Apa
  - Populatie aprovizionata
  - Volum de apa furnizat

b) Rapoarte **judet/an** referitoare la parametrii monitorizati
- cap tabel:
  - Judet
  - Numar parametrii monitorizari
  - Numar parametrii valori neconforme
- cap tabel:
  - Parametrul
  - Numar total de ZAA
  - Numar total de ZAA neconforme
  - Numar total de analize efectuate (total, audit, control)
  - Numar total de analize neconforme (total, audit, control)
  - Procent analize conforme

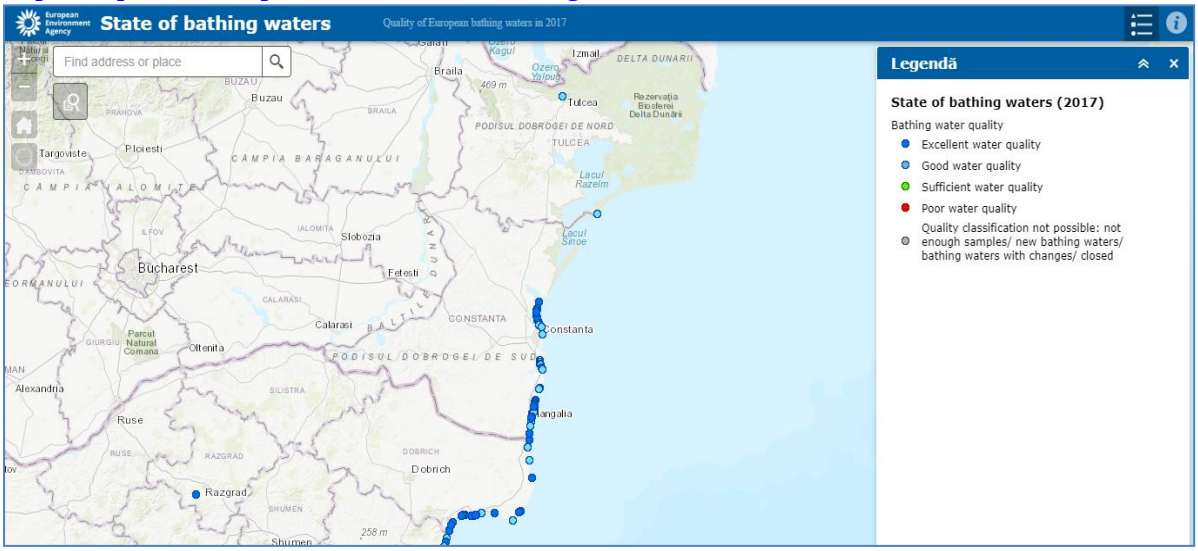
c) Rapoarte **ZAA/an** referitoare la
- cap tabel:
  - Parametrii
  - Numar de azalize efectuate (total, audit, control)
  - Numar de analize neconforme (total, audit, control)
- cap tabel:
  - Nume zap
  - Populatie aprovizionata
  - Volum apa furnizat
  - Sursa de apa
  - Parametrii neconformi (listati)

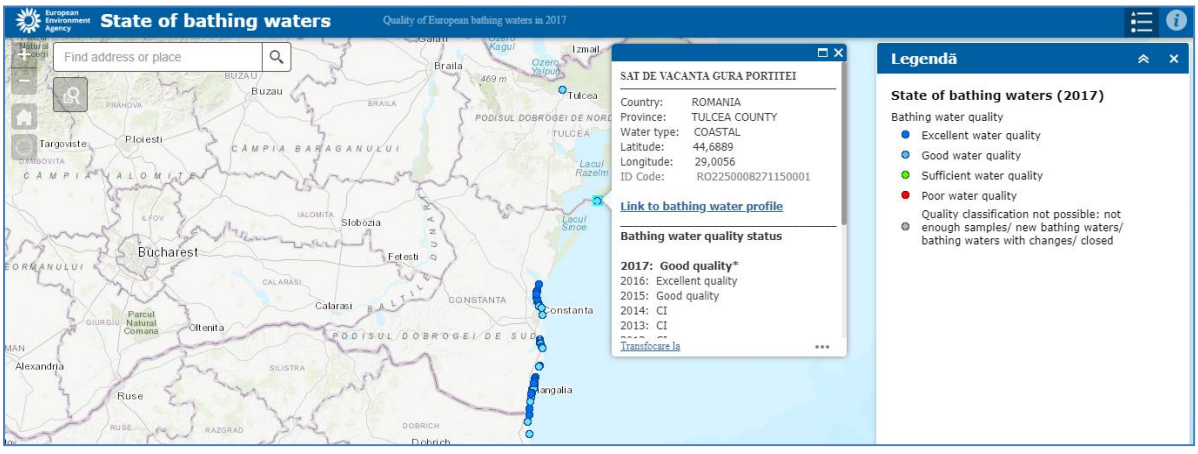
3. **Rapoarte tabelare selective parametrii neconformi** – posibilitatea selectarii unuia sau mai multor parametrii a caror rezultat al analizelor este neconform
   1. campuri selectate:
      - Parametrul (unul sau mai multi)
      - Judetul
      - ZAA

- Populatia aprovizionata
- Analize efectuate
- Analize neconforme

4. **Afisari geospatiale**
   - Afisarea ZAA pe harta (ca puncte)
   - Afisarea localitatilor racordate la ZAA (layer)
   - Afisarea populatiei aprovizionate la ZAA (layer)
   - Afisarea volumului de apa furnizat pentru fiecare ZAA (layer)
   - Afisarea sursei de apa
   - Posibilitatea de selectare si vizualizarea a buletinelor de analize referitoare la calitatea apei potabile pentru fiecare ZAA

Posibilitatea salvarii informatiilor de mai sus in format **jpg, PDF**
Exemplu aplicatie Online **European Environment Agency (EEA)**
http://maps.eea.europa.eu/wab/stateofbathingwaters/





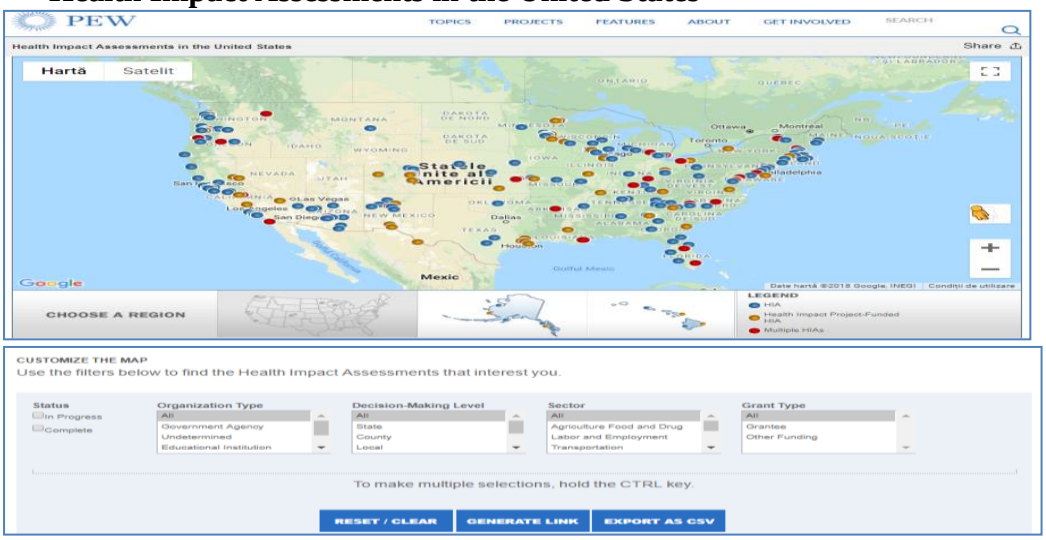
Informatiile afisate in harta de mai sus se refera la zonele de imbaiere din Romania.

5. **Afisari Google Maps/Earth/orice aplicatie cu ajutorul careia se pot afisa informatii/date pe harti**

Posibilitatea de afisare a informatiilor din RECAP pe o harta dinamica. Posibilitatea selectarii campurilor componente din structura bazei de date RECAP si afisarea acestora ca total sau ca un sumar al informatiilor pe harta.

Un exemplu de afisare a informatiilor pe harta (google maps) il puteti vizualiza mai jos.

Health Impact Assessments in the United States



sursa:
http://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2015/hia-map

Astfel, in urma campurilor selectate acestea sunt afisate pe harta in timp real, de exemplu pentru o ZAA se pot selecta si vizualiza lista parametriilor monitorizati si valorile obtinute in urma analizelor intr-o anumita perioada de timp sau chiar in timp real.

Beneficiarii acestui serviciu online vor fi specialistii INSP, MS, DSP, producatorii/distribuitorii de apa

Informatiile referitoare la statistici si rapoarte vor fi afisate diferit in functie de tipul de utilizator inregistrat in sistem.

Avantajele acestui serviciu online

- Crearea raportului trianual referitor la calitatea apei potabile distribuite in sistem centralizat din Romania
- vizualizarea per total a calitatii apei potabile pe harti dinamice
- baza de date constituită reprezintă o arhivă electronică şi un back-up al informaţiilor fiecărei ZAA din Romania
- crearea rapoartelor sanatate si mediu sectiunea apa potabila
- multitudinea de statistici, care pot fi oferite în baza informaţiilor deţinute într-o bază de date reală şi curenta

Buletin Analize

Buletinul de analiză a apei potabile este un raport care furnizează informaţii referitoare la proveniența apei potabile şi comparând diverse caracteristici şi componente ale acesteia cu standardele impuse de legislaţia în vigoare (Legea 458/ 2002 şi Legea 311/ 2004).

Fiecare buletin va fi practic punctul de recoltare a probelor pentru analiza apei potabile. Acestea va fi afisat pe o harta dinamica si va afisa/deschide in momentul in care se apasa pe acesta intregul bulletin de analize respectiv un istoric cu toate recoltarile recente.

Informatiile afisate pe harta dinamica vor fi urmatoarele:

a) Informatii despre Producator/Distribuitor
   - Numele Producatorului/Distribuitorului
   - Adresa
   - Judetul
   - Telefon/fax
   - Persoana contact

b) Informatii despre laboratoare
   - Denumire

- Adresa
- Judetul
- Telefon/fax
- Informatii despre acreditare
- Persoana contact

c) Informatii parametrii analizati (buletin de analiza)
- Denumire parametru
- Unitatea de masura
- Valoarea obtinuta
- Valoarea maxima admisa (cf legii)
- Referential de analiza
- Analiza neconforma (Da/Nu)

d) Informatii zona de aprovizionare cu apa (ZAA)
- Denumire
- Judet

Beneficiarii acestui serviciu online vor fi persoanele neinregistrate in sistem (publicul)
Avantajele serviciului online, cu ajutorul hartiilor interactive, RECAP va fi prima platforma online din Romania unde se pot vizualiza in timp real informatiile despre potabilitatea apei distribuite in sistem centralizat respectiv se pot vizualiza ultimele valori ale parametriilor analizati conform legislatiei in vigoare.

Registrul operativ naţional informatizat al bolilor profesionale

Înregistrarea furnizorilor de servicii medicale

Această funcţionalitate permite introducerea informaţiilor despre furnizorii de servicii medicale care vor avea acces la Registrul operativ naţional informatizat al bolilor profesionale.

Date de identificare furnizor:
- cod şi nume unitate sanitară,
- cod şi denumire secţie,
- cod şi denumire judeţ,
- cod şi denumire localitate,
- nume şi prenume medic specialist,
- specialitate medic,
- parafă medic

Datele de mai sus vor fi definitivate în etapa de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu medicii coordonatori ai fiecărui registru de boală.
Beneficiarii acestui serviciu online vor fi în primul rând furnizorii de servicii medicale (medici specialişti), care vor avea acces la un mijloc modern şi rapid de introducere a informaţiilor referitoare la pacienţi. De asemenea, celălalt beneficiar este Ministerul Sănătăţii, care va avea acces la informaţii complete si coerente privind imbolnavirea prin boli profesionale.
Avantajele utilizării serviciului online de înregistrare furnizori de servicii medicale:
- pentru furnizorii de servicii medicale:
  - vor avea la dispoziţie un mijloc modern şi rapid de completare şi actualizare a datelor pentru conectare la Registrul naţional de boli profesionale

Lista pacienţilor cuprinşi în registrul naţional

Pentru a facilita accesul la informaţiile existente în baza de date, aplicaţia va permite afişarea unei liste de pacienţi.

Informatii ce fac obiectul registrului:
- Crearea unei baze de date privind bolile profesionale pentru care exista o asociere cauzala directa cu prezenta factorului de risc profesional

- Reactualizarea permanenta a evidentei tinand seama si de informarile de boala profesionala declarata
- Inregistrarea bolilor asociate
- Inregistrarea absenteismului medical prin boli profesionale
- Inregistrarea deceselor datorate imbolnavirilor profesionale
- Inregistrarea si evidenta bolilor legate de profesiune

Datorită volumului mare de informaţii lista se va afişa în urma unei operaţii de filtrare. Filtrarea se va putea face după informaţiile de identificare a pacientului, ca de exemplu: nume, prenume, CNP/CID, data naşterii, unitatea medicală, data luării în evidenţă sau alte elemente care vor fi stabilite în timpul etapei de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu medicii coordonatori ai fiecărui registru de boală.
Motorul de căutare va fi accesibil în momentul accesării opţiunii Pacienţi din meniul principal
De asemenea, pentru a uşura căutarea în interiorul listei va exista posibilitatea sortării informaţiei.
Beneficiarii acestui serviciu sunt medicii şi angajaţii MS.
Avantajele utilizării serviciului atât pentru furnizorii de servicii medicale cât şi pentru angajaţii MS:

- accesul rapid la informaţii
- imagine clară şi completă asupra datelor despre pacienţi

Înregistrare online a pacienţilor
Această funcţionalitate este specifică furnizorilor de servicii medicale care se află înregistraţi în lista de furnizori de servicii medicale a sistemului.
Prin înregistrarea online a pacienţilor, se va furniza medicilor specialişti un mecanism online, modern şi uşor de utilizat pentru accesul la informaţia din registrul naţional. Astfel, înregistrarea online a pacienţilor va permite introducerea informaţiilor medicale specifice registrului naţional de boli profesionale.
Date de identificare pacient:

- CNP/CID
- nume
- prenume
- sex
- varstă
- data naşterii,
- locul naşterii,
- denumire localitate de domiciliu,
- sector de domiciliu,
- denumire judeţ de domiciliu,
- motivul de înregistrare.
- date antropometrice
- Profesia/ocupatie/meserie
- Status socioprofesional actual

Date referitoare la boală:

- data diagnosticului
- date din fisa de declarare BP2 (Judeţul, Localitate, Direcţia de sănătate publică, ÎNTREPRINDEREA/UNITATEA ANGAJATOARE, CUI, ADRESA COMPLETĂ A ÎNTREPRINDERII/ UNITĂŢII, COD CAEN, Secţia, atelierul/post de munca, COD OCUPAŢIE ACTUALĂ, Profesia/ocupatie/meserie, COD OCUPAŢIE CARE A GENERAT BOALA, Profesia/ocupatie/meserie, Status socioprofesional actual, Vechimea în ocupaţia care a generat boala, Data semnalării: an/luna/zi, Diagnosticul prezumptiv, Unitatea care a semnalat diagnosticul de profesionalitate, Diagnosticul de

boala profesionala precizat complet lista CIM, şi nr comisie de pneumoconioze .....codificarea radiologică în cazul diagnosticului de pneumoconioză – clasificare, Data declarării (anul, luna, ziua, Agentul cauzal (circumstanţe), Grup de cauze, Use category: conform EODS, Măsuri indicate pentru bolnav, Starea de gravitate (ITM), Bolnavul a decedat.

- date din fisa de semnalare a bolii profesionale BP1
- date din procesul verbal de cercetare a cazului de boala profesionala
- date din documentele medicale din dosarul de cercetare a bolii profesionale
- date legate de contestari/infirmari de boala profesionala declarata (Cine a contestatinfirmat boala profesionala declarata, Data contestarii/infirmarii, Motivatia contestariiinfirmarii, Stadiul cercetarii, Concluzia)
- tipul bolii
- vechimea bolii
- cum a debutat boala
- forma de boala
- factori de risc
  - Istoric familial
  - traumatisme (de orice fel, la orice vârstă)
  - expunere toxice (de orice fel)
- statusul bolii
  - aspecte motorii
  - aspecte non-motorii
- calitatea vieții

Date referitoare la evoluţia şi tratamentul bolii:

- Terapia intraspitalicească
- Tratament simptomatic motor
- Tragtament simptomatic non-motor
- Complicaţiile tratamentului
- Măsuri indicate pentru bolnav
- Data şi motivul de deces

Datele prezentate mai sus constituie structura setului minim de date necesar pentru înregistrarea unui pacient în Registrul naţional de boli profesionale. Acest set de date va fi definitivat în etapa de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu medicii coordonatori ai fiecărui registru de boală profesionala.

Sistemul va permite adăugarea de pacienţi noi sau modificarea datelor unui pacient existent.

Beneficiarii acestui serviciu online vor fi în primul rând furnizorii de servicii medicale (medici specialişti), care vor avea la dispoziţie un mijloc modern şi rapid de introducere a informaţiilor în baza de date. De asemenea, celălalt beneficiar este Ministerul Sănătăţii, care va avea acces la o informaţie completă şi coerentă referitoare la pacienţii.

Statistici si rapoarte

Sistemul va permite constituirea unei baze de date completă şi coerentă ce va conţine informaţii despre pacienţii, tratamentele aplicate si evoluţia bolii, informaţii pe baza cărora se vor putea defini rapoarte si statistici referitoare la apariţia bolii, la nivelul tuturor segmentelor populaţiei.

Statisticile şi rapoartele dorite vor fi definite în cadrul etapei de analiză.

Sunt prezente urmatoarele rapoarte predefinite care permit vizualizarea și urmărirea anumitor informații de interes:

- Numar total boli profesionale declarate
- Numar total boli profesionale declarate si diagnostic
- Numar total boli profesionale declarate si diagnostic detaliat (din diagnostic prezumptiv BP2)

- Numar total boli profesionale declarate pe judete
- Numar total boli profesionale declarate pe ocupatie
- Numar total boli profesionale declarate pe ramura economica
- Numar total boli profesionale declarate pe agent cauzal
- Numar total boli profesionale declarate pe sexe
- Numar total boli profesionale declarate pe grupe de varsta
- Numar total boli profesionale declarate pe grupe de vechime
- Numar total boli profesionale declarate pe grupe si boli asociate
- Numar pentru fiecare boala profesionala declarata si diagnostic detaliat (din diagnostic prezumptiv BP2)
- Numar pentru fiecare boala profesionala declarata pe judete
- Numar pentru fiecare boala profesionala declarata pe ocupatie
- Numar pentru fiecare boala profesionala declarata pe ramura economica
- Numar pentru fiecare boala profesionala declarata e pe agent cauzal
- Numar pentru fiecare boala profesionala declarata pe sexe
- Numar pentru fiecare boala profesionala declarata pe grupe de varsta
- Numar pentru fiecare boala profesionala declarata pe grupe de vechime
- Numar pentru fiecare boala profesionala declarata si boli associate
- Numar de boli profesionale declarate care au fost infirmate
- Combinatii intre diagnostic/ramura industriala/agent cauzal/profesie/sex/varsta/vechime/
- Tabele/grafice comparative pe perioade de timp pe baza de selectie de campuri.

Beneficiarii acestui serviciu sunt cetăţenii, furnizorii de servicii medicale şi angajaţii MS.
Avantajele utilizării serviciului:

- pentru cetăţeni:
  - existenţa unei baze centralizatoare a tuturor pacienţilor, a bolilor profesionale şi statisticile care sunt extrase de aceasta, pot furniza date concrete, şi-ntr-un mod eficient, în sprijinul unor decizii în beneficiul pacienţilor. Ajută în timp, la estimarea mai bună a necesităţilor reale şi reprezintă premisa unor viitoare îmbunătăţiri ale sistemului de asigurări de sănătate
- pentru medici:
  - consistenţa informaţiilor, centralizate într-o bază unică, şi păstrarea istoricului pentru fiecare pacient, asigură un plus de încredere în luarea deciziilor;
  - pot fi urmărite eventualele interferenţe ale diverselor tratamente acordate într-o anumită perioadă de timp, care ajută la luarea unei decizii medicale optime
  - administrarea unitară a informaţiilor aferente centralizat, asigură o diminuare a timpului în evaluarea situaţiei pacientului
  - utilizarea standardelor informatice medicale asigură interoperabilitatea şi schimbul de informaţii pentru pacienţii care solicită servicii medicale transfrontaliere
  - baza de date constituită reprezintă o arhivă electronică şi un back-up al informaţiilor fiecărui pacient
- pentru angajaţii Ministerului Sănătăţii:
  - multitudinea de statistici, care pot fi oferite în baza informaţiilor deţinute într-o bază de date reală şi curentă, sunt esenţiale în stabilirea politicilor în sistemul sanitar şi de luarea deciziilor ulterioare premiţînd:
    - asigurarea mediului necesar pentru controlarea impactului bolii la nivelul unei anumite comunităţi
    - planificarea mai eficientă a metodelor de prevenire a bolii
- monitorizarea serviciilor medicale oferite în tratamentul şi îngrijirea bolnavilor de boli profesionale

- Registrul operativ naţional informatizat al bolilor profesionale se doreste sa devina un suport pentru decidentii implicati in **managementul** riscurilor profesionale, a factorilor de risc profesional din mediul de munca, cu influente asupra sanatatii. Registrul operativ naţional informatizat al bolilor profesionale reprezinta un instrument de evaluare a impactului factorilor de risc profesional din mediul de munca asupra sanatatii populatiei active si un mijloc de **constientizare, informare si educare a lucratorilor** privind efectele pe termen scurt, mediu si lung asupra sanatatii.

Registrul privind gestionarea deseurilor rezultate din activitatea medicala
Inregistrarea furnizorilor de date
Această funcţionalitate permite introducerea informaţiilor despre furnizorii de date referitoare la gestionarea deseurilor medicale, care vor avea acces la Registrele specifice.

1. **Furnizorii de date**

- unitatile sanitare cu paturi generatoare de deseuri medicale (US);
- cabinetele de medicina de familie (CMF);
- cabinetele de stomatologie (CS);
- serviciile de medicina legala (SML);
- serviciile de ambulanta judetene (SAJ);
- alte unitati sanitare generatoare de deseuri medicale (AUS).

Se estimeaza ca vor raporta un numar de aproximativ de **15000 de furnizori de date.**

2. **Informaţiile utile - vor fi structurate pe grupe de date:**

Date de identificare furnizor:

- nume unitate sanitară;
- specialitate unitate sanitara;
- forma de proprietate publica/privata;
- numar total al personalului unitatii;
- numar total de paturi;
- denumire judeţ.
- denumire localitate;
- mediu urban/rural
- numele şi prenumele persoanei care raporteaza datele.

Date referitoare la categoriile de deseuri monitorizate:

- codul deseului;
- cantitate de deseuri generata pe categorii;
- cantitate de deseuri tratata;
- cantitate de deseuri incinerata;
- cantitate de deseuri depozitata.

Date referitoare la activitatea de gestionare a deseurilor la nivelul unitatii:

- modul de colectare si separare pe categorii a deseurilor medicale la nivelul unitatii;
- modul de stocare temporara a deseurilor medicale la nivelul unitatii;
- modul de transport a deseurilor medicale la nivelul unitatii;
- modul de tratare/eliminare a deseurilor medicale la nivelul unitatii;
- numar cazuri de imbolnaviri sau accidente in randul personalului, ca urmare a manipularii deseurilor medicale.

Datele de mai sus vor fi definitivate în etapa de analiză cu ajutorul specialiştilor stabiliţi de Ministerul Sănătăţii împreună cu persoanele care coordoneaza fiecare registru specific.

Pentru fiecare furnizor de date exista doua fise de raportare. Fisa 1 cuprinde monitorizarea lunara si raportarea trimestriala a datelor, iar fisa 2 cuprinde raportarea anuala a datelor privind evaluarea activitatii de gestionare a deseurilor medicale, la nivelul fiecarei unitati.

UNITATEA SANITARA

- Fisa (1) UNITATEA SANITARA (US) – cu paturi (monitorizare lunara si raportare trimestriala)
- Fisa (2) UNITATEA SANITARA – cu paturi (raportare anuala) – Raport privind activitatea de gestionare a deseurilor rezultate din activitatea medicala

Cabinete Medicina de Familie (CMF)

- Fisa 1 (monitorizare lunara si raportare trimestriala) – Cantitati (CMF)
- Fisa (2) – (raportare anuala) – Raport privind activitatea de gestionare a deseurilor rezultate din activitatea medicala – (CMF)

Cabinete de Stomatologie (CS)

- Fisa 1 (monitorizare lunara si raportare trimestriala) – Cantitati (CS)
- Fisa (2)– (raportare anuala) – Raport privind activitatea de gestionare a deseurilor rezultate din activitatea medicala (CS)

Serviciul de Medicina Legala (SML)

- Fisa 1 (monitorizare lunara si raportare trimestriala) – Cantitati - (SML)
- Fisa (2) – (raportare anuala) – Raport privind activitatea de gestionare a deseurilor rezultate din activitatea medicala – (SML)

Serviciul de Ambulanta Judetean (SAJ)

- Fisa 1 (monitorizare lunara si raportare trimestriala)- Cantitati (SAJ)
- Fisa (2) – (raportare anuala) – Raport privind activitatea de gestionare a deseurilor rezultate din activitatea medicala – (SAJ)

Alte unitati sanitare generatoare de deseuri medicale - (AUS)

- Fisa 1 (monitorizare lunara si raportare trimestriala) – Cantitati (AUS)
- Fisa (2) - (raportare anuala) – Raport privind activitatea de gestionare a deseurilor rezultate din activitatea medicala – (AUS)

Rapoarte

Se vor avea in vedere minim urmatoarele rapoarte:

- Centralizator cu nr total de unitati care au raporta pentru fiecare modul (cele 6 module)/la nivel de judet
- Harta interactiva cu nr. unitatilor sanitare cu paturi, care au raportat/judete, cu selectare:
    - Doar unitatile sanitare cu paturi publice
    - Doar unitatile sanitare cu paturi private
    - In functie de nr. total de paturi de la nivelul unitatii (producatori mari/mijlocii/mici)
    - Selectare in functie de specificul unitatii sanitare la cele publice: judetean, municipal, orasenesc, specialitati de chirurgie/pediatrie/etc
- Posibilitatea de a selecta o specialitate a unitatii sanitare cu paturi si afisare grafica a cantitalor de deseuri generate /pe parcursul unui an (cu afisarea lunilor) a tuturor unitatilor sanitare pe aceea specialitate (inclusive cu nr de paturi ocupate) - se poate urmari evolutia generarii cantitatilor de deseuri lunare – si depistare daca in loc de 100 kg intr-o luna, in medie, la urmatoarea luna a scapat un zero si apare 1000 kg, iar numarul de paturi ocupate nu s-a schimbat cu mult de la o luna la alta ca sa se justifice aceasta crestere.
- Afisare cantitatilor generate pe fiecare cod in parte si posibilitatea de a “merge in profunzime”: afisare doar pe regiune pt un anumit cod, si mai profund, pe judet sau pe toate spitale judetene de exemplu
- Centralizator cu judetele; nr unitatilor sanitare cu paturi (publice/private)/judet; cu numarul de total de paturi/judet; numarul total de paturi ocupate/judet; cantitati generate pe cele 9 coduri/judet/anual/lunar; cantitatea totala de deseuri pe judet;

- Centralizator la nivel de judet cu/nr unitati sanitare/ cantitatea generat/cantitatea tratata/cantitatea incinerate/cantitatea depozitata/cantitatea ramasa in stoc
- Harta interactiva – cu procent cantitatea de deseuri incinerate/tratata/judet.
- Centralizaotr cu medie de generare a deseurilor pe pat ocupat in functie de unitatea sanitara, la nivel de judet.
- Harta interactiva cu nr. cabinete care au raportat/judet, cu selectare:
  - in functie de specialitati (ex: CMF, CS, etc.)
  - in functie de mediul urban/rural
  - in functie de nr de pacienti
- Centralizator privind cantitatea medie generate/luna /coduri de deseuri/cabinet CMF/nr mediu de pacienti, la nivel de judet
- Centralizator privind cantitatea medie generate/luna /coduri de deseuri/cabinet CS /nr mediu de pacienti, la nivel de judet
- Centralizator privind cantitatea medie generate/luna /coduri de deseuri/cabinet SML /nr mediu servicii/investigatii/autopsii, la nivel de judet
- Centralizator privind cantitatea medie generate/luna /coduri de deseuri/cabinet SAJ /nr mediu solicitari, la nivel de judet
- Centralizator privind cantitatea medie generate/luna /coduri de deseuri/alte unitati sanitare AUS/nr. mediu …… (ex: cazuri, inestigatii) la nivel de judet
- Centralizator la nivel de judet, privind informatiile din Fisa 2 (raportare anuala) – pentru unitatile sanitare cu paturi
- Centralizator la nivel de judet, privind informatiile din Fisa 2 (raportare anuala) – pentru cabinete CMF
- Centralizator la nivel de judet, privind informatiile din Fisa 2 (raportare anuala) – pentru cabinete SC
- Centralizator la nivel de judet, privind informatiile din Fisa 2 (raportare anuala) – pentru cabinete SML
- Centralizator la nivel de judet, privind informatiile din Fisa 2 (raportare anuala) – pentru cabinete SAJ
- Centralizator la nivel de judet, privind informatiile din Fisa 2 (raportare anuala) – pentru cabinete alte unitati sanitare AUS
- Grafice la nivel national/judetean, exprimate procentual, privind raportarea unitatilor sanitare pe cele 6 module
- Grafice la nivel national/judetean, exprimate procentual, privind cantitatile generate pe cele 9 coduri/ anual

Beneficiari
Beneficiarii sunt reprezentati de catre Institutul National de Sanatate Publica, Ministerul Sanatatii, Directia de Sanatate Publica, unitatile sanitare publice si private, alte organisme interesate.

3.1.2. Disponibilitate ridicată

Sistemul informatic propus trebuie să fie disponibil online în permanenţă 24 de ore, 7 zile pe săptămână. Orice întrerupere accidentală va fi tratată cu maximă urgenţă, iar opririle programate pentru mentenanţă hardware şi software necesare vor trebui să fie anunţate în prealabil şi să se încadreze în afara intervalului orar 6:00 - 22:00.
Operaţiunile de realizare a copiilor de siguranţă trebuie incluse tot în intervalul de timp neprioritar. Salvarea datelor se va realiza în fiecare zi utilizând medii de stocare specifice.

În cazul unui incident se vor putea restaura rapid datele de pe unitatea de siguranţă pentru oricare din serverele de baze de date.

3.1.3. Administrare şi monitorizare

Sistemul informatic propus trebuie să pună la dispoziţia administratorilor o componentă pentru realizarea funcţionalităţilor necesare administrării sistemului precum şi pentru monitorizarea funcţionării acestuia în vederea urmăririi îndeplinirii obiectivelor de performanţă şi disponibilitate.
Aceasta componentă trebuie să răspundă următoarelor cerinţe generale:

- Definirea şi documentarea procedurilor şi proceselor necesare pentru operarea soluţiei.
- Minimum următoarele cerinţe vor fi acoperite de aceste proceduri şi definiţii de procese:
  - Operarea şi administrarea soluţiei în mod proactiv şi eficient
  - Monitorizarea permanenta a funcţionării sistemului cu alertarea anomaliilor – erori sau avertizări legate de funcţionalitate.
  - Readucerea sistemului în parametrii normali de operare
  - Persoane cu nivel mediu de cunoştinţe IT şi a produselor soluţiei să poată aplica procedurile definite.
- Toate componentele soluţiei vor înregistra principalele evenimente de succes sau de eroare în jurnale specializate care îndeplinesc următoarele cerinţe:
  - pot fi securizate pentru a limita accesul la aceste informaţii
  - permit consultarea lor directa de către un operator uman
  - permit interpretarea prin metode programatice – sunt organizate intr-un mod consistent şi structura este documentata.
- Toate componentele hardware şi software ale soluţiei respectă cerinţele de suportabilitate emise de producător.

Sistemul informatic propus trebuie să pună la dispoziţia administratorilor o componentă care va îndeplini atât funcţiile de audit informatic cât şi funcţiile de control al accesului la informaţii.
Soluţia de audit şi control va îndeplini următoarele cerinţe generale:

- Va păstra un istoric de tip log al activităţii utilizatorilor aplicaţiei.
- Va permite includerea informaţiilor despre momentul în care au fost modificate anumite seturi de date de către utilizatori, un istoric al tuturor modificarilor mai ales pe anumite date sensibile.

3.2. *Arhitectura funcţională a sistemului*

Prin arhitectura sistemului informatic înţelegem structurile, mecanismele şi interfeţele utilizate, precum şi comunicarea între părţile componente. Arhitectura de sistem descrie viziunea fizică şi logică a sistemului propus, relevă modul în care sistemul va fi construit, defineşte modul în care vor fi utilizate diferite concepte, cât şi aspecte vizând posibilitatea dezvoltării viitoare a sistemului.
Pentru arhitectura sistemului informatic se vor respecta următoarelor principii:

- implementarea unei soluții centralizate client-server WEB based cu acces autorizat la interfață și date, utilizand componente software mature, de tip COTS, cu drept de proprietate perpetuu;
- asigurarea unei securități adecvate a sistemului informatic pentru a proteja informația și subsistemele componente împotriva utilizării lor neautorizate sau a divulgării informației cu caracter personal sau a celei cu accesibilitate limitată;
- recunoașterea informației ca patrimoniu și gestionarea ei adecvată;
- dezvoltarea și implementarea sistemului informatic oferind posibilitatea reutilizării lor pentru alte procese sau în perspectiva asigurării posibilității de dezvoltare de noi funcționalități;

- asigurarea capacității de restabilire în urma dezastrelor (asigurarea securității fizice și logice) ca parte componentă a planului de implementare.

Soluţia tehnică pentru sistemul informatic propus va include, pe lângă sistemul de producţie, un subsistem de dezvoltare/testare şi instruire necesar exploatării în conformitate cu bunele practici internaţionale şi cu metodele actuale în domeniul formării profesionale continue a personalului. Astfel sistemul va include un mediu de producţie şi un mediu de dezvoltare/testare cu rol de a acoperi nevoile de dezvoltare, testare şi de integrare.

- **Mediul de producţie** este mediul principal folosit de utilizatorii soluţiei, implementând toate cerinţele funcţionale şi non-funcţionale.
- **Mediul de dezvoltare/testare** care îndeplineşte toate cerinţele funcţionale şi non-funcţionale ale mediului de producţie, mai puţin cele legate de performanţă şi disponibilitate, fiind utilizat pentru:
  - dezvoltarea de modificări ce vor fi aduse mediului principal de producţie;
  - testarea şi validarea modificărilor înaintea promovării acestora pe mediul de producţie;
  - validarea integrării cu sisteme externe;
  - instruirea utilizatorilor prin simularea de scenarii de utilizare reale folosind date de test, fără a afecta însă datele reale.

Din punct de vedere al arhitecturii fizice şi logice sistemul informatic propus trebuie să adere la următoarele principii arhitectonice:

- **Modularitate** – sistemul este descompus în subsisteme cu roluri şi caracteristici/ proprietăţi bine definite fără a avea o suprapunere de funcţionalităţi între două subsisteme
- **Deschidere** – pot fi adăugate componente, proprietăţi noi. Modulele (componentele), soluţiei au caracteristici generale, adaptabile în funcţie de cerinţele clientului;
- **Stratificare** – arhitectură separată pe mai multe straturi, fiecare strat având roluri şi responsabilităţi bine delimitate.
- **Flexibilitate** – arhitectura propusă se bazează pe standarde şi tehnologii deschise, sistemul fiind conceput modular astfel încât să poată integra uşor atât modificări ale funcţionalităţilor existente cat şi introducerea de noi funcţionalităţi
- **Scalabilitate** – utilizând tehnologii ce au suport pentru lucrul în arhitectura cluster suporta o scalare atât pe orizontala cat şi pe verticala pentru a acomoda uşor creşterea numărului de utilizatori sau a volumului de operaţii efectuate de aceştia
- **Eficienţă** – prin optimizarea utilizării resurselor hardware şi de comunicaţii şi prin eficientizarea activităţii operatorilor prin automatizarea activităţilor repetitive
- **Ergonomie** – prin utilizarea conceptelor moderne şi bunelor practici ale interacţiunii om-calculator, a standardelor legate de proiectarea interfeţelor utilizator, precum şi a principiilor de uzabilitate moderne şi a tendinţelor contemporane din domeniul aplicaţiilor Web.
- **Interoperabilitate** – prin integrarea programatică cu alte sisteme informatice bazate pe tehnologii eterogene prin intermediul uneia sau mai multor interfeţe programatice. Nefuncţionarea unuia din sistemele externe nu trebuie să afecteze disponibilitatea şi funcţionalitatea soluţiei.

Din punct de vedere funcţional sistemul informatic propus trebuie să îndeplinească următoarele obiective:

- Sistemul informatic online trebuie sa permita accesul sigur şi de încredere la informaţiile referitoare la pacienti şi la furnizorii de servicii medicale prin expunerea unor servicii de validare online pentru medici.
- Sistemul informatic va aplica măsuri uniforme pentru protecţia şi siguranţa datelor, indiferent de locul sau timpul accesării acestora;
- Sistemul informatic va face posibilă o colectare eficientă a datelor prin intermediul importului din fişiere formatate si a solutiilor de tip API, conform unei specificaţii standard.
- aplicațiile rulează pe sisteme de operare în mediu virtual;

- la defectarea unuia dintre servere, aplicațiile vor continua să ruleze pe celelalte servere fără ca utilizatorii să sesizeze întreruperi ale serviciului;
- legăturile dintre servere și sistemul de stocare se vor face exlusiv prin legături de mare viteză;
- sistemul de stocare va fi împărțit în volume separate pentru fiecare mașină virtuală, având capacitatea și nivelul RAID adecvat pentru fiecare tip de mașină (ex. baza de date, server aplicații etc);
- legătura de date dintre infrastructură și internet se va realiza exclusiv prin intermediul echipamentelor unificate de securitate și va fi protejată de acestea;
- pentru asigurarea unui nivel adecvat al securității informaționale soluția informatică implementată trebuie să permită realizarea de conexiuni securizate între terminalele utilizatorilor și serverul de aplicație pentru asigurarea siguranței informației expediate (prin intermediul sesiunilor SSL);
- infrastructura sistemului nu va avea niciun SPOF (Single Point of Failure);
- sistemul trebuie să fie scalabil, atât din punct de vedere hardware (adăugare de nuclee de procesare, memorie RAM sau discuri), software (adăugare de noi utilizatori), dar și din punct de vedere business (adăugare de noi funcționalități).

Categorii de utilizatori

- **Cetatean** - cetăţean înregistrat în sistemul de asigurare medicală, beneficiari de servicii medicale.
- **Furnizor de servicii** - Adăugare și gestionare pacienti, vizualizare, programare și evenimente (vizită medicală), import date, marcare obervații și discrepanțe, gestionare grupuri, reguli pentru registru, vizualizare și analiză
- **Administrator** - personal specializat în administrarea sistemului informatic, responsabil pentru administrarea utilizatorilor şi pentru gestiunea şi întreţinerea conţinutului publicat.
- **Operator** - personal care verifică datele din sistem, creează situaţii statistice, sau efectuează alte operaţii permise.
  Sistemul va permite definirea rolurilor pentru fiecare funcție importantă pentru fiecare categorie de utilizatori.

Sistemul informatic central va fi proiectat astfel încât să funcţioneze în regim de înaltă performanţă şi disponibilitate şi va fi separat pe trei niveluri, conform celor mai bune în domeniu: stocarea datelor, prelucrare şi prezentare.
Sistemul astfel proiectat va prezenta 3 zone distince:

- **Nivel de prezentare**: este compus din servere web de prezentare si acces la serviciile sistemului.
- **Nivel de aplicatie**: este compus din servere de aplicatii ce gestioneaza modulele software ce vor fi instalate.
- **Nivel baze de date**: trebuie sa fie constituit din servere de baza de date configurate in cluster mod activ activ care sa asigure balansarea incarcarii, precum si scalabilitate si disponibilitate maxima, pe care ruleaza sistemul de gestiune a bazei de date.

In cazul in care se utilizeaza mecanisme de virtualizare a resurselor hardware trebuie avut in vedere ca alocarile de resurse hardware pe cele 3 nivele sa fie facute intr-un mod eficient si care sa asigure parametrii de performanta necesari functionarii in conditii optime.
Zonele pot fi delimitate la nivel logic si separate prin intermediul functionalitatilor de tip firewall. Accesul utilizatorilor se va permite doar la nivelul de prezentare, iar cererile catre nivelul aplicativ vor gestionate de acesta. Utilizatorii nu trebuie sa aiba acces direct sub nici o forma catre nivelul bazelor de date.

3.3. *Managementul utilizatorilor si accesul la sistem*

Pentru asigurarea managementului utilizatorilor (administratori de sistem si cetateni - pentru zona publica) și accesului la sistem, se vor avea în vedere următoarele:

- identificarea în mod unic a fiecărui utilizator în sistem prin crearea de conturi unice și personalizate de acces;
- gestionarea centralizată și unitară a accesului utilizatorilor în sistem prin autorizarea utilizatorului doar la componentele și modulele funcționale ale sistemului conform cu drepturile de acces și atribuțiile specifice;
- accesul la sistem se va putea realiza doar prin autentificarea utilizatorilor, excepție făcând doar acele informații de interes public publicate în portal.

Managementul utilizatorilor si accesul lor in sistem implică obținerea accesului la credențiale privilegiate de catre administratori, întrucât acestea oferă acces extins, și în unele cazuri, nelimitat (de ex.: root, administrator) la sisteme și date.

3.4. *Securitatea sistemului*

Sistemul va fi proiectat astfel încât să respecte Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE precum si legislatia nationala in domeniul prelucrarii datelor cu caracter personal.
Sistemul informatic trebuie să fie protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care aceasta le gestionează. Designul soluției de securitate trebuie să fie astfel conceput încât să asigure securitatea și confidențialitatea atât a datelor personale ale utilizatorilor, dar și a conținutului și a anumitor funcționalități ale aplicației, astfel încât utilizatorii să acceseze doar acele secțiuni și conținut care le este permis prin apartenența la un profil sau machete de securitate.
Soluția de securitate vă fi astfel configurată încât:

- Să nu permită persoanelor neautorizate modificarea sau alterarea semantică a informațiilor din sistem;
- Să asigure consistența datelor și să permită identificarea sursei datelor inițiale și a persoanelor care au accesat sau au înregistrat aceste date în sistem;
- Să asigure securizarea/protecția datelor vehiculate în sistem pe mai multe niveluri – la nivel de acces în rețea, la nivel de aplicație și la nivel de baza de date.
-

3.4.1. Securitatea logică

Prevederile de securitate vor fi implementate la următoarele niveluri ale soluției informatice propuse:
Controlul Accesului Logic

- Nu se permite acces neautentificat la date și informații (mai puțin secțiunea publică a nodului). Orice acces în aplicație, atât la nivelul utilizatorilor cât și la nivelul altor module de aplicație, este precedat de identificarea, autentificarea și autorizarea accesului;
- Parolele de acces între modulele aplicației (de ex: la baza de date) sunt stocate criptat în fișierele de configurare;
- Credențialele de acces nu se transmit în clar prin rețea între componentele sistemului;
- Sesiunile de lucru inactive trebuie să expire după o perioadă de timp configurabilă (implicit 10 minute);
- Serviciile și porturile de comunicație folosite vor fi documentate într-o listă a serviciilor utilizate. Serviciile și porturile neutilizate vor fi dezactivate;
- Sistemul informatic și componentele acestuia se vor instala și configura numai pe sisteme care au aplicate ultimele patch-uri de securitate.

Jurnalizare, monitorizare, auditare
Jurnalizarea evenimentelor semnificative legate de controlul accesului

- Înregistrarea în jurnal a autentificărilor cu succes (dată, oră, adresa IP)
- Înregistrarea în jurnal a autentificărilor fără succes (dată, oră, adresa IP)
- Aceste jurnale vor fi disponibile în aplicație pentru vizualizare de către administratorii sistemului.

Testare de securitate

Aplicația va fi supusă unor verificări riguroase de securitate (auditare de securitate și test de penetrare) pentru a se identifica și elimina orice vulnerabilități înainte de a se utiliza în producție, precum și regulat, la intervale definite de timp. Testele vor respecta cel puțin metodologiile OSSTM (Open Source Security Testing Methodology) sau OWASP (Open Web Applications Security Project). Raportul final de testare de securitate vă cuprinde vulnerabilitățile existente în cadrul sistemului și componentelor acestuia, și va fi structurat astfel:

- Sumar Executiv;
- Obiectivele și scopul evaluării;
- Prezentare succintă a metodologiei utilizate;
- Descrierea contextului în care s-a desfășurat evaluarea;
- Lista testelor de securitate efectuate;

Prezentarea individuală a vulnerabilităților descoperite după cum urmează:

- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnică;
- Analiza severității și probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere;
- Alte detalii și recomandări.

Scanarea de vulnerabilități informatice se va realiza prin utilizarea de aplicații dedicate și actualizate la momentul realizării scanărilor. În acest sens se vor utiliza aplicații care să conțină baze de date de vulnerabilități la nivel de rețea, sisteme de operare, aplicații/servicii, care, pe de-o parte, trebuie să permită auditarea activităților realizate astfel încât să poată fi demonstrată efectuarea acestor activități și, pe de altă parte, să conțină baze de date actualizate cu exploit-uri (coduri care demonstrează că o vulnerabilitate poate fi exploatată însă fără ca sistemul să fie propriu-zis compromis).

3.5. *Confidențialitatea datelor*

Confidențialitatea este o activitate de bază pentru furnizarea serviciilor publice.

In cadrul proiectului se vor respecta urmatoarele principii:

- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că respectă cerințele și obligațiile juridice privind **protecția și confidențialitatea datelor** recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

De asemenea, trebuie să asigure respectarea de către operatori a legislației privind protecția datelor, prin:

- **„Planuri de gestionare a riscurilor”** pentru identificarea riscurilor, evaluarea potențialului impact al acestora și planificarea intervențiilor cu măsuri tehnice și organizatorice adecvate. Pe baza ultimelor evoluții tehnologice, aceste măsuri trebuie să asigure un nivel de securitate proporțional cu gradul de risc;
- **„Planuri de continuitate a activității”** și **„planuri de rezervă și de redresare”** pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucerea tuturor funcțiilor la situația normală cât mai curând posibil;

- Un **„plan de acces la date și autorizare”** care stabilește persoanele care au acces la date, datele care sunt accesibile și condițiile accesării datelor, pentru a asigura confidențialitatea. Accesul neautorizat și încălcarea normelor de securitate trebuie monitorizat, și măsurile corespunzătoare pentru a preveni orice repetare a încălcărilor trebuie documentate si planificate;
- Utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS[2] pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

[2] Regulamentul (UE) nr. 910/2014.

3.6. *Arhitectura tehnica*

Fig. 1 Arhitectura fizica RegInterMed

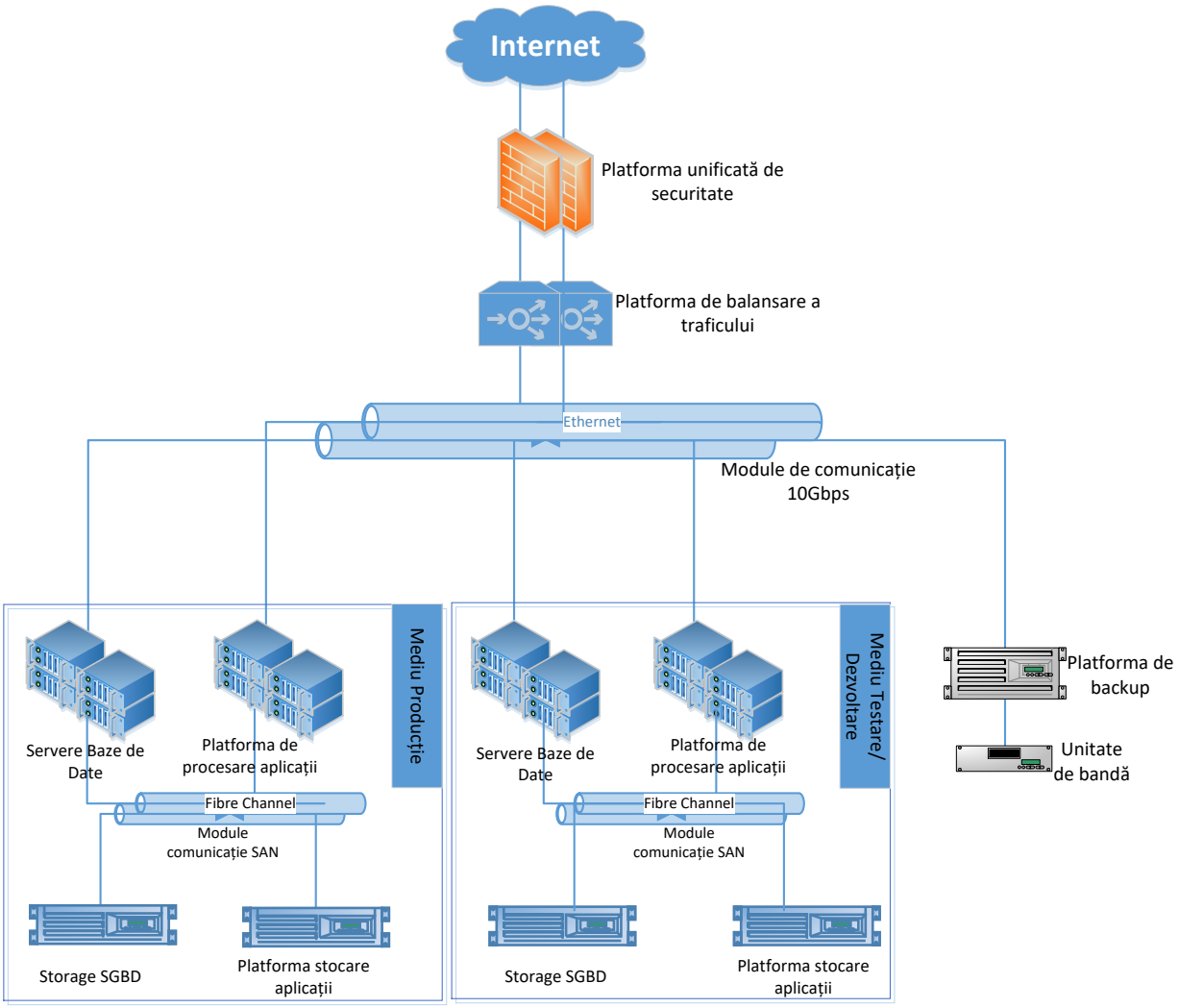
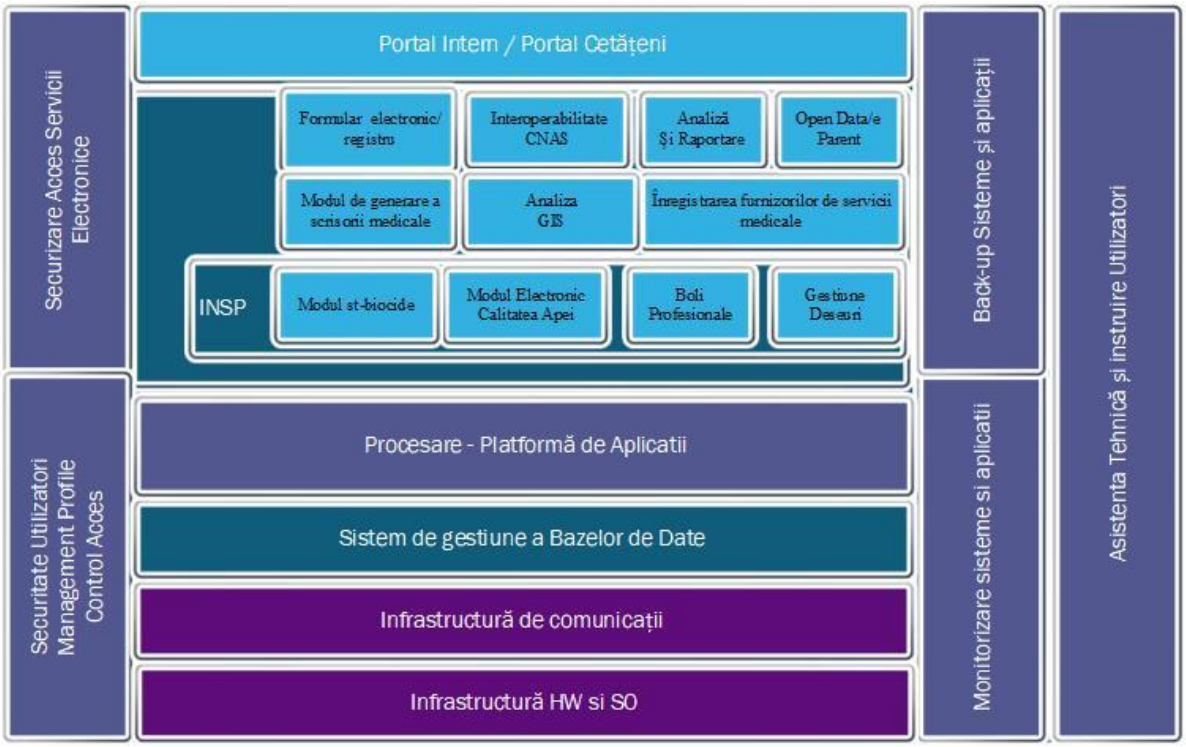
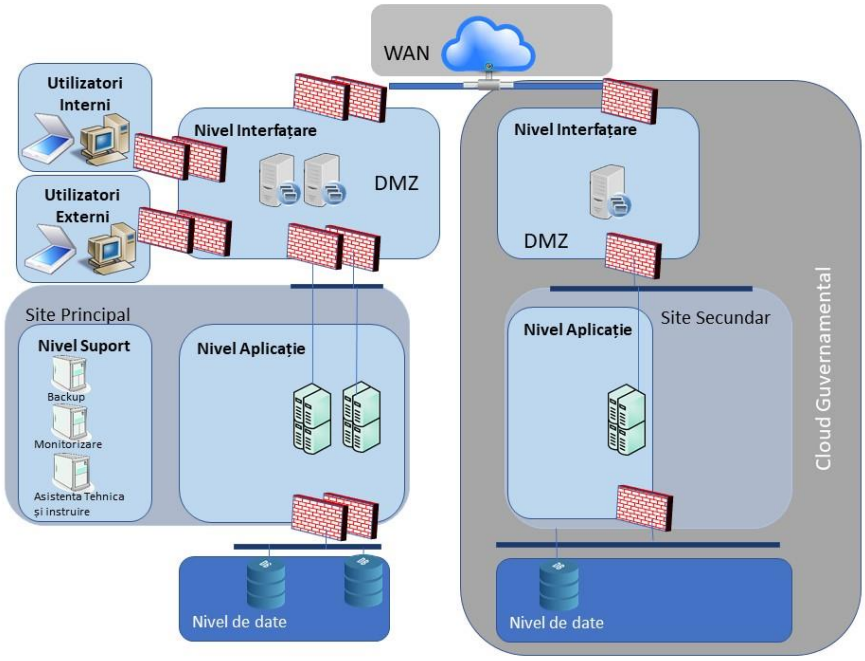


Fig. 2 Arhitectura logica RegInterMed



Se va configura un site de tip Disaster Recovery care va folosi infrastructura hardware si de comunicatii pusa la dispozitie de cloud-ul guvernamental la aceleasi capacitati cu cele ale mediului de productie.
Nu se vor achizitiona licente pentru site-ul de DR.

Fig. 3 Arhitectura DR



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 trebui 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**
1.	Portal	2	Cluster Activ-Activ	8
2.	Server web/Reverse proxy	2	Cluster Activ-Activ	8
3.	Platforma de aplicatii	2	Cluster Activ-Activ	8
4.	Componenta de interoperabilitate	2	Cluster Activ-Activ	16
5.	SGBD	2	Cluster Activ-Activ	8
6.	Analiza si Raportare – BI	2	Cluster Activ-Pasiv	16
7.	Securitate Utilizatori: Managementul profilelor Control acces LDAP Securizare acces servicii electronice	2	Cluster Activ-Pasiv	 12 32 12 8
8.	Consolidare si replicare de date	2	Cluster Activ-Pasiv	8
9.	Monitorizare date, sisteme si aplicatii	1		24
10.	Asistenta tehnica	1		12
11.	Monitorizarea logurilor si a traficului de retea	1		46
12.	Componenta de mascare a datelor	1		16
13.	Componenta de securizare a accesului la bazele de date	2	Cluster Activ-Pasiv	16
14.	Recuperare in caz de dezastru	1		8
15.	Componenta GIS	2	Cluster Activ – Pasiv	16

3.7. *Componente hardware si de comunicatii pentru nodul central*

RegInterMed va fi compus din cel puțin urmatoarele componente hardware și de comunicații pentru nodul principal care va fi localizat la sediul STS:

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.	Platforma de procesare aplicații pentru mediul de productie	2
4.	Platforma de procesare aplicații pentru mediul de test/dezvoltare	1
5.	Echipamente de procesare aplicații pentru mediul de productie	14
6.	Echipamente de procesare aplicații pentru mediul de test/dezvoltare	10
7.	Platforma de interconectare - Echipamente de comunicatie si interconectare integrate in sasiu – Ethernet 10 Gbps	6
8.	Platforma de interconectare - Echipamente de comunicatie si interconectare integrate in sasiu – Fibre Channel 16 Gbps	6
9.	Platforma de interconectare - Echipamente de comunicatie SAN – Fibre Channel 16 Gbps	4
10.	Platforma de interconectare - Echipamente de comunicatie pentru interconectare interna - Ethernet 10 Gbps	2
11.	Platforma de stocare pentru baza de date si aplicații pentru mediul de productie	1
12.	Platforma de stocare pentru baza de date si aplicații pentru mediul de test/dezvoltare	1
13.	Platforma unificata de backup	1
14.	Platforma de securizare a masinilor virtuale	1
15.	Platforma de balansare a traficului de aplicatie	2
16.	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.

3.7.1. Suport fizic de tip rack pentru montarea şi poziţionarea echipamentelor – 5 buc

Ansamblu modular standard de 19 inchi, cu 42U disponibili pentru pozitionarea echipamentelor.Se vor include reperele de montare necesare, inclusiv şine extensibile telescopic (sau soluţii similare) cel puţin 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.) şi deservirea acestora fără a fi necesară oprirea funcţionării şi/sau deconectarea echipamentului (ori de câte ori acest lucru este posibil din punct de vedere funcţional).
Structura internă a rack-ului va facilita poziţionarea cablurilor, pentru distribuirea echilibrată a bugetului de conexiuni, respectiv pentru a implementa o schemă de asigurare a redundanţei (la nivel de alimentare, interconectare SAN, LAN, etc.) şi evitarea condiţiilor de tip single-point-of-failure.
Suport fizic de tip rack pentru montarea şi poziţionarea 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 montate	Sine telescopice care sa permita extractia completa a echipamentelor montate. 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.
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 funcționalitățile 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 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

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 funcționare in regim de avarie de minim 15 de minute la o încărcare preconizata de minim 50%.
Soluția 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.
Unitățile 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 unităților 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 aplicații

In stransa legatura si prin integrarea cu celelalte elemente de infrastructura solicitate, specific cu platforma de stocare si platforma de virtualizare, platforma de procesare aplicații 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 si aplicare proactiva de politici asupra resurselor fizice si virtuale 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, distribuirea uniforma a capacitatilor de procesare si stocare cu imbunatatirea semnificativa a gradului de utilizare relativ la fiecare resursa fizica, diminuarea costurilor operationale.

Platforma de procesare aplicații 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 toate nodurile de procesare, respectiv pentru fiecare instanţă de hypervizor instalata pe acestea, 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 profesionale de monitorizare care vor rula în background şi vor putea genera rapoarte detaliate (cel puţin despre comportamentul procesoarelor, al memoriei şi al sub-sistemelor interne de I/O) utilizabile direct pentru reconfigurarea (fine-tuning) parametrilor relevanţi.

Soluţia/componentele oferite trebuie să îndeplinească următoarele cerinţe functionale 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.

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;
- Dispozitivele hardware trebuie să fie compatibile cu caracteristicile reţelei electrice din România astfel încât să nu existe probleme la conectarea acestora la reţeaua electrică;
- 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); în momentul reboot-ului componentele defecte vor fi deconfigurate;
    - 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, balansarea si integrarea modulelor de procesare, de stocare si a extensiilor de I/O ale acestora, precum şi a modulelor de management; ▪ Sasiul trebuie sa suporte interconectarea cu alte sasiuri similare si agregarea resurselor de procesare, stocare si a extensiilor I/O ale acestora intr-o singura platforma unificata, 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 un numar minim de 14 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, management (inclusiv procesoare de serviciu / management); ▪ Midplane de înaltă disponibilitate care suportă funcţii de tip hot-swap la nivel de server blade individual, module de interconectare LAN, module de management, surse de alimentare;
Dimensiune	Configurat cu toate modulele de procesare, comunicatie si management
Interfete I/O	▪ Suport pentru minim 2 module I/O interne pentru interconectare în tehnologie 1Gbps Gigabit Ethernet, 10/40 Gbps Ethernet, 8/16 Gbps Fibre Channel sau InfiniBand (QDR/FDR); ▪ 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 integrat si virtualizat, disponibil la toate nivelurile platformei (module fizice de procesare, stocare, comunicatie, management, module virtuale), respectiv unificat din punct de vedere al interfetei de acces, sasiul modular pentru suportul procesarii centralizate trebuie sa includa componente redundante de management dedicate functiilor administrative primare.
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”;

Caracteristica	Cerinta tehnica minimala
	▪ 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 şasiurile ofertate;
Procesor	▪ Minim 2x Procesor cu 22 core-uri de procesare, frecvenţa 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 256 GB 2933MHz 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 1,5 TB RAM prin extindere ulterioară;
Interfete I/O	▪ Suport pentru minim 2 module I/O interne pentru interconectare în tehnologie 1/10 Gbps Ethernet, 16 Gbps Fibre Channel; ▪ Minim 1 port 10 Gbps Ethernet integrat, suport pentru failover şi load balancing, suport TCP/IP Offload Engine (TOE), Virtual LANs (VLANs), IEEE 802.3ad Link Aggregation, Jumbo Frames (9 KB), IEEE 802.3x Flow Control, SR-IOV, PXE, IEEE 802.1au, IEEE 802.1p, IEEE 802.1Qaz DCBX, Load Balancing, LACP; ▪ Minim 1 port 16 Gbps Fibre Channel;
Stocare interna	Minim 2 harddisk-uri SAS de 300 GB, configurate in RAID 1 si controler RAID cu suport pentru RAID 0, 1
Sloturi de expansiune	Suport pentru module integrabile pentru extinderea numarului de porturi PCI Express disponibile (minim 2 porturi PCI Express aditionale);
Management	▪ Procesor de management integrat, capabilităţi de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local şi la distanţă; ▪ Sistem predictiv de analiza a componentelor modulului (procesoare, memorie, discuri), alertare in cazul depasirii pragurilor optime de functionare, respectiv actiuni automate de corectare a respectivelor erori si evenimente; ▪ Integrare intre modulul de management din fiecare sistem blade si modulul de management avansat disponibil in sasiul suport de multi-procesare;

Caracteristica	Cerinta tehnica minimala
	▪ Functii de monitorizare si acces de la distanta prin intermediul interfetelor standardizate: IPMI 2.0, SNMP v3. CIM, interfata web dedicata; ▪ 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, configurare pe baza de asistenti; 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 unificata de stocare, platforma unificata de backup 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

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 distincte de echipamente redundante de comunicatie atat in tehnologie 10 Gbps Ethernet cat si 16 Gbps Fibre Channel.

Echipamente de comunicatie 10 Gbps Ethernet – 6 buc
Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare, platforma de backup si restul de elemente de infrastructura, respectiv pentru asigurarea conexiunilor transparente catre platforma de virtualizare si masinile virtuale disponibile in aceasta, fiecare sasiu din platforma de procesare trebuie sa includa 2 echipamente redundante de comunicatie Ethernet 10 Gbps integrate. Echipamentele vor respecta fiecare urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Echipament de comunicatie 10 Gbps Ethernet cu management Layer 2/3

Caracteristica	Cerinta tehnica minimala
Interfete I/O	▪ Pentru functionalitati de switching la Layer 2/3 trebuie sa includa nu mai putin de 24 conexiuni active de tip 10 Gbps Ethernet ce pot fi alocate dinamic atat intern catre modulele de procesare cat si extern catre porturile de uplink; ▪ Porturile Ethernet 10 Gbps trebuie sa suporte echiparea cu conectori SFP+ pentru fiecare server blade. ▪ 2 porturi Ethernet 1 Gbps Full-Duplex pentru conectarea interna la modulele de management din sasiu; ▪ 2 porturi 40 Gbps Ethernet, echipate cu conectori QSFP+ si activate in configuratia ofertata;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 1 Tbps; ▪ Suport pana la 128 de adrese IP/rute statice pentru fiecare modul de comunicatie in parte; ▪ Suport pentru agregarea conexiunilor atat in mod static cat si in mod LACP, cu un maxim de 64 de grupuri de interfete cu cate 16 porturi per grup pentru un total de 220 Gb de trafic per modul de comunicatie; ▪ Arhitectura de tip non-blocking cu functionalitati pentru Broadcast/Multicast Storm Control; ▪ Capabilitati de virtualizare a interfetelor de comunicatie (vNIC); ▪ 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 configuratii de tip activ/pasiv in agregarea conexiunilor de retea din modulele de procesare; ▪ 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 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, BGP-4), cu un minim de 2048 de intrari in tabela de rutare; ▪ Suport atat pentru IPv4 cat si IPv6; ▪ Capabilitatea de a crea interfete virtuale si agregari de interfete virtuale ▪ Posibilitatea de a imparti modulele de comunicatie in mai multe module de comunicatie virtuale, fiecare adresabile in mod individual; ▪ Posibilitatea de a interconecta modulele de comunicatie intre ele astfel incat sa se creeze o stiva de comunicatie; ▪ Suport pentru SNMP v1, v2 si v3, acces prin interfata web, acces prin Telnet, SSH, si SFTP; ▪ Suport pentru actualizari de firmware in mod securizat (TFTP); ▪ Suport pentru sincronizarea de timp in protocol NTP si PTP;

Caracteristica	Cerinta tehnica minimala
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 16 Gbps Fibre Channel – 6 buc

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma unificata de stocare, platforma unificata de backup si restul de elemente de infrastructura, respectiv pentru asigurarea conexiunilor transparente catre platforma de virtualizare si masinile virtuale disponibile in aceasta, fiecare sasiu din platforma de procesare trebuie sa includa 2 echipamente redundante de comunicatie de tip Fibre Channel 16 Gbps integrate. Echipamentele vor respecta fiecare urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Echipament de comunicatie 16 Gbps Fibre Channel;
Interfete I/O	▪ Pentru functionalitati de tip SAN trebuie sa includa nu mai putin de 24 conexiuni active de tip 16 Gbps Fibre Channel ce pot fi alocate dinamic atat intern catre modulele de procesare cat si extern catre porturile de uplink; ▪ Porturile Ethernet 16 Gbps Fibre Channel trebuie sa suporte echiparea cu conectori SFP+, iar in configuratia ofertata un minim de 8 porturi trebuiesc efectiv echipate cu conectori SFP+; ▪ 2 porturi Ethernet 1 Gbps Full-Duplex pentru conectarea interna la modulele de management din sasiu; ▪ 1 port Ethernet 1 Gbps Full-Duplex pentru acces extern la functiile administrative;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 750 Gbps; ▪ Suport pentru compresie/decompresie FC in-line cu o viteza de minim 60 Gbps, respectiv criptare/decriptare FC in-line cu o viteza de minim 30 Gbps; ▪ Suport pentru minim 40 de canale virtuale de comunicatie per port FC; ▪ Scalabilitate de pana la 200 de module de comunicatie FC in topologie de tip Full Fabric; ▪ Arhitectura de tip non-blocking cu functionalitati pentru Dynamic Fabric Provisioning (DFP), Dynamic Path Selection (DPS), FDMI, Frame Redirection, Frame-based Trunking, FSPF, IpoFC, Port Fencing, Reliable Commit Service (RCS), Simple Name Server (SNS); ▪ 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 v1, v2 si v3, acces prin interfata web, acces prin Telnet, SSH, si SFTP; ▪ Suport pentru actualizari de firmware in mod securizat (SFTP); ▪ Suport pentru sincronizarea de timp in protocol NTP si PTP; ▪ Suport pentru transmiterea evenimentelor de stare direct catre modulele de management integrate in platforma de procesare;

Caracteristica	Cerinta tehnica minimala
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 SAN – 4 buc

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare, platforma unificata de backup 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 Gbps.
Cele patru echipamente vor respecta fiecare urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Echipament de comunicatie 16 Gbps Fibre Channel;
Dimensiune	Configurat cu toate modulele de comunicatie nu trebuie sa depaseasca 2U;
Interfete I/O	▪ Pentru functionalitati de tip SAN trebuie sa includa cel putin de 24 conexiuni active de tip 16 Gbps Fibre Channel; ▪ Porturile Ethernet 16 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+; ▪ 2 porturi Ethernet 1 Gbps Full-Duplex pentru acces extern la functiile administrative;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 350 Gbps; ▪ Suport pentru tehnologii de tip N_Port ID Virtualization (NPIV), Mirror Port (M-Port) si Diagnostic Port (D_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; ▪ Arhitectura de tip non-blocking cu functionalitati pentru Dynamic Fabric Provisioning (DFP), Dynamic Path Selection (DPS), FDMI, Frame Redirection, Frame-based Trunking, FSPF, IpoFC, Port Fencing, Reliable Commit Service (RCS), Simple Name Server (SNS); ▪ Suport Pentru Broadcast, Unicast si Multicast; ▪ Suport pentru cel putin 128 de domenii de tip Fabric, respectiv posibilitatea de functionare in mod Full Fabric sau Access Gateway; ▪ 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 v1, v2 si v3, acces prin interfata web, acces prin Telnet, SSH, si SFTP; ▪ Suport pentru actualizari de firmware in mod securizat (SFTP); ▪ Suport pentru sincronizarea de timp in protocol NTP si PTP; ▪ Licentiere completa a tuturor facilitatilor oferite de echipament, dar nu mai putin decat urmatoarele: ▪ Licenta monitorizare, management si diagnosticare;

Caracteristica	Cerinta tehnica minimala
	▪ 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 (suporţi, şuruburi/captive);

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

Pentru asigurarea interconectarii redundante cu platforma de procesare, platforma de stocare, platforma unificata de backup 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 Gbps Ethernet cu management 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 Gbps Ethernet; ▪ Porturile Ethernet 10 Gbps trebuie sa suporte echiparea cu conectori SFP+, iar in configuratia ofertata un minim de 24 porturi trebuiesc efectiv echipate cu conectori SFP+; ▪ 1 port Ethernet 1 Gbps Full-Duplex pentru acces extern la functiile administrative; ▪ 4 porturi 40 Gbps Ethernet, echipate cu conectori QSFP+ si activate in configuratia ofertata;
Caracteristici	▪ Throughput total pentru fiecare modul de comunicatie de minim 1,2 Tbps; ▪ Throughput total in pachete/secunda de minim 900 Mbps; ▪ Suport pana la 128 de adrese IP/rute statice pentru fiecare modul de comunicatie in parte; ▪ Suport pentru agregarea conexiunilor atat in mod static cat si in mod LACP, cu un maxim de 64 de grupuri de interfete cu cate 32 porturi per grup; ▪ Arhitectura de tip non-blocking cu functionalitati pentru Broadcast/Multicast Storm Control; ▪ Suport pentru functionalitati de tip Flow Control; ▪ Capabilitati de virtualizare a interfetelor de comunicatie (vNIC); ▪ 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;

Caracteristica	Cerinta tehnica minimala
	▪ 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 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, BGP-4), cu un minim de 2048 de intrari in tabela de rutare; ▪ Suport atat pentru IPv4 cat si IPv6; ▪ Posibilitatea de a imparti modulele de comunicatie in mai multe module de comunicatie virtuale, fiecare adresabile in mod individual; ▪ Posibilitatea de a interconecta modulele de comunicatie intre ele astfel incat sa se creeze o stiva de comunicatie; ▪ Suport pentru SNMP v1, v2 si v3, acces prin interfata web, acces prin Telnet, SSH, si SFTP; ▪ Suport pentru actualizari de firmware in mod securizat (TFTP); ▪ Suport pentru sincronizarea de timp in protocol NTP si PTP;
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 unificata 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 nodurile active de control vor fi simultan conectate la toate structurile de tip bus sau loop (SAS loops şi similare), pentru a face posibilă arondarea iniţială şi reconfigurarea ulterioară facilă a alocării discurilor între nodurile de control, între diferitele volume (sau structuri similare), precum şi între servicii diferite (SAN/NAS).
Platforma unificata de stocare pentru mediul de productie trebuie sa indeplineasca urmatoarele specificatii tehnice minimale:

Caracteristica	**Cerinta tehnica minimala**
Descriere	Platforma unificata de stocare pentru mediul de productie;
Arhitectura	▪ Soluţia de stocare trebuie sa fie echipata cu doua controllere (SAN/NAS) in acelasi sasiu 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;
Protocol de acces la date	Soluţia de stocare trebuie să ofere acces la datele stocate atat prin protocol de tip block (SAN), prin FC (Fiber Channel) precum si prin protocol de tip file (NAS), prin NFS (v2/v3/v4) si CIFS (SMB2/SMB3);
Porturi instalate	▪ Platforma trebuie să dispuna de minim 4 porturi SAS 12 Gbps, câte 2 pe fiecare controler; ▪ Platforma trebuie să dispuna de minim 8 porturi 10 Gbps Ethernet, câte 4 pe fiecare controler, echipate efectiv cu conectori SFP+; ▪ Platforma trebuie să dispuna de minim 8 porturi 16 Gbps FC, câte 4 pe fiecare controler, echipate efectiv cu conectori SFP multi-mode; ▪ Platforma trebuie să dispuna de minim 2 porturi 1 Gbps Ethernet dedicate interfetelor de management
Memorie	▪ Soluţia de stocare trebuie să aibă o cantitate de memorie de minim 48 GB per controler; ▪ Platforma va include extinderea memoriei cache Read/Write cu discuri in tehnologie SSD, cu o capacitate totala minima de 1 TB (configurata redundant cu minim un disc de tip hot-spare), pentru intreaga platforma, indiferent de marimea volumelor de date accelerate, respectiv de tipul de protocol folosit pentru accesul la accesul la volumele de date accelerate (SAN/NAS);

Caracteristica	Cerinta tehnica minimala
Nivele RAID	Configurarea si optimizarea matricilor RAID in configuratii cu unul si doua discuri de paritate asociate fiecarui set de discuri componente al unei matrici RAID, precum si posibilitatea de a folosi aceste matrici RAID in mod de replicare integrala de tip mirror, respectiv in agregare de performanta de trip stripe;
Conexiuni SAN	▪ Minim 220 host-uri per platforma de stocare, prin conexiune intermediara de tip Full Fabric; ▪ Minim 250 LUN-uri per platforma de stocare;
Hard discuri	▪ Suport pentru echiparea cu minim 200 de discuri; ▪ Trebuie sa permita utilizarea in paralel a discurilor de tip SAS 6/12 Gbps, NL-SAS 3 Gbps, SSD; ▪ Capacitatile pentru un HDD minim disponibile trebuie sa fie de 2 TB pentru discurile NL-SAS, 600 GB pentru cele SAS, 400 GB pentru cele SSD;
Capacitate instalata	Echipamentul trebuie sa ofere o capacitate minima utila, instalata la livrare, ce se va incadra in urmatorii parametri: ▪ Minim 127 TB capacitate utila totala, in configuratie echivalent RAID 10; ▪ Sa contina atat discuri SSD cat si discuri rotative de 7200/10000/15000 RPM; ▪ Proportia de discuri de tip SSD trebuie sa reprezinte minim 10% din totalul de capacitate utila instalata; ▪ Proportia de discuri rotative cu 10000 RPM trebuie sa reprezinte minim 40% din totalul de capacitate utila instalata; ▪ Proportia de discuri rotative cu 7200 RPM trebuie sa reprezinte maxim 50% din totalul de capacitate utila instalata; ▪ Toate discurile trebuie sa foloseasca interfata de tip SAS 12Gbps; ▪ Pentru fiecare matrice RAID 10 se va aloca cel putin un SSD/HDD pentru hot-spare sau global-spare in functie de solutia tehnica ofertata; ▪ Ofertantul va prezenta detaliat numarul de SSD/HDD ofertat, capacitatea de stocare reala rezultata si numarul si tipul SSD/HDD definite ca hot-spare sau global-spare;
Extensia capacitatii de stocare	Platforma de stocare trebuie să asigure următoarea capabilitate minimă de extensie a capacităţii de stocare: ▪ Suport pentru de discuri interne in sistemul de stocare ofertat, de tip hot-swap; ▪ Suport pentru module de expansiune cu discuri de 3,5” respectiv 2,5”; ▪ Modulele de expansiune trebuie sa se conecteze la echipamentul de stocare prin magistrale de date redundante, cu latime de banda de cel putin 48 Gbps (SAS 12 Gbps cu 4 cai de acces).
Managementul platformei	▪ Platforma de stocare trebuie să asigure un sistem de management şi monitorizare integrat; ▪ Platforma de stocare trebuie să aibă capabilitatea de monitorizare şi management a mai multor echipamente din aceeaşi gamă într-o singură instanţă a interfeţei, atât pentru serviciile SAN, cât şi pentru cele NAS; ▪ Platforma de stocare trebuie să asigure provizionarea automată a sistemelor de fişiere; ▪ Platforma de stocare trebuie sa asigure monitorizarea performantei si capacitatii platformei de stocare atat la nivel fizic cat si la nivel

Caracteristica	Cerinta tehnica minimala
	virtual.Solutia trebuie sa asigure functionalitatile respective atat pentru platforma propusa cat si pentru alte platforme de la acelasi producator; ▪ Echipamentul trebuie 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/Telnet. Toate functiile sistemului de stocare, separat trebuie sa fie accesibile prin intermediul acestor unelte de administrare, astfel incat operatiunile de configurare si administrare sa poata fi efectuate indiferent de locatie si de modalitatea de acces. Deasemenea pentru integrarea in aplicatii si unelte comune de management, disponibile in alte platforme si sisteme de operare, echipamentul trebuie sa permita cel putin integrarea uneltelor de administrare in console de tip MMC; ▪ Atat in scop administrativ cat si in vederea accesului la seturile de date, echipamentul trebuie sa permita definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita 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 trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp. Mecanismele de export ale volumelor prin intermediul protocolului CIFS trebuie sa beneficieze de suportul integrarii echipamentului de stocare cu sistemele de tip director si cu serverele de timp; ▪ Uneltele de administrare prin interfata web si/sau aplicatie dedicata trebuie sa fie usor de folosit si sa implementeze majoritatea actiunilor administrative (definirea de volume, LUN-uri, exportul seturilor de date indiferent de protocolul folosit pentru export, configurarea functiilor de partajare, optimizare si backup, adaugarea/eliminarea de noduri la/din cluster, definirea relatiilor de replicare, etc) intr-o singura interfata fara a fi nevoie de acces la uneltele in linie de comanda, iar pentru un numar de operatiuni importante de configurare sa puna la dispozitie asistenti de configurare.Uneltele trebuie sa permita atat configurarea si administrarea sistemului curent cat si orice alt sistem existent de la acelasi producator, indiferent de gama si/sau generatie. Deasemenea trebuie sa integreze 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; ▪ Tot ca parte a uneltelor standard de administrare, echipamentul trebuie sa includa posibilitatea de integrare cu platforma de virtualizare aleasa astfel incat sa permita definirea volumelor, LUN-urilor, aplicarea politicilor si mecanismelor integrate de optimizare, backup si recuperare,

Caracteristica	Cerinta tehnica minimala
	efectuarea operatiunilor de instantiere rapida a seturilor de date ce apartin de masinile virtuale, analizarea si corectarea dinamica a parametrilor de export ai seturilor de date catre platforma virtuala, identificarea si modificarea modului de aliniere logica a partitiilor din sistemele de operare virtuale, direct din uneltele de management puse la dispozitie de platforma de virtualizare, fara a folosi un alt set de unelte terte ce nu apartin nici de platforma de stocare, nici de cea de virtualizare. Astfel se obtine o platforma unitara de management, ce reduce efortul si costul administrativ, indiferent de natura operatiunilor efectuate; ▪ Platforma de stocare trebuie sa permita accelerarea hardware a operatiunilor ce au loc intre hipervizor si sistemul de stocare, prin degrevarea unor procese de la nivelul hipervizorului si preluarea lor la nivelul echipamentului de stocare. Aceasta functionalitate trebuie sa permita accelerarea mutarii unei masini virtuale intre doua volume de date ale hipervizorului si accelerarea efectuarii unei copii identice a unei masini virtuale; ▪ Pentru asigurarea unui nivel optim de disponibilitate operationala, solutia oferita va permite update si upgrade software si hardware al platformei fara intreruperea serviciilor; ▪ In scopul alocarii eficiente si dinamice a spatiului de stocare in functie de cerintele previzionate sau de moment, echipamentul trebuie sa includa prin licentiere ulterioara, un mecanism de integrare directa la nivelul sistemului de operare ce acceseaza platforma 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 trebuie sa fie disponibil cel putin pentru sistemele de operare de tip server pentru care platforma de stocare trebuie sa ofere suport de conectivitate directa: Windows, Linux, UNIX, Sun Solaris, AIX, HP-UX, MacOS, Vmware ESX; ▪ Ca parte a functiilor de administrare si diagnosticare echipamentul trebuie 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. Deasemenea trebuie sa permita 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 sa se faca in mod facil in uneltele de management ce nu au implicit profile definite pentru sistemul specific ofertat.;
Optimizarea capacitatii de stocare	▪ Platforma de stocare trebuie să asigure rebalansarea datelor pe matricile de discuri în cazul în care sunt adăugate discuri suplimentare; • Platforma de stocare trebuie sa permita definirea de volume de date pe matrici ce suporta discuri in tehnologii diferite, organizate in matrici cu nivele de protectie RAID diferite; • Sistemul de stocare trebuie sa ofere, fara licentiere ulterioara optiunea de prioritizare si accelerare a accesului la date in mod automat si transparent pentru aplicatiile si utilizatorii ce folosesc aceste seturi de date.

Caracteristica	Cerinta tehnica minimala
	Mecanismele de accelerare si prioritizare trebuie sa beneficieze de suportul hardware al unui set dedicat de discuri de mare viteza. Pentru economisirea spatiului si a costurilor asociate, sistemul trebuie sa permita instalarea lor in acelasi sertar cu un tip mai lent de discuri de la acelasi producator (SAS, spre exemplu).
Protectia si replicarea datelor	▪ Echipamentul trebuie sa aiba incoporate baterii ce asigura protectia controller-elor si a memoriei cache la cadererile de curent prin salvarea automata a datelor din cache pe discuri dedicate flash/SSD, inainte de oprirea echipamentului; ▪ Platforma de stocare trebuie sa includa mecanisme de realizare a copiilor complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp. Spatiul rezervat copiilor de date trebuie sa poata fi configurat pe discuri separate fata de cele unde stau datele de productie. Sistemul trebuie sa permita si realizarea de copii ale oricarei copii de date. Copiile de date complete, sau bazate pe imagini, trebuie sa poata fi accesate atat in mod „citire”, cat si in mod „scriere”; ▪ Suport software si hardware inclus pentru realizarea de copii de siguranță a datelor, local și la distanță, folosind o tehnologie de jurnalizare a tuturor operațiunilor de scriere, care să permită restaurarea datelor la orice moment de timp. Copiile de siguranță trebuie să poată fi grupate pe aplicație, pentru a asigura consistența recuperării aplicațiilor interdependente; ▪ Suport software si hardware inclus pentru replicarea sincrona/asincrona a datelor la distanta, intre mai multe echipamente similare, respectiv intre echipamente diferite de la producatori diferiti. Pentru utilizarea eficientă a canalelor de comunicatie dintre centrele de date, soluția de replicare trebuie să ofere suport pentru replicare doar a datelor modificate, precum și transmiterea numai a blocurilor de date unice (deduplicare) si comprimate (compresie); ▪ 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;
Licentiere	▪ Conectarea prin protocol NFS (v2/v3/v4) sa fie disponibila in configuratia initiala; ▪ Conectarea prin protocol CIFS (SMB2/SMB3) sa fie disponibila in configuratia initiala; ▪ Conectarea prin protocol FC sa fie disponibila in configuratia initiala;
Sisteme de operare suportate	Platforma de stocare trebuie să suporte minim următoarele sisteme de operare: ▪ Microsoft Windows Server; ▪ Microsoft Hyper-V; ▪ VMware vSphere; ▪ Red Hat Enterprise Linux; ▪ Suse Enterprise Linux; ▪ Oracle Solaris 10/11; ▪ IBM AIX; ▪ HP-UX;

Caracteristica	Cerinta tehnica minimala
	Platforma de stocare trebuie sa includa licentele necesare pentru sistemele de operare ofertate;
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 (suporţi, şuruburi/captive);

3.7.8. Platforma unificata de backup

In stransa legatura si prin integrarea cu celelalte elementele de infrastructura descrise, platforma unificata de backup 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;
- 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 ce include mecanisme integrate de optimizare a capacitatii de stocare, prevenind astfel upgrade-urile de capacitate pentru un timp mai indelungat si asigurand in acelasi timp 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,

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;

Solutia va include o platforma de backup dedicata, bazata pe echipamente hardware si componente software integrate cu platforma de stocare, respectiv cu platforma de virtualizare ofertate.
Platforma unificata de backup trebuie sa indeplineasca urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Platforma unificata de backup;
Arhitectura	▪ Soluţia de backup trebuie sa ofere cel putin un echipament hardware dedicat operatiunilor de salvare si restaurare a datelor, respectiv componentele software pentru asigurarea functionalitatii solicitate. Acest echipament va asigura protectia datelor prin mecanisme de backup pe suport de tip disc; ▪ Solutia de backup trebuie sa ofere cel putin echipament hardware dedicat operatiunilor de deduplicare si compresie a datelor salvate, indiferent de platformele, aplicatiile si serviciile ce beneficiaza de mecanismele de backup implementate si sa ofere integrare cu echipamentul de backup pe disc propus. Solutia propusa trebuie sa asigure accelerarea operatiunilor de backup prin utilizarea simultana a mai multor fluxuri de backup, prin interfete separate de retea si/sau prin agregarea conexiunilor de retea disponibile, indiferent de protocolul de comunicatie folosit si de tipul de date salvate; ▪ Solutia trebuie sa poata scala la o arhitectura de tip multi-nod (multiple noduri independente ce sunt agregate intr-un model de redundanta activ-activ/activ-pasiv);
Protocol de acces la date	▪ Soluţia de backup trebuie să ofere acces la datele stocate, respectiv catre platformele si aplicatiile ce beneficiaza de procesele de backup, prin protocol de tip file (NAS), prin NFS (v2/v3/v4) si CIFS (SMB2/SMB3); ▪ Deasemenea trebuie sa permita conectivitate prin protocol de tip FTP, NDMP si VTL; ▪ Platforma unificata de backup trebuie sa permita utilizarea simultana a tututror protocoalelor si interfetelor de retea, respectiv sa permita rularea simultana a proceselor de backup si restore utilizand protocoale diferite si/sau interfete diferite de retea;
Porturi instalate	▪ Platforma dedicata de backup pe disc trebuie să dispuna de minim 4 porturi 1 Gbps Ethernet, cu posibilitatea de agregare a tuturor conexiunilor Ethernet, respectiv minim 2 porturi 10 Gbps Ethernet, echipate efectiv cu conectori SFP+; ▪ Platforma dedicata de deduplicare trebuie să dispuna de minim 4 porturi 10 Gbps Ethernet, echipate efectiv cu conectori SFP+ si posibilitatea scalarii numarului de porturi;
Nivele RAID	Trebuie sa permita configurarea si optimizarea matricilor RAID in configuratii cu unul si doua discuri de paritate asociate fiecarui set de discuri componente al unei matrici RAID si/sau posibilitatea de a folosi aceste matrici RAID in mod de replicare integrala de tip mirror;

Caracteristica	Cerinta tehnica minimala
Capacitate instalata	Solutia unificata de backup trebuie sa ofere o capacitate minima rezultata in urma operatiunilor de deduplicare cel putin egala cu intreaga capacitatea a platformei de stocare ofertate plus o rezerva de 100%, dar nu mai putin de 20 TB capacitate efectiv instalata, in vederea extinderii ulterioare fara a implica costuri aditionale cu extinderea capacitatii de stocare a datelor salvate;
Extensia capacitatii de stocare	Pentru intreaga solutie unificata de backup trebuie sa se asigure scalabilitate la minim 5 PB de date salvate (capacitate calculata inainte de aplicarea procesului de deduplicare);
Managementul platformei	▪ Platforma unificata de backup trebuie să asigure un sistem de management şi monitorizare integrat; ▪ Platforma unificata de backup trebuie să aibă capabilitatea de monitorizare şi management a mai multor echipamente din aceeaşi gamă într-o singură instanţă a interfeţei; ▪ Platforma unificata de backup trebuie sa asigure monitorizarea performantei si capacitatii.Solutia trebuie sa asigure functionalitatile respective atat pentru platforma propusa cat si pentru alte platforme de la acelasi producator; ▪ Platforma unificata de backup trebuie 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/Telnet.Toate functiile ale platformei unificate de backup, precum si functionalitatea licentiata separat trebuie sa fie accesibile in mod integrat prin intermediul acestor unelte de administrare, astfel incat operatiunile de configurare si administrare sa poata fi efectuate indiferent de locatie si de modalitatea de acces; ▪ Atat in scop administrativ cat si in vederea accesului la seturile de date, echipamentul trebuie sa permita definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date.Deasemenea trebuie sa permita 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 trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp; ▪ Tot ca parte a uneltelor standard de administrare, platforma unificata de backup trebuie sa includa posibilitatea de integrare cu platforma de virtualizare aleasa astfel incat sa permita aplicarea politicilor si mecanismelor integrate de optimizare, backup si recuperare, efectuarea operatiunilor de instantiere rapida a seturilor de date ce apartin de masinile virtuale, direct din uneltele de management puse la dispozitie de platforma de virtualizare, fara a folosi un alt set de unelte terte ce nu apartin nici de platforma unificata de backup, nici de cea de virtualizare.Astfel se obtine o platforma unitara de management, ce reduce efortul si costul administrativ, indiferent de natura operatiunilor efectuate; ▪ Platforma unificata de backup trebuie sa asigure o interfata grafica la nivel de client. Utilizatorii trebuie sa-si poata restaura datele fara a implica administratorul sistemului;

Caracteristica	Cerinta tehnica minimala
	▪ Deasemenea trebuie sa ofere un API pentru integrarea cu alte aplicatii de administrare, raportare sau control din cadrul infrastructurii clientului; ▪ Pentru asigurarea unui nivel optim de disponibilitate operationala, solutia oferita va permite update si upgrade software si hardware al platformei fara intreruperea serviciilor; ▪ Ca parte a functiilor de administrare si diagnosticare echipamentul trebuie 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.Deasemenea trebuie sa permita 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 sa se faca in mod facil in uneltele de management ce nu au implicit profile definite pentru sistemul specific ofertat.Tot in scopul operatiunilor de management si diagnosticare sistemul trebuie sa integreze un set de led-uri ce afiseaza cel putin starea curenta a echipamentului; ▪ Platforma trebuie sa permita raportarea in timp real a indicilor de performanta si capacitate, respectiv raportarea avansata asupra tuturor configuratiilor specifice si a parametrilor de functionare, prin intermediul interfetei grafice de tip web sau prin aplicatie dedicata de raportare;
Optimizarea capacitatii de stocare	Platforma unificata de stocare trebuie sa ofere optimizarea capacitatii de stocare prin mecanisme transparente de deduplicare a datelor salvate, mecanisme ce vor indeplini urmatoarele cerinte tehnice specifice: ▪ Procesul de deduplicare a datelor sa poata fi distribuit la sursa sau la destinatie in functie de aplicatia de salvare si restaurare utilizata; ▪ La nivelul sursei de deduplicare (prin intermediul unui agent de backup sau prin integrare cu sistemul de operare, aplicatiile si serviciile sursa), solutia trebuie sa foloseasca un mecanism de deduplicare pe baza unor dimensiuni variabile ale blocurilor de date; ▪ Procesul de deduplicare a datelor sa poata fi oferit pentru orice tip de fisier si orice dimensiune de fisier, folosind o singura tabela de deduplicare pentru toate datele stocate, independent de tipul de date (Exchange, Oracle, fisiere, etc.), de protocolul utilizat sau de numarul de sesiuni; ▪ Procesul de deduplicare a datelor sa se faca utilizand segmente de dimensiuni variabile, in scopul eficientizarii factorului de deduplicare; ▪ Platforma unificata de backup trebuie sa utilizeze exclusiv procesorul si memoria din echipamentul/echipamentele dedicate procesului de deduplicare, compresie si scriere a fluxurilor de backup, independent de activitatea discurilor interne; ▪ Sistemul trebuie sa sustina protectia datelor salvate in urma unui process de backup sau a unor procese de arhivare in mod independent de aplicatia sursa sau a protocolului utilizat; ▪ Sistemul trebuie ofere o tabela unica de deduplicare indiferent de tipul sau dimensiunea datelor și independent de protocolul de scriere a acestora sau a interfetei de retea utilizata; ▪ Solutia trebuie sa fie bazata pe un backup full initial, urmand ca backup-urile succesive sa transmita prin retea doar blocurile unice de date modificate;

Caracteristica	Cerinta tehnica minimala
	▪ Pentru optimizarea traficului prin retea, platforma unificata de backup trebuie sa identifice blocurile de date unice la nivelul echipamentelor, sistemelor de operare, aplicatiilor si serviciilor ce beneficiaza de mecanismele de backup implementate; ▪ Pentru evitarea congestionarii traficului prin retea in timpul operatiunilor de backup, platforma unificata de backup trebuie sa permita restrictionarea cantitatii de date transmise prin mediul de comunicatie; ▪ Platforma unificata de backup trebuie sa asigure backup-ul rapid si eficient al datelor unice (nemodificate) cum sunt datele sistemului de operare, documentele si alte date existente in sistemele de fisiere, precum si in platforma de virtualizare ofertata; ▪ Platforma unificata de backup trebuie sa suporte salvarea datelor pentru utilizatori si sisteme aflate la distanta si sa asigure functii de salvare si recuperare indiferent de conectivitatea existenta: LAN, WAN, WLAN sau VPN;
Protectia si replicarea datelor	▪ Platforma unificata de backup trebuie sa aiba incoporate baterii ce asigura protectia controller-elor si a memoriei cache la cadererile de curent prin salvarea automata a datelor din cache pe discuri, inainte de oprirea echipamentului/echipamentelor; ▪ Platforma unificata de backup trebuie sa dispuna de sistem de operare cu auto- regenerare si verificare activa, continua, a datelor stocate; ▪ Platforma unificata de backup trebuie sa dispuna de capacitate de protectie prin snapshot la nivelul intregii platforme, respectiv pentru totalitatea datelor de backup stocate; ▪ Trebuie sa ofere suport pentru operatiuni de curatarea a sistemului de fisiere fara a afecta operatiunile de salvare sau restaurare a datelor; ▪ Trebuie sa permita limitarea utilizarii resurselor interne in procesul de curatare a sistemului de fisiere; ▪ Trebuie sa ofere mecanism de comunicatie direct catre producator in scopul operatiunilor de suport proactiv; ▪ Suport software si hardware inclus pentru replicarea sincrona/asincrona a datelor la distanta in mod bi-directional. Pentru utilizarea eficientă a canalelor de comunicatie dintre centrele de date, soluția de replicare trebuie să ofere suport pentru replicare doar a datelor modificate, precum și transmiterea numai a blocurilor de date unice deduplicate și comprimate; ▪ Mecanismul de replicare va permite monitorizarea si optimizarea latimii de banda, intre sistemele ce participa in procesul de replicare, respectiv va permite efectuarea operariunilor administrative dintr-o singura consola de management atat pentru echipamentele locale cate si pentru cele aflate la distanta; ▪ Mecanismul de replicare trebuie sa asigure integritatea datelor protejate prin verificarea zilnica a acestora; ▪ Platforma unificata de backup trebuie sa ofere posibilitatea criptarii datelor stocate, respectiv criptarea fluxului de date in procesul de replicare; ▪ Platforma unificata de backup trebuie sa ofere suport pentru protectie de tip WORM (Write-Once-Read-Many);

Caracteristica	Cerinta tehnica minimala
	▪ Toate functionalitatile software solicitate mai sus vor fi incluse in configuratia ofertata a platformei unificate de backup, respectiv pentru intreaga capacitate de stocare integrata;
Functii suplimentare	▪ Platforma unificata de backup trebuie sa permita instalarea unui numar nelimitat de clienti de backup, indiferent de tipul acestora sau de nivelul logic la care sunt instalati (sistem de operare, aplicatii, servicii); ▪ Platforma unificata de backup trebuie sa ofere integrare prin interfete de tip API cu platforma de virtualizare ofertata, pentru managementul operatiunilor de backup si definirea de politici dinamice de protectie a sistemelor virtuale; ▪ Platforma unificata de backup trebuie sa permita instalarea unor masini virtuale de tip proxy pentru a reduce incarcarea pe masinile virtuale asupra carora este aplicat mecanismul de backup; ▪ Platforma unificata de backup trebuie sa permita utilizarea mecanismelor de analiza a schimbarii blocurilor de date, mecanisme ce sunt integrate in platforma de virtualizare ofertata, astfel incat sa optimizeze procesul de salvare si restaurare doar a datelor modificate in discurile virtuale; ▪ Platforma unificata de backup trebuie sa ofere posibilitatea ca utilizatorii sa-si poata vizualiza fisierele salvate;
Sisteme de operare suportate	Platforma unificata de backup trebuie să suporte backup-ul online prin integrare cu minim următoarele sisteme de operare si aplicatii: ▪ Microsoft Windows Server; ▪ Debian Linux; ▪ CentOS 6/7; ▪ Ubuntu 11/12/14; ▪ Apple MacOS X; ▪ Microsoft Hyper-V; ▪ VMware vSphere; ▪ Red Hat Enterprise Linux; ▪ Suse Enterprise Linux; ▪ Oracle Solaris 10/11; ▪ IBM AIX; ▪ HP-UX; ▪ Oracle Database 11/12; ▪ Microsoft SQL Server 2012/2014; ▪ IBM DB2;
Alimentare	Pentru asigurarea redundantei complete a platformei unificate de backup propuse fiecare element major component al platformei 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	▪ Componentele platformei unificate de backup trebuie să fie montabile în rack-uri standard de 19”; ▪ Ofertantul trebuie să livreze toate kit-urile cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive);

Platforma de backup va dispune si de o unitate de tip librarie de benzi, pentru transportarea si stocarea datelor salvate in alta locatie decat cea in care se va implementa prezentul proiect (stocare off-site). Unitatea de banda trebuie sa respecte urmatoarele cerinte functionale specifice:

Caracteristica	Cerinta tehnica minimala
Descriere	Unitate de tip librarie de benzi;
Unitate citire/scriere	Minim 2 unitati de citire/scriere de tip LTO-8 instalate la nivelul librariei de benzi, cu posibilitatea de a scala la minim 4 unitati de citire/scriere;
Capacitate benzi	Minim 48 de benzi, cu minim 3 sloturi de inserare benzi fara a afecta operatiunile de citire/scriere curente;
Capacitate livrata	Minim 300 TB comprimat, disponibil in maxim 48 de benzi;
Interfata de conectare	Minim 2 porturi 8 Gbps FC;
Viteza de transfer	Minim 160 Mbps;
Alimentare	Pentru asigurarea redundantei complete unitatea de tip librarie de benzi 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;
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);

3.7.9. Platforma de securizare a masinilor virtuale

Solutia ofertata trebuie sa includa o platforma de securizare a masinilor virtuale, platforma ce se va integra in infrastructura de virtualizare si va oferi servicii transparente de criptare/decriptare, respectiv managementul ciclului de viata al materialului criptografic.
In stransa legatura si prin integrarea cu celelalte elemente de infrastructura 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 de virtualizare, pentru protectia continua si completa a masinilor virtuale deservite si a datelor stocate in masini virtuale si platforme, in eventualitatea unor defectiuni majore;
- Platforma scalabila in mod transparent pentru masinile virtuale deservite si datele stocate in masini virtuale, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate 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, platforma de virtualizare, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;
- Functionalitati integrate de securitate si protectie criptografica a datelor din platforma de virtualizare, integrate cu restul elementelor de infrastructura de virtualizare, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;

- Functionalitati integrate de administrare a ciclului de viata al materialului ciptografic, integrate cu restul elementelor de infrastructura de virtualizare, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
- 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;
- Mecanisme integrate de recuperare in caz de dezastru si continuitate operationala, in scopul reducerii complexitatii asociate scenariilor de protectie si redundanta.

Solutia va include o platforma de securizare a masinilor virtuale, platforma ce se va integra in infrastructura de virtualizare si va oferi servicii transparente de criptare/decriptare, respectiv managementul ciclului de viata al materialului criptografic pentru totalitatea masinilor virtuale ce rezida in platforma de virtualizare.
Platforma de securitate trebuie sa indeplineasca urmatoarele cerinte functionale specifice:

Caracteristica	**Cerinta tehnica minimala**
Descriere	Platforma de securizare a masinilor virtuale si management al intregului ciclu de viata al materialului criptografic;
Functionalitati	▪ Platforma de securitate trebuie sa asigura criptarea integrala a discurilor masinilor virtuale din platforma de virtualizare ofertata (incluzand volumele de stocare atasate din platforma de stocare unificata ofertata), astfel incat accesul si manipularea respectivelor masini virtuale sa se faca intr-un mediu complet securizat; ▪ Procesul de control al accesului la masinile virtuale, respectiv de criptare a discurilor virtuale trebuie sa fie disponibil atat pentru platforme de virtualizare implementate local (on-premise) cat si pentru platforme de virtualizare implementate exclusiv la un provider de infrastructura virtuala in cloud; ▪ Platforma de securitate trebuie sa integreze in platforma de virtualizare mecanismele proprii de autorizare si control al accesului administrativ la masinile virtuale rezidente, astfel incat masinile virtuale sa nu poata fi pornite sau mutate in platforma de procesare fara autentificarea securizata a administratorilor desemnati; ▪ Solutia trebuie sa ofere un mediu administrativ centralizat ce va permite criptarea/decriptarea masinilor virtuale si a volumelor de stocare asociate, crearea si modificarea profilelor/grupurilor administrative de securitate, respectiv a politicilor granulare de securitate asociate respectivelor identitati si masini virtuale; ▪ Procesul de autentificare in platforma de securizare a masinilor virtuale trebuie sa fie disponibil in mediul de boot al fiecarei masini virtuale, astfel incat mecanismul in sine sa nu poata fi anulat de procese terte active in sistemul de operare rezident in masinile virtuale; ▪ Solutia trebuie sa ofere mecanisme integrate de separare a rolurilor administrative, respectiv de alcatuire granulara a politicilor de securitate aplicabile respectivelor roluri; ▪ Solutia trebuie sa ofere mecanisme proprii de audit si raportare asupra politicilor de securitate aplicate, respectiv asupra incalcarilor acestor politici (Ex.: incercari de acces neautorizat la masinile virtuale, operatiuni nepermise asupra masinilor virtuale, etc);

Caracteristica	Cerinta tehnica minimala
	▪ Solutia trebuie sa ofere mecanisme integrate de revocare a accesului in cazul constatarii incalcarii unei anumite politici de securitate; ▪ In vederea integrarii cu platformele de virtualizare majore solutia ofertata trebuie sa ofere suport pentru cel putin: VMware vSphere/vCloud, Microsoft Azure, Amazon EC2/VCP, IBM SoftLayer Cloud; ▪ Platforma de securitate trebuie sa ofere suport cel putin pentru urmatoarele sisteme de operare rezidente in masinile virtuale protejate: Microsoft Windows Server, Red Hat Enterprise Server, Suse Linux Enterprise Server, CentOS, Ubuntu; ▪ Echipamentul dedicat trebuie sa ofere serviciile de management al cheilor criptografice atat pentru platforma de securizare propusa cat si pentru un numar cat mai mare de aplicatii, sisteme si servicii terte ce utilizeaza material criptografic (sisteme de stocare ce cripteaza volumele de date, discuri cu criptare, benzi cu criptare, sisteme proprietare de criptare in baze de date si servere de aplicatie, sisteme de criptare a canalelor de comunicatie, orice alt sistem conform cu standardul de interoperabilitate a materialului criptografic KMIP); ▪ Echipamentul trebuie sa permita administrarea centralizata a cheilor criptografice simetrice/asimetrice, respectiv a certificatelor conforme cu standardul X.509 impreuna cu politicile de securitate asociate; ▪ Trebuie sa ofere o interfata centralizata de management, cu acces departajat pe roluri de utilizare, respectiv prin integrare cu sisteme de tip directory; ▪ Trebuie sa ofere mecanisme integrate de audit si raportare asupra tuturor operatiunilor ce implica un risc de securitate (schimbarile de stare ale cheilor criptografice, accesul administrativ, schimbarile de politici de securitate, etc). Jurnalele de audit trebuiesc stocate securizat si semnate criptografic pentru a asigura validitatea lor, respectiv vor putea fi exportate catre solutii terte de analiza (sisteme de tip SIEM); ▪ Echipamentul dedicat managementului ciclului de viata al materialului criptografic trebuie sa accelereze operatiunile de criptare/decriptare aplicate asupra masinilor virtuale din platforma de virtualizare ofertata si trebuie sa fie conform cu standardul FIPS 140-2 Level 1; ▪ Trebuie sa ofere suport pentru urmatoarele API-uri: Java, C/C++, .Net XML, KMIP; ▪ Trebuie sa permita managementul prin retea folosind protocolul SNMP; ▪ Echipamentul trebuie sa permita administrarea ciclui de viata a minim 20000 de chei criptografice, respectiv sa permita accesul simultan a minim 100 de utlizatori;

3.7.10. Platforma de balansare a traficului de aplicatie

Solutia va include o platforma de balansare a traficului de aplicatie, platforma ce se va integra in infrastructura de hardware, software si de virtualizare si va oferi servicii transparente de balansare, accelerare si protejare a aplicatiilor deservite.

In stransa legatura si prin integrarea cu celelalte elemente de infrastructura si de aplicatie, 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 si de aplicatie, pentru protectia continua si completa a alicatiilor deservite in eventualitatea unor defectiuni majore;
- Platforma scalabila in mod transparent pentru aplicatiile deservite, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate 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, platforma de aplicatie, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;
- Functionalitati integrate de securitate si protectie a aplicatiilor deservite, integrate cu restul elementelor de infrastructura, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
- Functionalitati integrate de accelerare a performantei, respectiv de distribuire a incarcarii si disponibilitatii pentru aplicatiile deservite;
- 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;
- Mecanisme integrate de recuperare in caz de dezastru si continuitate operationala, in scopul reducerii complexitatii asociate scenariilor de protectie si redundanta.

Platforma de balansare a traficului de aplicatie trebuie sa indeplineasca urmatoarele cerinte functionale specifice:

Caracteristica	**Cerinta tehnica minimala**
Descriere	Platforma de de balansare, accelerare si protejare a aplicatiilor din infrastructura;
Specificatii hardware	▪ Sloturi Gigabit Ethernet SFP: 8; ▪ Sloturi 10 Gigabit Ethernet SFP+: 4 populate cu transceiver-e 10 Gbps MMF Short-range conector LC; ▪ Capacitate de stocare interna: 500 GB HDD; ▪ Memorie RAM: 32 GB; ▪ Posibilitate de instalare in rack: 1U; ▪ Surse redundante de alimentare;
Caracteristici de performanta	▪ Trafic procesat la Layer 4/7: 20 Gbps; ▪ Trafic compresat hardware: 10 Gbps; ▪ Trafic criptat hardware: 12 Gbps; ▪ Numar de cereri pe secunda la Layer 7: 1.100.000; ▪ Numar de tranzactii SSL pe secunda: 10.000 ECC/20.000 RSA;
Functionalitati disponibilitate aplicatii	▪ Distributia incarcarii de procesare pentru 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 a aplicatiei;

Caracteristica	Cerinta tehnica minimala
	▪ 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 redirectare a traficului pentru diferite tipuri,HTTP to HTTPS; ▪ Capacitatea de a folosi o combinatie mixta de adrese virtuale si noduri IPv4 si IPv6; ▪ Capacitatea de insertie XFF in header-e 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 built-in de compresie HTTP pentru reducerea traficului; ▪ Capabilitate built-in pentru accelerare si caching HTTP; ▪ Capabilitate built-in pentru optimizare simetrica de date, compresie, criptare si tunneling; ▪ 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;

Functionalitati Global Server Load Balancing	▪ Posibilitatea de a furniza raspunsuri de autoritate DNS;
	▪ Posibilitatea de a obtine informatii despre starea obiectelor definite si de a interactiona cu platformele ADC ce deservesc fiecare obiect;
	▪ Posibilitatea de a functiona in modul authoritive slave DNS server;
	▪ Suport pentru DNSSEC;
	▪ Functie de GeoIP pentru determinarea obiectului cel mai apropiat de catre client;
	▪ Functia de balansare a cererilor pe baza urmatoarelor metrici:
	  ▪ Round trip time;
	  ▪ Hops;
	  ▪ Completion rate;
	  ▪ Packet rate;
	  ▪ Virtual server capacity;
	  ▪ Link capacity;
	▪ Posibilitatea de raportare detaliata a statisticilor pentru cereri de tipul A, CNAME, NS, RRSIG, AAAA, SRV;
	▪ Suport IPv6 si topologii de NAT64;
	▪ Suport pentru IP Anycast;

Functionalitati de securitate	▪ Protectie impotriva atacurilor DoS si DDoS; ▪ Protectie impotriva atacurilor de tip SQL injection; ▪ Protectie impotriva atacurilor de tip Web Scraping; ▪ Protectie impotriva atacurilor de tip Cross Site Scripting;

Caracteristica	Cerinta tehnica minimala
	▪ 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 politicii 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;
Controlul accesului	▪ 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 utilizarorii platformelor Microsoft Windows; ▪ Posibilitatea de a exporta si importa politicile de acces; ▪ Licenta pentru minim 500 de utilizatori concurenti autentificati;
Administrare si Monitorizare	▪ Functionare in cluster de tip activ/activ; ▪ Functionare in cluster de tip activ/pasiv; ▪ Posibilitatea sincronizarii configuratiilor; ▪ Posibilitatea de rulare a unor versiune de software diferite pe fiecare nod;

Caracteristica	Cerinta tehnica minimala
	▪ Sistem de operare pentru management independent de sistemul folosit pentru procesarea traficului; ▪ Sistem de operare pentru procesarea traficului modular; ▪ Interfata web; ▪ Interfata cli; ▪ Acces securizat HTTPS sau SSH; ▪ SNMP v2/3; ▪ Extinderea functionalitatilor ADC prin limbaj de scripting , cu urmatoarele caracteristici: ▪ Capabil sa foloseasca declaratii conditionale (if/then) si bucle (for, while); ▪ Capabil sa genereze alerte SNMP in functie la aparitia diferitelor tipuri de evenimente; ▪ Capabil sa permita modificarea/alterarea cerere/raspuns in functie de: parametri standard HTTP (header, cookie, hostname, URN, etc), username, parametri ai certificatelor X.509

3.7.11. Platforma unificată de securitate

Solutia ofertata trebuie sa includa o platforma unificată de securitate care să îndeplinească următoarele cerințe:

Arhitectura	Arhitectura de tip Next Generation Firewall, cu separare la nivel hardware al nivelului de comunicatii (data plane) de nivelul de control (management plane); implementeaza simultan printr-un singur proces de inspectie a traficului mecanisme de protectie la nivel de retea (filtru de pachete), firewall de aplicatie, mecanisme anti-intruziune (IPS), filtrare anti malware, filtrare de adrese URL, mecanisme de protectie impotriva exfiltrarii datelor (anti spyware), identificare de utilizator si de terminal, servicii de concentare VPN IPSec si SSL, decriptare SSL de tip inbound si outbound (forward proxy), decriptare SSH, inspectie tunele GRE, IPsec non-criptate. Densitate de porturi de minim 16 porturi de 10Gbps si capabilitate de conectare la 40Gbps.
Echipare minima	4 porturi Ethernet 1Gb/10Gb RJ45 12 porturi SFP/SFP+ ce pot fi configurate cu module transceiver de 1Gbps sau 10Gbps, din care 8 porturi echipate cu transceiver SFP+ 10G 2 porturi 40Gb
Capabilitati minimale de retea	Suport IPv4 si IPv6 120000 adrese MAC 100000 rute IPv4 100000 rute IPv6 4000 tag-uri VLAN 5000 interfete fizice si logice (subinterfete, intefete VLAN, loopback) 200 routere virtuale cu tabela de rutare proprie 10000 reguli NAT

	Permite integrarea in retele existente in mod Layer 2 (cu integrare de VLAN-uri), Layer 3 (in mod routing), transparent (fara a fi vizibil din punct de vedere ARP pentru restul echipamentelor). Echipamentul permite ca seturi de interfete sa fie integrate in mod diferit in retea dpdv topologie. Serviciile de securitate, inclusiv decriptare SSL/SSH sa fie disponibile indiferent de topologia de retea implementata. Sa permita configurarea de interfete de monitorizare read-only, in mod TAP, pentru identificarea atacurilor fara a influenta traficul monitorizat
Capabilitati minime firewall, IPS, ADS, anti-malware	Throughput de baza sustinut de 50Gbps cu identificare si filtrare de aplicatii, pentru tranzactii HTTP de 64k Throughput sustinut de 25Gbps in conditii de activare concurenta a filtrelor anti intruziune, anti malware, anti spyware, pentru tranzactii HTTP de 64k 15Gbps trafic sustinut IPSec VPN 35000 utilizatori simultani VPN Ipsec sau SSL 10000 utilizatori simultani SSL fara client (peste interfata web HTTPS) 300000 mapari de utilizator cu adresa IP mentinute in nivelul de control (management plane) 300000 mapari de utilizator cu adresa IP mentinute in nivelul de retea (data plane) Functionalitate inclusa pentru posibilitatea de creare și de utilizare a 25 partiții interne administrativ independente. Integrare directa cu servere multiple de LDAP pentru identificarea utilizatorilor. Politica de control al accesului trebuie să defineasca in mod precis drepturile de acces ale utilizatorilor la serviciile și rețelele specifice iar aceste drepturi trebuie sa fie mentinute chiar si atunci cand utilizatorul schimbă locatia si adresa IP. Pentru utilizatorii care lucreaza pe statii virtualizate sau terminal server, avand astfel o adresă IP comună, stabilirea identitătii trebuie sa fie , de asemenea , asigurata in mod transparent. Functionalitate inclusa de firewall de aplicatie pentru aplicatii web based si non-web, minim 2000 semnaturi de aplicatii definite de producator Posibilitate de definire semnaturi de aplicatii custom, minimum 5000 aplicatii Suport pentru identificarea aplicatiilor indiferent de portul TCP/UDP utilizat Identificarea traficului de fisiere in cadrul aplicatiilor si capabilitate de control inclusiv pe baza de filtre de continut al fisierelor. Permite blocarea transferului de fișiere, nu mai puțin de : BAT, CAB, DLL, doc, doc criptat, docx, ppt, PPT criptat, PPTX, XLS, .xls criptat, .xlsx, RAR, RAR criptat, zip, zip criptat, exe, gzip, hta, mDB, mdi, OCX, PDF, PGP, .pif, reg, sh, tar, text / html, TIF. Recunoașterea fișierului trebuie să se bazeze pe antet și tip MIME, nu pe extensia numelui. Trebuie sa permita analiza si blocarea fișierele trimise în aplicațiile identificate. In cazul in care mai multe aplicații functioneaza pe același port UDP / TCP (de ex. TCP / 80) trebuie sa fie in masura sa utilizeze profiluri separate de analiză si de blocare a fisierelor pentru fiecare aplicatie in parte.

	Sa permita definirea unui set separat de politici de tratare a traficului SSL care sa fie excluse la decriptare și inspectia profunda, separat de politicile de securitate. Implementeaza actualizarea automata de catre producător a listelor de servere pentru care este imposibila decriptarea traficului SSL (de ex. utilizatorul se autentifica utilizând un certificat sau aplicatia implementeaza mecanism de tip „certificat pinning“). Aceasta lista este exceptata în mod automat de la regulile generale de decriptare. Orice intrare din lista poate fi activata sau dezactivata administrativ. Permite inspectarea traficului SSH, inlusiv identificarea si (conform politicilor definite) blocarea tunelarii altor protocoale in traficul SSH Urmarirea starii protocoalelor si verificarea conformitatii acestuia cu standardul Capabilitati de limitare a latimii de banda pentru aplicatii, utilizatori, zone de securitate, interfete Filtrare web URL pe baza de reputatie si clasificare continut, cu subscriptie la serviciul de actualizare regulata a bazei de date reputationale si de clasificare Detectare a atacurilor bazata pe semnaturi de tip IPS Detectie a continutului malware pe baza de semnaturi de continut Detectie si blocare a traficului catre retele de bot-net si servere de comand and control pentru distributie malware Facilitati de management trafic cu reguli de permitere, blocare, limitare a ratei traficului (rate limit), reset de conexiune Captura selectiva de trafic ce traverseaza echipamentul Protectie la nivel de vulnerabilitate (nu doar exploit) Posibilitatea inspectarii protocoalelor de comunicatie conform RFC Posibilitatea instalarii de noi filtre in mod automat, fara interventia utilizatorului de sistem Posibilitatea instalarii de filtre si baze de date de semnaturi in mod offline, prin interfata de management Facilitati de raportare pentru traficul care face match pe filtru de protectie, pentru fluxuri de date categorisite pe protocol, dimensiune frame, port, atacuri DDOS, aplicatii, utilizatori, zona de securitate Facilitati de export automat al rapoartelor (log-urilor) de trafic Facilitati de filtrare a rapoartelor (log-urilor) de trafic dupa criteriiȘ utilizator, adrese IP, aplicatie, regula de securitate corespondenta, actiune asupra fluxului de date, si de export programat al rapoartelor filtrate. Disponibilitate: Activ/Activ si Activ/Pasiv cu prezervare a sesiunilor si starii acestora (full state failover) Include suport hw si sw precum si update-uri la semnaturi pe o perioada de 3 ani
Management	CLI WEB (HTTPS) SSH SCP pentru export de rapoarte de trafic (log-uri)

	API deschis de control si configurare bazat pe servicii WEB si XML Creearea utilizatorilor de sistem de tip ierarhic pentru access la comenzile sistemului SNMP v2c, v3 NTP LLDP Ofera versionarea fisierelor de firmware si capabilitati de restore la versiuni anterioare Syslog Capabilitate de rutare diferentiata pentru serviciile de management si control prin interfete fizice sau logice diferite
Layer 3	Stiva duala IPv4 si IPv6 Servere multiple DHCP, minim 150 RIP v1/v2 OSPFv2/OSPFv3 cu graceful restart BGP cu graceful restart Policy Routing ICMP
QoS	Clase de trafic bazate pe profile definite in functie de adrese IP sursa si destinatie (IPv4 si IPv6), aplicatie, liste sau grupuri de utilizatori, interfete, zone de securitate Remarcarea pachetelor cu 802.1p, Precedenta IP, si DSCP
Disponibilitate si fiabilitate	Sa suporte clustering pentru High Availability de tip active-activ cu suport pentru rutare asimetrica Sa suporte clustering pentru High Availability in mod active-passive cu prezervare a sesiunilor si starii acestora (full state failover) Redundanta 1+1 la nivel de sursa de alimentare Cai diferite pentru Control si Servicii a.i. orice serviciu configurat pentru traficul de date sa nu influenteze controlul asupra echipamentului LACP: pana la 8 porturi per grup de trunk
Surse de alimentare Ventilatoare Racire	2 surse de alimentare AC incluse, 220V, maxim 1200W fiecare, redundanta 1+1 O baterie de ventilatoare

3.7.12. Centru de management operational

Ministerul Sanatatii va fi dotat cu sisteme de sistem de afisare in timp real a datelor prelucrate pe baza registrelor de sanatate intr-un centru de management operational. Aceste sisteme au in componenta statii de lucru, monitoare, imprimante, tastaturi, dispozitive periferice de comanda tip „mouse”, boxe audio si conectica necesara functionarii in ansamblu a echipamentelor.
Sistemul de afișare video a alertelor va avea o dimensiune de minim 4,5m2 cu posibilitatea de afișare concomitentă a mai multor surse video.

Se vor realiza toate conexiunile necesare inclusiv cele de date la un standard minim Cat 6a. Echipamantele audio si video vor fi amplasate intr-un rack standard.

3.8. *Componentele software*

3.8.1. Componenta de Portal

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;
- Personalizarea experienţei utilizatorilor prin posibilitatea personalizării interfeţei de portal (aranjare în pagină, alegere skin-uri etc);
- Să imbunătăţească experienţa utilizatorilor prin utilizarea unor tehnologii bazate pe Web 2.0 / AJAX / WebSockets ;
- 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;
- Suport pentru apelul la distanţă a portlet-ilor folosind standardul Web Services for Remote Portlets

(WSRP);

- Să permită rularea Portalului pe toate distribuţiile majore de sisteme de operare prezente pe piaţă: Windows, Linux şi UNIX.
- 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 platforma pentru rularea aplicatiilor – server de aplicatie

Componenta software pentru rularea aplicatiilor oferă suport pentru asigurarea infrastructurii software necesara executiei aplicatiilor moderne bazate pe standarde deschise. Serverul de aplicatii trebuie sa asigure un set de servicii standard pe care toate aplicatiile dezvoltate si instalate sa il poata accesa si utiliza:

- servicii de clusterizare pentru o scalabilitate si disponibilitate ridicata;
- servicii de securitate pentru protejarea resurselor gazduite;
- servicii de definire si context de executie pentru resursele de aplicatie: conexiuni catre baze de date relationale, cozi de mesaje;
- servicii de manipulare a datelor in format XML;
- servicii de management al tranzactiilor la nivelul aplicatiilor.

Platforma software pentru serverele de aplicatii trebuie sa permita rularea componentelor aplicative conform cu specificaţiile platformei Java Enterprise Edition 7 sau echivalent dar oferind si compatibilitate cu specificaţiile platformelor anterioare.
Platformă tehnologică trebuie să permită instalarea şi execuţia site-urilor web dinamice, serviciilor web şi aplicaţiilor J2EE sau echivalent. Trebuie să ofere suport complet pentru servicii web utilizând specificaţiile JAX-WS si JAX-RPC sau echivalent , respectiv suport pentru Simple Object Access Protocol (SOAP); să ofere suport complet pentru specificaţia Enterprise JavaBeans sau echivalent pentru încapsularea logicii de business a aplicaţiilor.
Plaftoma trebuie sa ofere suport complet pentru standardul Java Messaging Service (JMS), suport complet pentru managementul tranzacţiilor utilizând specificaţia Java Transaction API (JTA) sau echivalent, suport complet pentru standardul Java Authentication and Authorization Service (JAAS) sau echivalent.
Pentru a asigura inalta disponibilitate a sistemului, platoforma trebuie sa includa mecanisme de grupare a serverelor în clustere de servere de aplicaţii atât în topologii de tip activ-activ cât şi activ-pasiv, respctiv stoparea temporara a unui nod din cluster pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale; o alta caracteristica importanta sunt mecanismele de balansarea dinamică a încărcarii sistemului între resursele administrate în cadrul aceluiaşi cluster si mecanismele de scalare a sistemului pe orizontală (Scale Out) şi verticală (Scale Up).
Componenta server de aplicatie trebuie să permită rularea serverului de aplicaţii pe toate distribuţiile majore de sisteme de operare prezente pe piaţă: Windows, Linux şi UNIX.
Componenta server de aplicaţie trebuie să permită folosirea in conjunctie cu un cluster de servere proxy pentru serverele de aplicatie în scopul realizarii administrarii traficului de date dintre serverele de aplicatie avand capabilităţi de balansare, caching, reverse-proxy.
Componenta server de aplicatie trebuie să suporte funcţionarea aplicatiilor pe care le ruleaza in mod balansat intre servere, cu continuarea sesiunii utilizatorului atat timp cat cel putin un server fizic din cluster este functional.

3.8.4. Componenta de tip interoperbilitate

Aceasta componenta va avea suport pentru interoperabilitatea diverselor module ale solutiei conform cu principiile si conceptele arhitecturilor "Service Oriented Architecture" si "Event Driven Architecture": WS-I Basic Profile, WSDL, WS-*, XML, SOAP.
Pentru a asigura mecanismele necesare dezvoltarii facile si urmaririi in activitate a aplicatiilor, componenta de integrare trebuie sa permita includerea sub-proceselor apelate dintr-un proces principal in tranzactia fluxului initiator, precum si posibilitatea de a implementa un mecanism de export al informatiilor (de exemplu variabile de proces, activitati, exceptii) din fluxul de proces direct in baza de date relationala sau cozi de mesaje. Specificarea şi modificarea fluxurilor de mesaje trebuie sa se poată face atât utilizând mediul de dezvoltare integrat al sistemului cât şi un simplu browser web. Pentru a asigura un nivel ridicat de flexibilitate in modelarea fluxurilor, componenta va suporta urmatoarele modele de comunicare: sincron cerere/răspuns, asincron one-to-one, asincron one-to-many, asincron cerere/răspuns (synchronous-to-asynchronous bridging). Toate modelele de comunicare trebuie sa asigure atat persistenta mesajelor cat si garantarea livrarii acestora. Pentru asigurarea decuplarii interfetelor de comunicare componenta va include capabilităţi extinse de transformare şi dirijare a datelor bazate pe conţinutul transportat.
Componenta de interoperabilitate trebuie să asigure modelarea și execuția fluxurilor de lucru, elaborate folosind standardele BPMN, în vederea îndeplinirii sarcinilor de automatizare a proceselor în cadrul arhitecturii orientate pe servicii.
Componenta de interoperabilitate trebuie să asigure utilizarea standardului WS-BPEL pentru combinarea de multiple servicii web sincrone și asincrone în cadrul fluxurilor de procese colaborative și tranzacționale, în cadrul arhitecturii orientate pe servicii.
Componenta de interoperabilitate trebuie să includă un registru centralizat de stocare (repository) conform standardului deschis Universal Description Discovery and Integration, prin care să se realizeze managementul artefactelor arhitecturii orientate pe servicii (procesele de afaceri, componente, politici, servicii de date) în ceea ce privește drepturile de acces, durata de viață, versionarea, etc. Pentru procesele de integrare ce nu pot fi executate în totalitate în mod automat și este nevoie de interacțiune umană, componenta de integrare și transformare trebuie să ofere posibilitatea definirii și gestionării de artefacte de interacțiune umană în cadrul proceselor BPEL, care să permită intervenția unor utilizatori cu roluri specifice la nivelul aplicațiilor.
Componenta de interoperabilitate trebuie să includă un modul de colectare și procesare a datelor în vederea extragerii informațiilor și prezentare a acestora într-o formă vizuală, cu scopul detectării problemelor de performanță. Modulul va dispune de o consolă Web de management și monitorizare, care să afișeze sub formă de dashboard-uri statistici privind cel puțin serviciile proxy, API-uri de tip REST, endpoint-uri și medieri, pentru o anumită perioadă de timp.
Componenta de interoperabilitate trebuie să asigure filtrarea și transformarea mesajelor XML utilizând cel puțin următoarele standarde deschise W3C Extensible Stylesheet Language Transformation (XSLT) și xQuery (XML Query).
Componenta de interoperabilitate trebuie să asigure interconectarea la sistemele externe pe baza conectorilor de tip SOAP, REST și Java API.
Componenta de interoperabilitate trebuie să asigure securitatea serviciilor Web pe baza specificațiilor standardelor WS-Security, WS-Policy și WS-Security Policy. Pentru a asigura criptarea / decriptarea mesajelor în vederea asigurării confidenţialităţii mesajelor transportate si semnarea / verificarea digitală a mesajelor în vederea asigurării integrităţii şi non-repudierii mesajelor.
Componenta de interoperabilitate va fi implementată în cluster de tip activ-activ, pentru a asigura comutarea sarcinilor de pe un nod pe altul in mod transparent si automat pentru aplicatiile care utilizeaza

aceste servicii – astfel, atat timp cat cel putin un nod din cluster este functional, sistemul nu trebuie sa sufere intreruperi.
Componenta de interoperabilitate trebuie sa ofere posibilitatea de a rula pe diverse platforme hardware precum si pe sistemele de operare majore existente pe piata (Windows, Linux, Unix).

3.8.5. 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 50 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;
- parametrii de memorie sa poata fi ajustati dinamic si automat de catre baza de date astfel incat zonele de memorie sa fie dimensionate in concordanta cu tipul de operatii ce se desfasoara la un moment dat iar pentru a face fata unui numar foarte mare de utilizatori, baza de date trebuie sa ofere un mecanism de connection pooling care sa optimizeze folosirea resurselor server-ului la operatiile de tip login/logout

Arhitectura de tip cluster trebuie sa asigure si o balansare a incarcarii intre noduri la nivelul cererilor si executiilor pe baza de date aflata in cluster oferind o incarcare uniforma a acesteia iar din punctul de vedere al utilizatorilor 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 numai pentru fisierele care au suferit schimbari de la ultimul backup si pentru fisierele nou create (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.
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).

3.8.6. 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 dezvoltate prin proiect, 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.
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 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.
- 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 (grafice, 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.
- 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 trasabilităţii 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.

Cerinţe 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, Ajax, 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

3.8.7. 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 și totodată pentru asigurarea confidențialității informațiilor și protejării datelor cu caracter personal, sistemul informatic va inlcude o componentă de mascare pentru transferul din bazele de date de producție 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 confidențialitatea și protecția datelor cu caracter personal.
Soluția trebuie sa îndeplinească următoarele caracteristici tehnice minime:

- Soluția trebuie să poata profila date existente pentru descoperirea automata a modelului de date și a conținutului sensibil.
- Soluția trebuie să asigure generarea de date în conformitate cu următoarele formate:
    - Oracle DB Server, MySQL
    - IBM DB2 / 400 iSeries, Informix
    - Microsoft SQL Server
    - PostgreSQL, Ingres
    - Sybase
    - Fișierele XML, SQL, CSV, fișiere JSON, fișiere HTML
- Soluția 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.
- Soluția trebuie să dispună de posibilitatea creării de date invalide, bazate pe cererile utilizatorilor
- Soluția trebuie să fie capabilă să modifice date sensibile cu un conținut alternativ. O astfel de capacitate trebui să includă următoarele funcții:
    - Conservare genului - atunci când substituirea nume, nume masculine sunt substituite numai cu alte nume de sex masculin, și în mod similar de sex feminin, cu doar nume feminine.
    - Conservarea integrității semantice - păstrarea constrângerilor aplicate unui set de date ca o valoare maximă sau pentru numere de card de credit
    - Valoarea Cumulată - valorile totale și medii ale unei coloane mascată de date ar trebui să fie păstrate, fie strâns sau cu precizie
- Abilitatea de a extrage în mod condiționat seturi de date intacte referențial, în mod constant din multiple tipuri de baze de date sau fișiere

- Soluția trebuie să dispună de capacitatea de a asocia cazuri de testare cu atributele de date necesare, de a le găsiți în conținutul de date existente și de a le rezerva pentru utilizatori autorizați și de a bloca înregistrările/cheile de la alte utilizări de testare.
- Soluția trebuie să aibă capacitatea descoperi automat relațiile între date și să ofere, de asemenea, posibilitatea administratorilor să modifice regulile de descoperire utilizate.
- Soluția trebuie să furnizeze o analiză a datelor și a metadatelor bazelor de date descoperite
- Urmare a procesului de descoperire, soluția trebuie să furnizeze rapoarte și documentare privind datele descoperite.
- Soluția trebuie să dispună de capacitatea de a înțelege modelele de date, în scopul de a menține integritatea referențială într-o bază de date. De asemenea, soluția trebuie să fie capabilă de a înțelege modelele de date, în scopul de a menține integritatea referențială între diferite baze de date.
- Soluția trebuie să dispună de posibilitatea modificării datelor generate
- Soluția 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
- Soluția trebuie să permită o mascare directă a datelor
- Soluția trebuie să permită programarea rulării funcțiilor de mascare a datelor.
- Soluția trebuie să fie capabilă să lucreze și cu date care nu sunt 100% corecte, pentru a putea folosi aceste date greșite în timpul procesului de testare. Soluția trebuie să fie configurabilă ca și aceste date să fie prelucrate.
- Soluția trebuie să fie capabilă să genereze date invalide pentru a fi folosite in teste specifice.
- Soluția trebuie să ofere posibilitatea extragerii unui subset de date care să fie mascate și să poată fi prelucrate în procesul de testare.
- Soluția trebuie să suporte autentificarea folosind integrarea cu sisteme de tip LDAP
- Soluția trebuie să ofere mecanisme de control a accesului la date bazate pe utilizatori, roluri și grupuri
- Soluția 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

3.8.8. Componentele de securitate

Din punct de vedere al componentelor necesare pentru a asigura cerintele 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

Securizare Acces Servicii Electronice

Datorita cerintelor de integrare ale sistemului REGINTERMED 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 doreste 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 funcţii 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.
- Sa poata fi integrat cu solutii de tip directory incluzand directoare compatibile LDAP v.3
- 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.

Controlul accesului utilizatorilor la sistem

REGINTERMED 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 doreste 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 mai metode de autentificare si autorizare diferite pentru fiecare grup de resurse in parte
- Sa ofere o interfață de administrare de tip web pentru accesul facil la 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.
- 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
- 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.
- Solutia trebuie sa permită definirea de politici de acces individualizate pentru sisteme, in functie de rolul acestora.
- 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 SDK.
- 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.

Componenta de administrare unitara a conturilor de utilizator

Datorita specificului datelor cu caracter personal gestionate in cadrul REGINTERMED 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 doreste 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 toate drepturile de acces pe care utilizatorul le are in alte sisteme, 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 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)
- 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

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 doreste 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 interfaţă de administrare
- Să permită diagnosticare pentru timp de răspuns slabi la operaţii de autentificare, căutare sau replicarea
- Să permită generarea de alarme dacă procesorul a ajuns la limită
- 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

Componenta de autentificare securizată a utilizatorilor

Soluția trebuie să analizeze în timp real a riscurile pentru a proteja datele și tranzacțiile sensibile.
Soluția trebuie să protejeaze atat canalele web, mobile și să integreaze datele din toate canalele de comunicare pentru o analiză cuprinzătoare a riscurilor.
Soluția trebuie să efectueze o analiză transparentă, inteligentă a riscurilor pentru a oferi o mai mare siguranță că utilizatorul este corect.
Soluția trebuie să asigure autentificarea securizată a utilizatorilor la resursele publicate.
Soluția trebuie să asigure autentificarea utilizată a utilizatorilor care utilizeaza dispozitive mobile de tip smartphone și tabletă pentru actualizarea informațiilor.
Soluția de autentificare nu trebuie să necesite modificarea aplicației cu care se conecteaza. Soluția de autentificare trebuie să se integreze cu aplicațiile existente fără să necesite modificarea acestora.
Soluția de autentificare trebuie să asigure autentificarea sigură a utilizatorilor atât la conectarea acestora (login) cât și la utilizarea unor funcționalități specifice.
Soluția de autentificare securizată trebuie să analizeze permanent nivelul de risc aferent autentificării utilizatorilor, pe baza cel puțin a următorilor parametri:

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

Soluția trebuie să suporte metode out-of-band, cum ar fi notificările push și parolele unice (OTP) livrate prin e-mail, text sau voce pentru autentificarea step-up.
Soluția trebuie să ofere seturi de reguli implicite, care acoperă modele tipice de atacuri și impersonări, ușor de utilizat și personalizate.
Soluția de autentificare securizată trebuie să detecteze automat situațiile în care există un risc de autentificare și în aceste situații să solicite o autentificare suplimentară de tip: cod acces de unică folosință (One Time Password – OTP), întrebare de securitate sau similar.
Soluția 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, soluția de autentificare va putea iniția urmatoarele acțiuni:

- Permite accesului utilizatorului la sistemul informatic sau la funcționalitățile sensibile
- Solicită utilizatorului un element de securitate suplimentar: cod acces de unică folosință (One Time Password – OTP) sau întrebare de securitate
- Inițiază 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 canalele 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 iPhone store, 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.

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 și 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 înregistreze informații de audit referitoare la toate operațiunile efectuate de utilizatori, inclusiv cele efectuate de utilizatorii anonimi
- 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 tendințe și modele ascunse de atacuri
- Soluția trebuie să asigure menținerea tuturor datelor de audit privind autentificarea și activitatea utilizatorilor și administratorilor într-o baza de date relațională, precum și exportarea log-urilor soluției în format Syslog către sisteme externe de analiză a log-urilor
- Soluția trebuie să ofere un set de rapoarte predefinite privind managementul și activitatea utilizatorilor și administratorilor – rapoarte ce pot fi vizualizate în cadrul soluției sau exportate către instrumente de raportare externe

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 REGINTERMED - detecţia rapidă a incidentelor de securitate, a utilizării incorecte a resurselor de reţea sau a performanţelor 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
- Solutia trebuie sa ofere monitorizarea traficului de reţea prin captura acestuia sau colectarea şi/sau generarea de metadate de tip flow
- Solutia trebuie sa ofere prin intermediul unei console centrale vizibilitate unificată asupra întregii infrastructuri de comunicaţii prin agregarea datelor primite pe baza traficului de retea si loguri de la diferite siteme, precum și detecţia rapidă a incidentelor de securitate, a utilizării incorecte a resurselor de reţea sau a performanţelor neoptimale
- 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. 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 2500 EPS sustinute
- Solutia trebuie sa ofere posibilitatea de a rula query-uri in timp real si detectia anomaliilor
- Solutia trebuie sa ofere cel putin 20TB de spatiu de stocare a datelor pe termen lung pentru investigatii amanuntite
- Solutia trebuie sa ofere posibilitatea instalarii in mediu virtual
- Solutia trebuie sa ofere licentele necesare atât pentru sistemele de operare, cat si pentru aplicatii terte

Cerinte minime

- Solutia trebuie sa ofere o consola unica centralizata de administrare web pentru toate componentele
- 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: click 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 posibilitatea de import si export din/in sistem a regulilor de corelare
- Solutia trebuie sa ofere capabilități de investigare detaliata direct din pagina de sumarizare a corelarii 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 de export si import a regulilor de corelare

- 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 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 acces pe baza de roluri
- Solutia trebuie sa ofere interfață web cu suport HTML5
- Solutia trebuie sa suporte cel putin urmatoarele browsere web: Chrome, Internet Explorer, si Mozilla Firefox
- 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 functionalitati de auditare si log-uri ale sistemului
- Solutia trebuie sa permită detectarea atacurilor de tip DDoS sau similare prin analiza traficului de rețea
- 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 reţea şi compararea în permanenţă a traficului observat în timp real cu tiparele observate în trecut
- Solutia trebuie sa permită introducerea în analiză a informaţiilor ce provin de la alte tipuri de tehnologii cum ar fi web-proxy, IDS/IPS, firewall sau NAC
- Solutia trebuie sa ofere capabilităţi DPI asupra traficului folosind soluţii de tip SPAN sau TAP
- Solutia trebuie sa permită generarea de rapoarte bazate pe trafic, servicii, protocoale, adrese IP, incidente de securitate sau utilizatori
- 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 suporte o lista de variabile ce pot fi folosite la 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 permită adaugarea de informații aditionale rapoartelor: header, body text si comentariu
- Solutia trebuie sa ofere optiunea de a programa rularea rapoartelor: ad-hoc, ora de ora, zilnic, saptamanal, lunar
- Solutia trebuie sa ofere posibilitatea inestigatiei detaliate (drill-down) direct din raportul generat
- 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, fără a fi nevoie de licente aditionale
- Solutia trebuie sa ofere posibilitatea de a exporta din interfață web log-urile colectate
- Solutia trebuie sa permită configurarea mesajului de login in aplicatie

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:

- Realizează teste de vulnerabilitate pentru baza de date precum si descoperirea si clasificarea datelor confidențiale (date personale, date financiare si date customizate).
- Detectează vulnerabilitățile cunoscute ale bazei de date ofertate si face verificări de actualizare a bazelor de date la noi versiuni si verifică conturile de utilizatori de bază de date
- Monitorizează accesul la informațiile din baza de date (cu suport pentru limbajele DCL, DML, DDL si procedurile salvate). Definirea politicilor de monitorizare trebuie sa permită următoarele criterii: utilizatorul bazei de date, utilizatorul aplicației, tabele, coloane, tip de date, schema bazei de date, număr de apariții, acces către date sensibile (definite de administrator) sau manual, precum regex sau cuvânt cheie) cat si date luate dintr-un sistem extern (LDAP, baza de date externa cu interogare SQL si date importate din fisiere)
- Asigură definirea criteriilor de acces pentru utilizatorii bazei de date catre obiecte specifice din baza de date prin crearea automata a listelor de utilizatori si a interogarilor sql pe care utilizatorul le-ar putea face in tabela bazei de date. Totodata solutia trebuie sa permita crearea automata a listelor pentru: IP sursa, nume aplicatie, numele sistemului de operare din care utilizatorul are acces la resurse. Acele liste de obiecte invatate si create automat trebuie sa fie accesibile administratorului in timpul creari politicilor fara a se specifica continutul listelor.
- Asigură crearea unei liste de tabele la care anumiti utilizatori nu au acces. Trebuie sa existe si posibilitatea de a defini zile din saptamana si ore in care un utilizator se poate conecta la baza de date.
- In logurile de evenimente si anomalii trebuie sa fie disponibile urmatoarele: utilizatorii de aplicatie, ID de sesiune, adresa IP sursa si intreaga interogare SQL, pentru o identificare precisa si un raspuns eficient din punct de vedere al securității.
- Asigură implementarea unei solutii de protectie bazata pe semnaturi pentru vulnerabilitatile gasite prin metodele de testare specifice mentionate mai sus.
- Asigură detectarea comenzilor executate pe sistemul de management al bazei de date si identificarea unei incercari de export direct al bazei de date.
- Asigură stocarea tuturor evenimentelor in mod securizat in forma criptata.
- Solutia trebuie sa raporteze numarul de coloane afectate in baza de date cand un utilizator adauga date.
- Solutia trebuie sa raporteze numarul de inregistrari prezentate de baza de date cand un utilizator citeste date din aceasta.
- Solutia trebuie sa aiba posibilitatea de a defini politici prin care sa verifice numarul de inregistrari prezentate unui anumit utilizator intr-o anumita perioada chiar din mai multe cereri (suma cererilor dintr-o perioada definita)
- Solutia trebuie sa trimita alerte folosind minim urmatoarele: SNMP, syslog, e-mail
- Solutia trebuie sa ofere rapoarte predefinite pentru:
    a. Alerte securitate
    b. Evenimente de sistem

c. Monitorizarea utilizatorilor bazei de date
d. Rezultatele evaluarii de securitate

- Solutia trebuie sa aiba posibilitatea de a crea rapoarte customizate in mod text si grafic.
- Sistemul trebuie sa fie actualizat lunar, pentru urmatoarele: semnaturi atac, lista politicilor de securitate, verificari de vulnerabilitati si rapoarte. Actualizarile de sistem trebuie sa fie disponibile automat pe internet, programabile de catre administrator sau prin download manual al fisierului de update.
- Monitorizarea activității bazei de date se va realiza pe bază de agent. Agentul trebuie sa trimita catre serverul de management activitatile locale ale utilizatorilor, in timp real.
- Solutia trebuie sa monitorizeze parametrii agentului si sa raporteze in cazul in care:
  a. Agentul functioneaza correct
  b. Nu exista comunicatie din partea agentului
  c. Agentul nu detecteaza nicio activitate pentru o perioada definita de timp
  d. Agentul incepe sa detecteze activitati
- Agentul trebuie sa functioneze in doua moduri: inline si sniffing. In mod “sniffing” activitatea userului este trimisa imediat catre sistemul de management, fara intarzieri, dar actiune de blocare nu este garantata. In modul “inline” actiunea utilizatorului este oprita pana se realizeaza verificarea cu politicile de securitate si este blocata in cazul in care actiunea nu este conforma.
- Agentul trebuie sa descopere automat noi interfete a bazelor de date, de orice tip (locale sau in retea) si sa aplice reguli de monitorizare automat.
- Solutia trebuie sa fie capabila sa trimita datele culese prin politicile active catre minimum: NFS, HTTP repositories, servere FTP si copii SCP catre o anumită masina.

3.8.9. Integrare, consolidare si replicare de date

Pentru asigurarea cerintelor de integrare, pe langa componenta de integrare la nivelul aplicatiilor si serviciilor web este necesara si o integrare la nivel de date pentru a se putea asigura integrarea, consolidarea si replicarea datelor cu bazele de date si a altor sisteme cu care sunt necesare integrari si replicari.

Din punct de vedere functional, pentru asigurarea consistentei si consolidarii datelor din bazele de date este necesara asigurarea unei solutii de integrare si replicare de date care sa asigure:

- replicarea de date intre baza de date a aplicatiilor existente si baza de date a solutiei cu impact minim asupra sistemului de productie (ex: mediul de DR), cu posibilitatea de transmitere a datelor imediat, in timp real, sau la un moment de timp ulterior definit de administrator, cu asigurarea integritatii tranzactiilor.
- integritatea tranzactionala atat la nivel surselor de date cat si la nivelul bazei de date destinatare, iar pentru consolidarea bazei de date centrale sa se permita replicarea inclusiv a bazelor de date distribuite la nivelul sucursalelor;
- sincronizarea datelor intre centre de date aflate la distanta intr-o configuratie de tipul activ-activ, de exemplu intre un centru de rezerva principal si unul rezerva care se va constitui ulterior pentru recuperarea in caz de situatii neprevazute.

Din punct de vedere tehnic, pentru asigurarea necesitatilor de replicare a datelor intre bazele de date ale Institutiei solutia de replicare a datelor trebuie sa indeplineasca urmatoarele:

- Sa permita replicarea de volume mari de date tranzactionale intre baze de date eterogene din punct de vedere tehnologic cu impact minim asupra bazei de date de productie. Replicarea volumelor de date mari sa poata fi realizata in timp real.

- Sa asigure integritatea tranzactionala si consistenta datelor din bazele de date sursa si destinatie, cu asigurarea posibilitatii de transmitere a datelor imediat sau la un moment de timp ulterior, ales de catre administratorul sau operatorul solutiei de replicare;
- Pentru consolidarea unei bazei de date centrale sa permita replicarea datelor si sincronizarea acestora si din baze de date distribuite sau intre bazele de date distribuite;
- Sa permita doar replicarea datelor comise la nivelul bazei de date, bidirectional pe baza de jurnal, cu asigurarea unor mecanisme de captare a datelor modificate in sistemele supuse operatiilor de replicare.
- Mecanismele de replicare sa fie rapide si sa permita operatii paralele de mutare masiva a datelor intre bazele de date, diferite de metodele standard de export/import al datelor.
- Sa dispuna de o interfata web pentru urmarirea si vizualizarea executiei proceselor ce au loc la nivelul bazelor de date sursa si destinatie, si o interfata grafica de dezvoltare prin intermediul careia sa se poata defini conexiunile la bazele de date sursa si destinatie, si definirea parametrilor corespunzatori incarcarii initiala a datelor, sincronizarii, si altor pasi aferenti replicarii.
- Pentru optimizarea si asigurarea securitatii datelor, solutia trebuie sa permita criptarea si compresia datelor supuse operatiilor de replicare si sa permita gestionarea automata a memoriei;
- Pentru asigurarea integritatii tranzactionale si consistenta datelor trebuie sa se asigure instrumente de urmarire imediata a tranzactiilor nivelul bazelor de date sursa si destinatie si sa dispuna de instrumente de detectare a conflictelor de date, de solutionare a acestora si de notificare prin email la aparitia unor eveniment stabilite.
- Sa dispuna de o arhitectura modulara si de o topologie flexibila - de tipul una sau mai multe surse replicate la una sau mai multe destinatii cu posibilitatea de asigurare a configurarilor bidirectionale;
- Sa foloseasca protocolul TCP/IP pentru a replicarea datelor, asigurand astfel posibilitatea de replicare a datelor aflate la distanta din punct de vedere geografic.
- Pentru indeplinirea cerintelor de disponibilitate si recuperare solicitate solutia trebuie sa permita:
    - mentinerea noului sistem disponibil in permanenta, atat in timpul intreruperilor planificate, cat si a celor neplanificate.
    - zero timp de nefunctionare pentru intretinerile planificate cum ar fi operatiile de migrare sau de actualizare.
    - disponibilitate, toleranta si recuperare in caz de dezastru sau situatii neprevazute
    - sincronizarea de date intre mai multe centre de date intr-o configuratie de tip activ-activ.

3.8.10. Monitorizare date, sisteme si aplicatii

Având în vedere complexitatea tehnică și funcțională a REGINTERMED, 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.

Monitorizare infrastructura de aplicații
Cerinte:

- 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 IT și de aplicație să înțeleagă nivelurile acceptate ale serviciilor livrate către utilizatorii finali, pentru a asigura continuitatea sistemului în condiții 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.

Soluția pentru Sistemul de monitorizarea a performanțelor aplicațiilor trebuie să fie una consacrată în piață care să poate oferi o perspectivă asupra aplicațiilor web din toate punctele de vedere (sistem, rețea, aplicație și experiența 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 performanțelor aplicațiilor va fi utilizat pentru a asigura o strategie de monitorizare în timp real a perfomanțelor aplicațiilor web utilizate (portal, website, acces web, etc.) ce va permite:

- monitorizarea experienței 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 aplicație, 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 și gestionarea informațiilor referitoare la calitatea serviciilor oferite utilizatorilor - măsurarea serviciilor de tip Service Level Agreements (SLA);
- asigurarea unei vizibilități a tranzacțiilor de grad înalt;
- determinarea rapidă a sursei problemelor de performanță;
- trierea și identificarea elementelor de infrastructură, precum și analiza cauzelor principale;
- prioritizarea și trierea incidentelor care se bazează cu adevărat pe impactul asupra activității;
- asigurarea monitorizării aplicațiilor în mod proactiv și predictiv;
- creșterea frecvenței de raportare și asigurarea unei continue îmbunătățiri a performanțelor;
- asigură monitorizarea istorică, dar și în timp real a performanțelor aplicațiilor și experienței utilizatorilor;
- analizarea traficului SSL, precum și importarea și gestionarea cheilor private pentru accesul la aplicațiile 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;
- 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 şi gestionarea tuturor componentelor din cadrul proiectului;

- Sistemul centralizat 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;
- 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/gatuiri;
- 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;
- Monitorizarea browser-elor în timp real, monitorizarea timpilor de răspuns la acțiunile utilizatorului în timp real;
- Starea de funcționare a paginilor web;

- Monitorizarea tranzacțiilor pe toată durata de viață a acestora

Monitorizare infrastructura de date

- Să ofere capabilităţi incluse si automate de monitorizare şi diagnosticare continuă a stării bazei de date în scopul identificării potenţialelor probleme de performanţă si a factorilor de degradare a acesteia.
- Soluţia oferită va trebui să monitorizeze disponibilitatea şi performanţele serverelor de baze de date.
- Să ofere agenţi specifici pentru monitorizarea bazelor de date Oracle, IBM DB2, Microsoft SQL şi Sybase
- Pentru bazale de date trebuie colectacte, fără a se limita la, cel puțin umătoarele informații: numărul utilizatorilor activi, buffer cache hit ratio, mărimea bazelor date, mărimea tablespace-urilor, cantitatea de memorie utilizată, cantitea de informație citită de pe disc.
- Datele capturate privind functionarea bazelor de date vor fi livrate printr-o interfaţă intuitivă şi vor fi disponibile prin intermediu de rapoarte date istorice şi în timp real.
- Sistemul trebuie să prezinte categorii de indicatori de performanță:
  - CPU și procese
  - Memorie și disk
  - Sesiuni și servicii
  - Conținut si cache
  - Host și aplicație
- Indicatorii de peformanță prezentați trebuie să cuprindă, fără a se limita la: tranzacții active, timp de răspuns pentru interogări, informații despre buffere (timpi de așteptare, eficiență), informații despre procese consumatoare de resurse (procesor și memorie), informații despre activitatea disk-ului (disk I/O) și eficiența lock-urilor.

- Sistemul trebuie să identifice automat situațiile de funcționare anormală a bazelor de date și să notifice administratorii în legătură cu problemele de performanță sau cele de alocare de resurse.

Monitorizarea infrastructurii server

Soluţia de monitorizare a sistemelor trebuie să ofere următoarele funcţionalităţi:

- Capabilitatea de a monitoriza sisteme Windows, UNIX şi 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 şi GUI.
- Soluția trebuie să permită autentificarea folosind integrare cu LDAP.
- Monitorizarea următorilor parametri:
    - Procesor: utilizarea fiecărui procesor din sistem şi compararea gradului de utilizare curentă cu praguri critice predefinite si configurabile
    - Sistem de fişiere: spaţiul ocupat din sistemul de fişiere şi comparaţia acestuia cu praguri critice predefinite şi configurabile.
    - Memorie şi I/O - utilizare
    - Starea serviciilor sistemului
    - Performanţele serverelor de baze de date şi ale serverelor de aplicaţii.
- Emiterea de alarme - soluţia trebuie să poată emite alerte prin mai multe mijloace: e-mail, mesaje în consolă, mesaje administrative, SMS
- Acţiuni corective: soluţia trebuie să se poată configura astfel încât să execute acţiuni corective automate (fără intervenţia administratorilor) în cazul detectării de erori sau în cazul degradării performanţelor.
- Agenţii pentru fiecare sistem nu trebuie să interfereze cu operaţiile normale ale sistemului pentru a nu afecta performanţele acestuia.
- Instalare/configurare agenţi dintr-o singură locaţie pentru toate sistemele şi componentele monitorizate.
- Extensibilitate facilă pentru includerea scripturilor customizate de monitorizare a aplicaţiilor dezvoltate în interiorul organizaţiei.
- 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 şi din trecut pentru orice sistem dintr-o consolă web, centralizată, pentru monitorizare.
- Capabilitatea de a trimite rezultatele de la colectarea datelor şi analiză la aplicaţia de corelare a evenimentelor.
- În cazul în care unul din serverele de monitorizare nu îşi poate îndeplini funcţiunile, agentul, fără intervenţia administratorilor, trebuie să poată transmite informaţiile către alt server de monitorizare.

Monitorizare sistemului de virtualizare

- Soluția trebuie să permită monitorizarea sistemelor folosind agenți configurabili cât și monitorizarea fără agenți (la distanță).
- Să ofere agenţi specifici pentru monitorizarea mediilor virtuale ca: VMWare vCenter, VMWare Cloud, IBM LPAR, Citrix XenServer, Solaris Zone, Cisco UCS, Red Hat Enterprise Virtualization, Microsoft HyperV.
- Soluția trebuie monitorizeze atât infrastructura fizică (hypervisor), cât și infrastructura virtuală (virtual machine).
- Soluția trebuie să dispună de o interfață de vizualizare și configurare facilă.
- Soluția trebuie să identifice automat toată infrastructura virtuală și să o monitorizeze atât pentru performanță cât și pentru funcționare curentă.

- Soluția trebuie să se integreze cu soluția pentru monitorizarea evenimentelor și a infrastructurii.
- Soluția trebuie să prezinte rapoarte ca: topul celor mai utilizate mașini virtuale, topul celor mai putin utilizate mașini virtuale, inventar al mașinilor virtuale, utilizare datastore, etc.
- Soluția trebuie să ofere posibilitatea de a proviziona noi mașini virtuale prin intermediul interfețelor de configurare.

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 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;
- Platforma ce include mecanisme integrate de agregare a resurselor fizice din infrastructura, mecanisme integrate de analiza predictiva si aplicare proactiva de politici asupra resurselor fizice si virtuale 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, 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.
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: IBM, Dell, HP, Sun, Intel, 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, Netware 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 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

Caracteristica	Cerinta tehnica minimala
	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 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

Caracteristica	Cerinta tehnica minimala
	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 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

Caracteristica	Cerinta tehnica minimala
	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; ▪ 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

Caracteristica	Cerinta tehnica minimala
	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 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;

Caracteristica	Cerinta tehnica minimala
	▪ 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 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 64 procesoare fizice, cu minim un centru de management si monitorizare. Solutia va contine toate

Caracteristica	Cerinta tehnica minimala
	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 soluţii de asistenta tehnica (help-desk) care sa limiteze cauzele și efectele defectelor REGINTERMED și totodată să sigure monitorizarea SLA-ului stabilit. Sistemul va permite preluarea, înregistrarea si urmărirea sesizărilor (incidente/tickete) privind funcţionarea 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 5. Furnizorul va asigura implementarea și operaţionalizarea soluţiei complet funcţionale de help-desk pentru cei 5 de operatori (din care 3 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.

3.8.13. Solutia de recuperare in caz de dezastru

Implementarea unei solutii de recuperare in caz de dezastru are ca obiectiv furnizarea unei solutii care sa asigure accesul la date si la aplicatii cu caracter critic pentru Beneficiar chiar si dupa un eventual dezastru ce face total inoperabila activitatea sistemelor IT din mediul Principal..
Necesitatea majora este dictata de:

- costurile importante ce pot surveni in urma declansarii unui dezastru, fara posibilitatea de a oferi utilizatorilor capacitarea de reluare a lucrului: penalitati, imposibilitatea transmiterii informatiilor asociate documentelor administrate, etc
- impactul de imagine si inicidente de natura legala ce pot afecta beneficiarul datorita nerespectarii legislatiei sau chiar si numai imposibilitatea de a prezenta informatia privitoare la diverse aspecte operationale organismelor legale sau de investigatie;

Cerinte disponibilitate
Din punct de vedere al performantei si al disponibilitatii solutia trebuie sa satisfaca urmatoarele cerinte:

- Reconfigurarea solutiei de comunicatii existente pentru obtinerea conectivitatii la solutia din mediul secundar atat pentru comunicatiile de replicarea datelor cat si pentru accesul utilizatorilor la aplicatiile protejate;
- Sa nu existe pierderi de date majore in caz ca principalele servere de productie sunt distruse
- Strategia pentru recuperarea datelor in cazul de dezastru trebuie sa ia in calcul intretinerea hardware planificata si testarea regulata a procedurilor care trebuiesc aplicate in cazul unui dezastru, fara a fi necesara oprirea sistemelor pentru o perioada mai mare decat cea specificata anterior;
- Strategia pentru recuperarea datelor in caz de dezastru trebuie sa nu afecteze performanta sistemelor de productie si, in anumite cazuri, sa poata chiar spori perfomanta sistemului prin posibilitatea de a rula rapoarte si/sau proceduri de backup al bazei de date pe baza de date standby din site-ul secundar;
- Solutia de replicare trebuie sa ofere o utilizare eficienta a retelei, astfel incit doar informatia asociata modificarilor sa fie transmisa catre sistemul secundar , fara a duplica inutil informatiile;
- Solutia trebuie sa poata functiona si pe o retea IP standard, fara a necesita spatii de stocare intermediare;
- Sa permita comutarea activitatii obisnuite pe site-ul DR, in cazul in care se decide aceasta;
- Solutia sa permita aplicarea schimbarilor cu o anumita intarziere definita, ca o posibila rezolvare in cazul datelor corupte pe site-ul primar sau in caz de erori umane;
- Solutia sa permita ca toate componentele aplicative sa-si poata relua activitatea pe mediul secundar in maxim 4 ore incepand de la momentul aparitiei evenimentului de dezastru.

Cerinte privind asigurarea integritatii datelor
Exista riscul aparitiei unor erori logice in ceea ce priveste stocarea datelor pe disc (aceste erori pot fi legate de stocarea fizica a fisierelor pe suportul de stocare sau deranjamente logice in interiorul fisierelor). In acest caz trebuie ca strategia de recuperare in caz de dezastru sa asigure integritatea datelor din bazele de date.

In acest scop se doreste asigurarea unei copii de siguranta, le nivel logic, care sa nu propage eventualele probleme care pot aparea la stocarea datelor, in mod fizic pe disc.
Mecanismul de replicare la distanta trebuie sa asigure:

- Operatiile de transformare a bazei de date standby in baza de date primara, in caz de nefunctionare sau controlata, sa fie posibila realizarea cu usurinta si schimbarea rolurilor primar si secundar intre bazele de date
- Minimizarea timpului de nefunctionare pentru sistemul de productie in cazul nefunctionarii planificate
- Erorile fizice la nivel de storage nu trebuie sa poata fi propagate catre baza de date standby
- Baza de date secundara trebuie sa poata fi utilizata in scopul degrevarii bazei de date de productie pentru operatii de backup, raportare, consolidare si interogare in general, reducand astfel incarcarea CPU si I/O pe baza de date primara
- Trebuie sa existe un mecanism de reluare a procesului de replicare in cazul intreruperii conexiunii dintre baza de date primara si cea standby, automat, fara interventia unui administrator de baza de date
- Trebuie sa existe o interfata grafica pentru administrarea procesului de replicare, care sa ofere date statistice si optiuni de diagnostic si investigare de performanta

3.8.14. Componenta geospatiala

Soluția ofertată trebuie să conțină o infrastructură GIS bazată pe produse mature de tip COTS și configurări ale acestora pentru implementarea funcționalităților solicitate, care să răspundă nevoilor privind numărul de utilizatori ai sistemului (utilizatori interni și utilizatori externi, inclusiv publicul larg), încărcarea rețelei și a traficului de date pentru vizualizarea, accesarea și consultarea resurselor geospațiale partaje prin sistemul GIS.
Minimal, se solicită următoarele produse și licențe COTS:

- Produs și licență desktop sau web pentru colectarea, producerea, gestionarea, filtrarea și configurarea resurselor și obiectelor geospațiale

Cerinte minimale:

- Să permită definirea de proiecte de tip GIS, incluzând diverse tipuri de proiecții geospațiale, tipuri de hărți – raster și vectori, definirea de obiecte geospațiale cu mai multe geometrii: punct, poligon, coridoane;
- Să permită definirea mai multor straturi grafice, definirea de metadate, posibilitatea de a îngloba obiecte georeferențiate și a face asocieri între acestea și față de straturile grafice existente;
- Să permită definirea unor seturi de atribute și metadate pentru tipurile de obiecte manipulate pe straturile grafice; Straturile grafice pot fi virtuale sau conectate direct la surse de date de stocare/furnizare date GIS: tabele GIS, baze de date GIS, servicii web GIS;
- Să permită încărcarea și afișarea de date raster și vector în diferite formate și proiecții;
- Să permită preluarea și înglobarea în proiectele GIS a resurselor online de date, prin servicii web OCG: WFS, WMS, WCS, WMTS;
- Să înglobeze instrumente vizuale pentru combinarea mai multor surse și resurse de date, care pot fi asociate între ele sau asociate cu elemente noi, planificate de către utilizator;
- Să conțină mecanisme pentru navigarea prin hărți și obiectele geospațiale, să conțină mecanisme de preview a datelor și hărților, să permită căutarea, filtrarea, accesarea și consultarea atributelor și metadatelor obiectelor și hărților;
- Să permită definirea de structuri de date geospațiale și salvarea și manipularea lor în baze de date GIS interogabile SQL;

- Să permită definirea de etichete, formate de afișare a simbolurilor și simboluri particularizate, atât din puncte de vedere grafic și parametrizabile în funcție de valorile atributelor obiectelor reprezentate;
- Să permită preluare de date GPS și încărcarea pe straturile grafice ale proiectului;
- Să permită operațiuni de manevrare a conținutului proiectelor: zoom, pan, mini-map, transparență, grid lines, snapping;
- Să înglobeze instrumente pentru măsurarea obiectelor de pe hartă: dimensiuni liniare, arii, volume, unghiuri;
- Să permită operațiuni de geoprocesare pe geometriile obiectelor: concatenare, alipire, intersecție, reuniune, scăderi/substragere; Managementul operațiunilor de geoprocesare să poată fi planificat, introdus pe scripturi de execuție și pe fluxuri condiționale de execuție; Operațiunile de geoprocesare să poată fi lansate individual dintr-o consolă de execuție sau în pachete de execuție, în mod programatic;
- Să dispună de mecanisme configurabile pentru planificarea/programarea geoprocesărilor și să permită integrarea cu librării de procesare (plugins, APIs, servicii web);
- Să permită înglobarea de scripturi prin limbaje de programare uzuale și să conțină librării de unelte software, librării și plugins pentru extinderea funcționalităților și programarea unro funcționalități specifice;
- Să ofere instrumente pentru publicarea sau partajarea de resurse pentru publicarea în Internet prin mecanisme standard WMS, WCS, WFS;
- Să permită exportul și printarea proiectelor GIS în materiale de tip Office petru raportări specifice;

- Produs și licență de tip server pentru partajarea și livrarea resurselor GIS către publicul larg, alte aplicații și sisteme informatice

Cerinte minimale:

- Să permită definirea de proiecte web de tip GIS pentru publicarea în Internet;
- Serviciile furnizate să fie conforme standardelor OGC, WFS, WCS, WMS;
- Să permită publicarea web a mai multor tipuri de resurse geospațiale: baze de date GIS, tabele, shapefiles, repartajarea altor servicii wen existente;
- Să permita controlul asupra straturilor grafice expuse în serverul web, pe stiluri de vizualizarea a informațiilor, graduri configurabile de transparență, graduri configurabile asupra proprietăților de zoom, etichetare, permisiuni asupra modalității de interacțiune cu obiectele geospațiale;
- Să înglobeze mecanisme pentru previzualizarea datelor ce urmează a fi expuse în Internet, gruparea resurselor geospațiale în grupuri de straturi grafice, partajarea acestora în grupe de pagini web distincte, accesibile pe link –uri și porturi distincte;
- Să conțină mecanisme pentru operațiuni configurabile de caching;
- Să contină instrumente pentru monitorizarea performanțelor sistemului, configurarea dimensiunilor resurselor geospațiale implicate și optimizarea în funcție de trafic și resursa solicitată de către utilizatorii externi (consumatorii web);
- Să înglobeze mecanisme de securitate pentru accesul controlabil al resursele geospațiale expuse către utilizatori autentificați sau neautentificați în sistem; Să permită definirea de grupuri de utilizatori, roluri și politici de acces, configurabile și integrabile (eg. LDAP);

- Produs și licență aplicație mobilă sau web pentru colectarea și consultarea din teren a datelor geospațiale

Cerinte minimale:

- Să permită rularea pe telefoane mobile tip smartphone (Android, iPhone) sau tablete;
- Să permită accesarea modulelor GPS ale dispozitivelor mobile de pe care sunt accesate și înglobarea acestor date în formularea și raportările necesare din teren;
- Să permită încărcarea de formulare pentru colectarea datelor din teren;

- Să permită transmiterea datelor în sistemul GIS, prin intermediul infrastructurii GIS a soluției ofertate;
- Să permită funcționarea în regim offline: încărcarea datelor în dispozitiv și tramsmiterea către server când există conexiune Internet;
- Să permită accesarea site –urilor și serviciilor web expuse prin intermediul serverului GIS, inclusiv a aplicatiilor specializate care implementează funcționalitățile solicitate.

3.9. *Servicii de dezvoltare si implementare proiect*

3.9.1. Serviciile de livrare si instalare echipamente HW

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-ul/urile puse la dispozitie de către Beneficiar;
- 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.

3.9.2. Serviciile de livrare si instalare software de baza

Pentru asigurarea livrarii cu succes a infrastructurii software ale sistemului, trebuie sa fie instalata 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.

3.9.3. 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;
  - Proiectarea componentelor şi arhitectura de sistem;
- Dezvoltarea softului de aplicație
  - Dezvoltarea componentelor de software;
  - Integrarea componentelor software;
  - Testarea soluţiei software;
  - Configurarea sistemului software;
  - Obţinerea acordului final din partea beneficiarului proiectului;

Se va realiza o aplicație deschisă și modulara pentru realizarea registrelor de sănătate și oferirea unui mediu de analiza care garantează o integritate ridicată a datelor, date demne de încredere și respectarea unor standarde riguroase de calitate.
Specialistii din cadrul MS trebuie să poată construi cu ușurință un registru accesibil pe mobil și pe web, cu capabilități puternice de colectare a datelor, flux de lucru, mesagerie și vizualizare pornind de la un template prestabilit si definit in cerintele functionale ale proiectului.
La realizarea unui registru Beneficiarul va trebui sa poata alege combinația unor instrumente moderne de tip web și mobil precum si cantitatea adecvată de informații specifice domeniului precum și integritatea și securitatea datelor garantate pentru a realiza obiectivele proiectului.
Caracteristicile fundamentale ale registrelor vor fi construite în jurul datelor sursă, modelelor flexibile de date si a API-urilor REST securizate.

3.9.4. 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, cerinţele reţelei de comunicaţii a 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 activități cu rezultatele lor respective:

- toate componentele software de bază şi hardware-ul 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, CD-uri de instalare și licențele legate de acest proiect au fost livrate;
- accesul la datele din REGINTERMED pentru utilizatorii din locaţiile fixe;
- 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 puțin 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 (aplicații, 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 producție.

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.
- 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 şi hardware-ul livrat, 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 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 performanța

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 Prestatorului**:

1. Expert cheie 1 - Manager de Proiect
- Studii superioare finalizate cu diploma de licenţă;
- Experienţa generală: minim 5 ani experienţă generală;
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect/contract la nivelul căruia să fi deţinut poziţia de manager/ coordonator;
- Deţinerea de cunoştinţe în domeniul managementului de proiecte dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel naţional/ internaţional.

2. Expert cheie 2 - Expert Analist de business
- Studii superioare finalizate cu diploma de licenţă sau echivalent în domeniul ingineria sistemelor, domeniul calculatoare şi tehnologia informaţiei, domeniul informatică, domeniul inginerie electronică, telecomunicaţii şi tehnologii informaţionale, domeniul cibernetică, statistică şi informatică economică;
- Experienţă generală: minim 5 ani experienţă generală in domeniul studiilor;
- 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 (CBAP sau echivalent);
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect, pe o poziţie similară, la nivelul căruia să fi desfăşurat activităţi de (re)inginerie a serviciilor;

3. Expert cheie 3 - Expert Tehnic Securitate Cibernetică
- Studii superioare finalizate cu licenţa sau echivalent in domeniul ingineria sistemelor, calculatoare si tehnologia informaţiei, informatica, inginerie electronica, telecomunicaţii si tehnologii informaţionale, domeniul cibernetica, statistica si informatica economica;
- Experienţa generala minim 5 ani in domeniul studiilor;
- 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 cunoştinţe dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel national/international pentru cel putin doua din solutiile oferite in cadrul prezentei proceduri de achizitie
- Deţinerea de cunoştinţe dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel national/international: Managementul securităţii informatice (certificare CISM/ CISSP/ GSEC sau echivalent)

4. Expert cheie 4 - Expert Arhitect de sistem
- Studii superioare finalizate prin diplomă de licenţă sau echivalenta în domeniul ingineria sistemelor, domeniul calculatoare şi tehnologia informaţiei, domeniul informatică, domeniul inginerie electronică, telecomunicaţii şi tehnologii informaţionale, domeniul cibernetică, statistică şi informatică

economică;
- Experienţă generală: minim 5 ani experienţă generală în domeniul studiilor;
- Experienţă specifică demonstrată prin participarea în cel puţin un proiect/contract, pe o poziţie similară la nivelul căruia sa fi desfăşurat activităţi similare cu responsabilităţile din acest contract;
- Deţinerea de cunoştinţe în domeniul arhitecturii de sistem dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel naţional/ internaţional (TOGAF sau echivalent).

5. Expert cheie 5 - Expert hardware și rețele

Expert în derularea activităților de instalare și configurare echipamente hardware și rețelistică, cu cel puțin 5 (cinci) ani experiență în domeniul instalării si/sau configurării de echipamente hardware și cu o experiență relevantă dovedită prin implicarea, pe o poziție similară, în cadrul a cel puțin un proiect în care să fi fost instalate și configurate echipamente hardware și de rețea asemănătoare cu cele ofertate.

6. Expert cheie 6 - Expert software

Expert în implementarea de soluții software, sisteme și aplicații, cu cel puțin 5 (cinci) ani experiență în domeniul dezvoltării de soluții IT și cu o experiență relevantă dovedită prin implicarea, pe o poziție similară, în cadrul a cel puțin un proiect în care să fi fost implementată o soluție utilizând produsele software ofertate.

7. Expert non-cheie 1 – Expert testare

Expert în derularea activităților de testare, cu cel puțin 5 (cinci) ani experiență în domeniul dezvoltării de soluții IT și cu o experiență relevantă dovedită prin implicarea, pe o poziție similară, în cadrul a cel puțin un proiect în care să fi fost dezvoltate componente/module pe bază de software de bază.

8. Expert non-cheie 2 – Expert instruire

Expert în derularea activităților de instruire, cu cel puțin 5 (cinci) ani experiență în domeniul dezvoltării de soluții IT și cu o experiență relevantă dovedită prin implicarea, pe o poziție similară, în cadrul a cel puțin un proiect în care să fi fost efectuate și activități de instruire de tipul „classroom” a utilizatorilor finali.

9. Expert non-cheie 3 – Expert soluții virtualizare și automatizare software

Expert în implementarea de soluții de virtualizare și automatizare software, cu cel puțin 5 (cinci) ani experiență în domeniul dezvoltării de soluții IT și cu o experiență relevantă dovedită prin implicarea, pe o poziție similară, în cadrul a cel puțin un proiect în care să fi fost implementată o soluție de virtualizare și automatizare software utilizând produsul software ofertat.

10. Expert non-cheie 4 – Expert în testarea securității

Expert în testarea securității, având cunoștințe în ceea ce privește managementul securității sistemelor informatice și cel al riscului în stabilirea arhitecturii de securitate, în asigurarea securității dezvoltării software și a securității rețelelor de comunicații, probate prin certificare/diplomă, precum și cunoștințe în ceea ce privește realizarea testelor de penetrare, elaborarea rapoartelor privind penetrarea rețelelor, a aplicațiilor web, a firewall-urilor, a codului sursă, a sistemelor de mesagerie electronică și în identificarea amenințărilor în vederea descoperirii și administrării vulnerabilităților din cadrul infrastructurilor informatice, probate prin certificare/diplomă (minim 3 certificări, conform standard de securitate al CTE).

4.1.2. Instruire utilizatori

Categorii de utilizatori care trebuie instruiti:

- **Furnizor de servicii detinatori de registre**

Instruirea utilizatori – dedicată deținătorilor de registre, **este estimata la 300 de persoane** la nivel national. Având în vedere distribuția geografică, bugetul a fost estimat în baza următoarelor premise:

- Se vor organiza 10 sesiuni de instruire, cu durata de 3 zile/sesiune, 8 ore/zi, pentru circa 20 persoane/sesiune, în centrele universitare din țară
- Se vor organiza 5 sesiuni de instruire, cu durata de 3 zile/sesiune, 8 ore/zi, pentru circa 20 persoane/sesiune, în București

Sistemul va permite definirea rolurilor pentru fiecare funcție importantă pentru fiecare categorie de utilizatori.

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

- cunoaşterea sistemului integrat în ansamblul său
- învăţarea modului de operare a funcţionalităţilor sistemului propus
- învăţarea modului de rezolvare a problemelor curente de folosire a componentelor sistemului
- înţelegerea implicaţiilor sistemului propus şi a avantajelor acestuia.

Sesiunile de instruire vor fi realizate de furnizorul soluţiei informatice. De asemenea, furnizorul soluţiei informatice va elabora şi pune la dispoziţia beneficiarului manuale de utilizare şi suport de curs în limba română, pentru toate categoriile de utilizatori ai sistemului.
La terminarea cursului, cursanţii din categoriile administrator de sistem şi personal MS vor primi de la furnizor certificate de instruire individuale. Certificarea se va face diferenţiat pentru cele două categorii.

Celelalte categorii de utilizatori vor beneficia doar de materiale de prezentare şi de instruire individuală (*self-trainig*), astfel:

- furnizorii de servicii medicale vor avea la dispoziţie materiale complete de instruire electronică pentru operarea funcţionalităţilor puse la dispoziţie de sistemul propus, care complementează funcţionalităţile aplicaţiilor de raportare utilizate în mod curent;

Furnizorul soluţiei va face instruirea utilizatorilor sistemului prin livrarea de documentaţie şi organizarea de cursuri de instruire la nivelul MS.
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.
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.

Soluție software de knowledge management

Această soluție trebuie să permită următoarele:

- Definirea drepturilor de acces diferențiate; 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, LMS, 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. *GRAFICUL DE IMPLEMENTARE*

Nr. crt.	Activitati \ Luna de proiect	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
3	**Implementare sistem informatic**																																				
3.1	Analiza necesitatilor																																				
3.2	Proiectarea solutiei informatice																																				
3.3	Servicii de livrare, instalare si punere in functiune echipamente HW si infrastructura software																																				
3.4	Dezvoltarea, configurarea si instalarea aplicatiei informatice si scanarea documentelor																																				
3.5	Testarea aplicatiei și operaționalizarea sistemului IT																																				
4	**Instruire utilizatori**																																				

5. GARANȚIA SISTEMULUI

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 1 an, începând cu data livrării sistemului informatic final.
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.

Pe durata de derulare a garanţiei, pentru echipamentele care constituie mediile de productie, se vor presta servicii de garantie in conditiile de mai jos:

- În cazul apariţiei unei defecţiuni, timpul de răspuns garantat va fi de maxim 1 oră, iar intervenţia se va asigura într-un interval de maxim 24 ore de la ora raportării de către beneficiar a defectului până la începerea remedierii
- Defecţiunile vor fi remediate pe loc, iar funcţionalitatea echipamentelor (servere si storage) va fi restabilită în maxim 24 ore de la ora raportării.
- Pentru defecţiuni majore ale echipamentelor care necesită o durată de depanare mai îndelungată de 24 ore, se va asigura imediat un echipament echivalent pentru desfăşurarea în continuare a activităţii. Echipamentul înlocuit ca urmare a defecţiunii majore va fi reparat

în maximum 48 de ore. Dacă acesta nu poate fi reparat, va fi înlocuit permanent cu un echipament cu caracteristici tehnice similare sau superioare.
- Garanţia echipamentelor înlocuite sau reparate se extinde cu perioada scursă de la data înştiinţării Furnizorului şi până la data când produsele au revenit, în stare de bună funcţionare, în posesia Beneficiarului.
- Subansamblele/componentele/echipamentele pe care se stochează date/informaţii ale Beneficiarului şi care necesită înlocuire/reparare pe perioada de derulare a garanţiei rămân în proprietatea acestuia (fără a părăsi locaţia de instalare aparţinând Beneficiarului) chiar dacă acestea s-au defectat şi au fost înlocuite conform garanţiei.

In perioada de garanţie pentru componentele soluţiei propuse se vor presta urmatoarele servicii de garantie:
- Reparatii/inlocuiri ale componentelor defecte la locatia de instalare a beneficiarului.
- Consiliere si suport telefonic 24 de ore pe zi, 7 zile pe săptămână prin serviciu Help-desk atat pentru produsele hardware cat si software.
- Remediere software de la distanta cu acordul beneficiarului.
- Actualizari software la locatia de instalare a beneficiarului sau de la distanta.
- Reconfigurari hardware si software la nivelul initial solicitat in cazul in care erorile aparute nu sunt datorate beneficiarului.
- Mentenanta preventiva periodica.
- Consiliere si suport tehnic pentru posibilitati de extindere a solutiei existente.

Pentru garantarea efectuarii acestor servicii in conformitate cu normele emise de catre producator se solicita certificari si autorizari necesare pentru a demonsta capabilitatile tehnice ale echipei de suport tehnic privind instalarea, configurarea, testarea si prestarea serviciilor de garantie ofertate.

Pe timpul derulării garanţiei, se vor presta următoarele intervenţii:
- În condiţiile apariţiei unei defecţiuni ale produselor hardware sau software instalate şi configurate, se vor asigura verificări tehnico-metologice pentru a determina dacă problemele apărute sunt de natură hardware sau software.
- Periodic (cel putin o dată la 6 luni), se vor asigura servicii verificare preventivă care constau în verificarea periodică a funcţionării produselor ofertate, cu scopul de a preveni căderile şi defecţiunile şi/sau degradarea funcţionalităţilor sau a disponibilităţii acestora. Aceste activităţi au ca scop verificarea stării componentelor aflate în funcţiune prin intermediul unor funcţionalităţi de audit. Fiecare verificare se va finaliza cu elaborarea unui raport conţinând rezultatele verificării şi acţiunile recomandate pentru a asigura buna funcţionare a produselor sau pentru a îmbunătăţi disponibilitatea acesteia.
- În condiţiile apariţiei unei erori în funcţionarea produselor hardware sau software instalate şi configurate, se vor asigura verificări pentru a determina natura problemelor apărute şi va decide care este cel mai potrivit mod de intervenţie pentru soluţionarea defecţiunii. Modalităţile de intervenţie sunt: help-desk online, procesare telefonică, transmiterea actualizărilor de software şi asigurarea asistenţei pentru instalarea acestuia si realizarea remedierii la locaţia beneficiarului.
- Actualizările de software se referă la compilarea pe un suport magnetic sau la descărcarea unor patch-uri care conţin corecţii ale unor erori sau îmbunătăţirea software-ului cu scopul

de a creşte uşurinţa în exploatare sau performanţele acestuia. Actualizările vor fi însoţite de actualizări ale manualelor destinate utilizatorilor.

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.

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

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

Autoritatea Contractantă este responsabilă pentru:
a. punerea la dispoziția Contractantului a tuturor informațiilor disponibile pentru obținerea rezultatelor așteptate, cum ar fi: date de intrare, raportări, situații specifice;
b. punerea la dispoziția Contractantului, dacă este cazul, a unui spațiu de lucru mobilat;
c. desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit Contractantului;
d. asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului.

Atribuțiile și responsabilitățile **MINISTERUL SANATATII**:
- Implementarea soluției informatice:
  - Analiza necesităților;
  - Proiectarea soluției informatice;
  - Servicii de livrare, instalare și punere în funcțiune echipamente HW și licențe software;
  - Dezvoltarea aplicației informatice;
  - Testarea aplicației;
  - Pilotare la nivel național;
- Instruirea echipei de proiect.

Prestatorul

Prestatorul serviciilor este responsabil pentru executia conforma si la timp a tuturor activitatilor si pentru furnizarea livrabilelor prevazute in prezentul Caiet de sarcini, corespunzatoare Proiectului.
Prestatorul va raspunde intocmai tuturor cerintelor prevazute in prezentul Caiet de sarcini, respectand si aplicand cele mai bune practici in domeniu.
Prestatorul 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 și 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 PRESTATOR*

Prestatorul 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, **Prestatorul** 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 Prestatorului.

Echipamente

Prestatorul 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

Prestatorul 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

Prestatorul 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, Prestatorul 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 Prestatorului 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, Prestatorul 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 Prestator.
- **Foarte nesatisfăcător (1 punct)** – Livrabilele prezintă neconformități / inexactități majore față de nivelul agreat iar aceste aspecte nu au putut fi corectate de către Prestator. 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 Prestator (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, MINISTERUL SANATATII (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, Prestatorul va preda Autorității Contractante codul sursă al aplicației informatice dezvoltate, documentația aferentă si kit-urile de instalare.

7.6. *ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI*

7.6.1. Propunerea tehnica

Ofertantul va descrie în detaliu modul de îndeplinire a cerințelor de realizare a activităților.
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 și 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 și 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 evidențiate ca activități 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 obligația să respecte toate cerințele prezentate în caietul de sarcini și să dezvolte într-o manieră proprie și originală punctele prezentate. Neregăsirea cerințelor minime prezentate în caietul de sarcini va presupune declararea ofertei ca fiind neconformă.

Propunerea tehnică va fi astfel prezentată încât să asigure posibilitatea verificării conformității acesteia cu cerințele minime obligatorii prevăzute în caietul de sarcini. Propunerea tehnică trebuie să reflecte modul în care Ofertantul înțelege să îndeplinească în integralitatea lor, cerințele prevăzute în Caietul de sarcini.

7.6.2. Propunerea financiară

Propunerea financiară va fi prezentată în lei, atât în sumă globală, cu evidențierea separată a TVA, cat si pe fiecare activitate/subactivitate, cu evidențierea unităților de măsură și a valorilor unitare, conform anexei la formularul de ofertă financiară, ce se regăsește și mai jos:

Nr. crt.	Livrabile Sistem informatic (inclusiv instruire)	Preț unitar fără TVA (lei)	Valoare totală fără TVA (lei)	Valoare TVA (lei)	Valoare totală maximă cu TVA (lei)
1	**HARDWARE, CU LICENTELE AFERENTE** (inclusiv cheltuieli de instalare, configurare, punere în functiune)				
2	**SERVICII DE DEZVOLTARE A APLICATIILOR SOFTWARE** (personalizarea aplicaţiilor software / licenţelor necesare implementării proiectului, configurarea şi implementarea bazelor de date, migrarea şi integrarea diverselor structuri sau volume de date existente, achiziţionarea şi implementarea				

	de soluţii de semnătură electronică, back-up şi recovery)				
3	**SERV. DE INSTRUIRE** (pregătirea personalului care va utiliza echipamentele achiziționate prin proiect şi aplicaţia / serviciul software achiziționat şi/sau dezvoltat prin proiect)				
TOTAL OFERTA FINANCIARA					

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

7.7. *MODALITATEA DE PLATĂ ȘI TERMENE*

Autoritatea Contractantă va efectua plăți către Prestator, în baza facturilor emise de către acesta din urmă și în baza proceselor verbale de recepție semnate de comisia de recepție din partea Beneficiarului conform graficului de plăți agreat de părți.

Platile se vor efectua pentru realizarea și finalizarea sub-activităților (conform Gantt al proiectului si livrabilelor):
- Analiza necesităților;
- Proiectarea soluției informatice;
- Amenajare centru de date ;
- Servicii de livrare, instalare și punere în funcțiune echipamente HW și licențe software;
- Dezvoltarea aplicației informatice;
- Testarea aplicației;
- Pilotare la nivel national;
- Instruirea echipei de proiect.

Modalitatea de plată și termenele sunt prevăzute în Contract, anexa la prezenta documentație de atribuire.

Documentele tip, necesare pentru efectuarea plății din cadrul contractului de către Prestator, sunt prezentate mai jos:
1. Aviz de însoțire a mărfii (dacă este cazul);
2. Certificate de garanție și declarație conformitate (dacă este cazul);
3. Set de proceduri și mecanisme pentru coordonare și consultare factori interesați;
4. Manuale de utilizare a aplicației;
5. Suport de curs, în format electronic;
6. Liste de prezență;
7. Chestionare evaluare instruire;
8. Certificate de participare;
9. Raport al activității;
10. Proces verbal de recepție calitativ si cantitativ al produselor/serviciilor cat și a raportului aferent activitatii;
11. Factura fiscală.

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

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. Riscuri

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 activităților 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 și coordonare între membrii echipei de proiect	-stabilirea și monitorizarea respectării unui circuit de 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 influențeze realizarea investiției.

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

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

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

Ofertantul va introduce în propunerea tehnică:

a. descrierea ipotezelor pe care Ofertantul trebuie să le aibă în vedere în pregătirea Ofertei și 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 și 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 și dacă Contractantul poate contribui la diminuarea efectelor riscurilor.

7.8.2. Ipoteze

Ipoteze avute în vedere sunt:

a. conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
b. corelația dintre resursele necesare și rezultatele așteptate este realistă;
c. începerea serviciilor se va realiza în perioada preconizată;

d. nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
e. toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Contractantului;
f. Contractantul va semna un acord de confidențialitate la momentul semnării Contractului și va respecta toate instrucțiunile privind utilizarea informațiilor confidențiale.

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