Aprobat,
……
.....

CAIET DE SARCINI

pentru
SERVICII DE DEZVOLTARE ȘI IMPLEMENTARE SISTEM INFORMATIC INTEGRAT PENTRU EVIDENTA CLINICA A SECTIILOR A.T.I. (S.I.E.C.-A.T.I.)

în cadrul proiectului
Sistem Informatic pentru Evidenta Clinica a sectiilor A.T.I. (S.I.E.C.-A.T.I.)

1. INFORMAȚII GENERALE. OBIECTIVELE PROIECTULUI

1.1.INFORMAȚII GENERALE

Autoritatea Contractantă este **MINISTERUL SANATATII** (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 confidenţial se aplică doar asupra datelor/informaţiilor indicate şi dovedite ca fiind date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală.

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

1.2.OBIECTIV GENERAL

Creșterea utilizării TIC în comunicarea directă între Ministerul Sănătății (MS) și cele mai importante 18 spitale de adulți și pediatrie din România (spitale de urgență și centre regionale) prin implementarea unui sistem informatic modern de monitorizare, documentare, schimb de date medicale în situații de urgență, consultarea și/sau acordarea celui de-al doilea aviz de la distanță și suport al proceselor aferente activităților de anestezie și terapie intensivă (ATI), sistem informatic ce va functiona ca suport pentru luarea deciziilor în situațiile de urgență intr-o unitate centrala din cadrul Ministerului Sanatatii.

1.3.OBIECTIVE SPECIFICE

Obiectivele specifice ale proiectului sunt:

- Dezvoltarea si implementarea unui sistem informatic (interoperabil cu sistemele informatice existente în cadrul celor 18 spitale, sisteme necesare îndeplinirii obiectivului general al acestui proiect care va sprijini decidentii (prin reprezentantii imputerniciti) in cadrul unui centru operativ din cadrul Ministerul Sănătății privind distribuirea marilor urgențe medico-chirurgicale (urgențe chirurgicale cardiace, vasculare, neurochirurgicale etc.) și controlul direcționării corecte, pe criterii bine stabilite a acestor pacienți către sălile de operație și secțiile ATI ale marilor spitale de urgență. Sistemele/aplicatiile informatice existente/viitoare ale Ministerului Sanatatii se vor putea interconecta cu sistemul implementat prin acest proiect.
- Creșterea calității îngrijirilor medicale și facilitarea accesului cetățenilor la servicii medicale de calitate prin implementarea unui Sistem Informatic Electronic Clinic pentru Anestezie și Terapie Intensivă (SIEC) unitar pentru cele mai importante 18 spitale de adulți și pediatrie din România (spitale de urgență și centre regionale). Sistemul va permite monitorizarea continuă, completă, precisă și trasabilă (inclusiv din punct de vedere medico-legal şi al arhivării informațiilor) a parametrilor vitali ai pacienților îngrijiți în secțiile de anestezie-terapie intensivă (ATI), a procedurilor executate si a medicației administrate în aceste secții precum şi a stării bolnavilor îngrijiți în aceste secții, având drept efecte: reducerea semnificativă a numărului de erori, creșterea productivității actului medical și a eficienței personalului medical prin reducerea încărcării cu operații administrative şi birocratice.

1.4.ENTITĂȚI IMPLICATE

Din punct de vedere al actorilor care vor participa in fluxul de oferire al serviciilor electronice prin SIEC-ATI, vor exista următoarele categorii importante de entități conectate:

- Ministerul Sănătății, unitățile din subordine (HUB-MS, SABIF, SAJ, etc) și structurile cu care există coordonare (DSU);
- Spitalele care vor subscrie proiectului;
- Alți furnizorii de servicii medicale, autorizați de către Ministerul Sănătății, care sesizează cazuri de transfer cu nevoia de ocupare pat ATI. Aceasta categorie va fi identificată în urma activității de analiza desfasurata in implementarea sietemului informatic si va fi detaliată într-un document aferent acestei activități. Echipamentele hardware si aplicațiile software necesare pentru ca aceste entitati să fie parte a proiectului vor fi suportate din surse independente de implementarea acestui proiect.

Centrul Operativ pentru Situații de Urgență (HUB-MS)
Un partener, indirect, în cadrul proiectului dar cu o importanță în gestionarea eficientă a situațiilor deosebite care pot să apară în eventualitatea unui eveniment care se încadrează într-o situație de cod roșu este HUB-MS.

Serviciul de Ambulanță Județean (SAJ)
Serviciu de ambulanță județean, respectiv al municipiului București sunt unități sanitare publice de importanță strategică, cu personalitate juridică, aflate în coordonarea departamentului de specialitate din Ministerul Sănătății și a Autorităților de sănătate publică județene, respectiv a municipiului București, având în structura lor un compartiment pentru asistență medicală de urgență și transport medical asistat, cu echipaje medicale de urgență, cu sau fără medic, și un compartiment pentru consultații medicale de urgență la domiciliu și transport sanitar neasistat.

Departamentul pentru Situații de Urgență din cadrul Ministerului Afacerilor Interne (DSU)
DSU este structura operațională fără personalitate juridică a MAI, cu atribuții de coordonare, cu caracter permanent, la nivel național, a activităților de prevenire și gestionare a situațiilor de urgența, asigurarea și coordonarea resurselor umane, materiale, financiare și de altă natură necesare restabilirii stării de normalitate, inclusiv primul ajutor calificat şi asistența medicală de urgență în cadrul unităţilor şi compartimentelor de primire a urgenţelor (UPU/CPU).

DSU coordonează operațional serviciile de ambulanță județene, respectiv al municipiului București, UPU/CPU, precum și serviciile publice Salvamont.

1.5.CADRUL LEGAL

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

Nr. crt.	Document
1	Strategia Europa 2020, o strategie pentru creştere inteligentă, ecologică şi favorabilă incluziunii, Cadrul Strategic Comun 2014-2020
2	Strategia europeana privind Piaţa Unică Digitală
3	Strategia Naţională privind Agenda Digitală pentru România (SNADR) 2020
4	Strategia de Securitate Cibernetica a Romaniei
5	Planul National de Reforma
6	POC 2014-2020
7	Legea nr. 455/2001 privind semnătura electronică
8	Hotărârea Guvernului nr. 1259/2001 pentru aprobarea Normei tehnice şi metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, actualizată
9	Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice
10	Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare
11	Legea nr. 98/2016 privind achiziţiile publice
12	HG nr. 395/2016 pentru aprobarea Normelor Metodologice de aplicare a prevederilor referitoare la atribuirea Contractului de achiziţie publică /acordului-cadru din Legea nr. 98/2016 privind achiziţiile publice
13	Ordonanţa de urgenţă nr. 38/2020 privind utilizarea înscrisurilor în formă electronică la nivelul autorităţilor şi instituţiilor publice
14	Hotărârea Guvernului nr. 285/2020 pentru modificarea şi completarea Hotărârii Guvernului nr. 1.235/2010 privind aprobarea realizării Sistemului naţional electronic de plată online a taxelor şi impozitelor utilizând cardul bancar

1.6.VALOAREA ŞI DURATA CONTRACTULUI

Valoarea contractului

Valoarea totală a achiziției este de **105.426.470,35** lei fără TVA, respectiv **125.457.499,72** lei cu TVA.

Durata de implementare a contractului

Durata de implementare a contractului este de **18 luni de la semnarea contractului**.
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

Pentru implementarea optima a sistemului informatic, se va realiza un sistem capabil sa asigure interoperabilitatea intre secțiile de Terapie Intensivă și Săli Operație (SO) ale spitalelor din lista locatiilor de implementare si Ministerul Sanatatii care va gazdui HUB-ul central unde se vor agrega datele din spitale, se va putea vizualiza situatia generala a paturilor libere si se va initia procesul de rezervare a paturilor libere din sectiile ATI in situatii de urgenta.

Ministerul Sanatatii, in calitate de lider de proiect si de ordonator principal de credite va contracta si gestiona sistemul informatic, cu toate componentele sale de la nivel central si cele din spitalele participante in cadrul proiectului.

Totodata, soluţia informatica trebuie să asigure informatizarea a două categorii de structuri din cadrul spitalelor participante la proiect:
- Sectiile ATI + Salile de Operatie din lista de spitale mentionate in proiect – in numar de 18
  - componenta cu paturi din secţiile de ATI cuprinse în proiect (în total 649 de posturi-paturi informatizate și monitorizate)
  - partea de anestezie-terapie intensivă aferentă sălilor de operaţii (posturi de anestezie, în număr de 275)
- Componenta centrala – Ministerul Sanatatii

Sistemul informatic va trebui să respecte prevederile legislative în vigoare aplicabile în domeniul sanatatii, sa asigure un schimb de informații ușor de gestionat și să ofere un grad înalt de accesibilitate.

Asigurarea unui schimb consistent de informații și date din sfera sanatatii si al gestionarii situatiilor de urgenta se poate realiza doar în condițiile abordării celor trei aspecte ale interoperabilitatii:
- La nivel organizațional: dotarea sectiilor ATI cu solutii informatice de ultima generatie care vor fi integrate cu solutiile informatice existente ale spitalelor (HIS's – Hospital Information Systems, etc.), cat si prin centralizarea la Ministerul Sanatatii a anumitor seturi de date si informatii relevante pentru obiectivele stabilite prin acest proiect colectate din spitale, imbunatatind timpii de reactie in situatii de urgenta.
- La nivel semantic: codificări, nomenclatoare, vocabulare contextuale (ex: registrii de baza) comune si standardul HL7.
- La nivel tehnic: interoperabilitate sintactica, standarde de comunicații intre sisteme si rețele (nivel OSI); la nivel tehnic sistemul va trebui sa asigure o arhitectura modulara, cu componente reutilizabile si funcționalități bine definite, cu conectori pe standarde deschise, conform EIF/CNI[1], fiind compatibilă cu infrastructura fizica IT care respectă criteriile de specificații non-proprietare si cu standardele existente, putând fi adăugate in orice moment componente noi, cu proprietăți noi, daca este necesar.

Interoperabilitatea intre Spitale si HUB

Ahitectura sistemului informatic va respecta următoarele cerințe:
- Unificarea procedurilor medicale și a managementului datelor in cadrul sectiilor ATI și SO conform celor mai bune practici ale domeniului;
- Implementarea unui model de securitate „by design";
- Sistemul informatic propune implementarea unor soluții software mature, cu drept de proprietate/licentiere perpetuu;
- Utilizarea unei arhitecturi modulare in care responsabilitățile fiecărei componente sunt specializate; structura modulara permite adăugarea de noi componente cu proprietăți diferite fără modificări in componentele software finalizate;
- Schimbul de date cu alte sisteme se va realiza utilizand standardul HL7, alte standarde deschise (XML sau JSON, etc.).

Sistemul propus va permite exportul si importul informațiilor in diverse formate web

Infrastructura hardware:
trebuie sa includă toate componentele necesare care sa satisfacă cerințele de performanta. Aceasta infrastructura trebuie sa conțină cel puțin:

- Servere;
- Statii de lucru aferente paturilor ATI si SO;
- Terminale specifice digitizarii semnalului medical (terminal servers);
- Sistem de stocare - storage (SAN);
- Sistem de asigurare continua a energiei electrice (UPS-uri);
- Rack-uri;
- Sisteme de securizare a traficului de date – firewall;
- Infrastructura de rețea necesara intre componentele ce compun sistemul propriu-zis.

Sistemul informatic:

- Sistemele si echipamentele livrate trebuie sa fie noi, neutilizate si de ultima generație. Ele trebuie sa asigure gradul necesar de performanta, fiabilitate si flexibilitate
- Procesoarele serverelor livrate trebuie sa apartina clasei Server conform clasificarii producatorului
- Furnizorul va trebui sa prezinte specificațiile tehnice privind organizarea si dotarea camerelor pentru servere in care se vor instala echipamentele astfel încât sa fie asigurate condițiile operaționale minime necesare pentru funcționarea acestora; spatiile vor fi puse la dispozitia implementarii proiectului de catre fiecare spital in parte si de catre Ministerul Sanatatii inainte de inceperea lucrarilor.
- Furnizorul va trebui sa precizeze care este puterea totala consumata de echipamentele livrate precum si caracteristicile de climatizare/ventilație necesare, pentru a le avea in vedere Beneficiarul la amenajare
- Furnizorul va avea în vedere că toate cerințele si caracteristicile hardware sunt minime si obligatorii

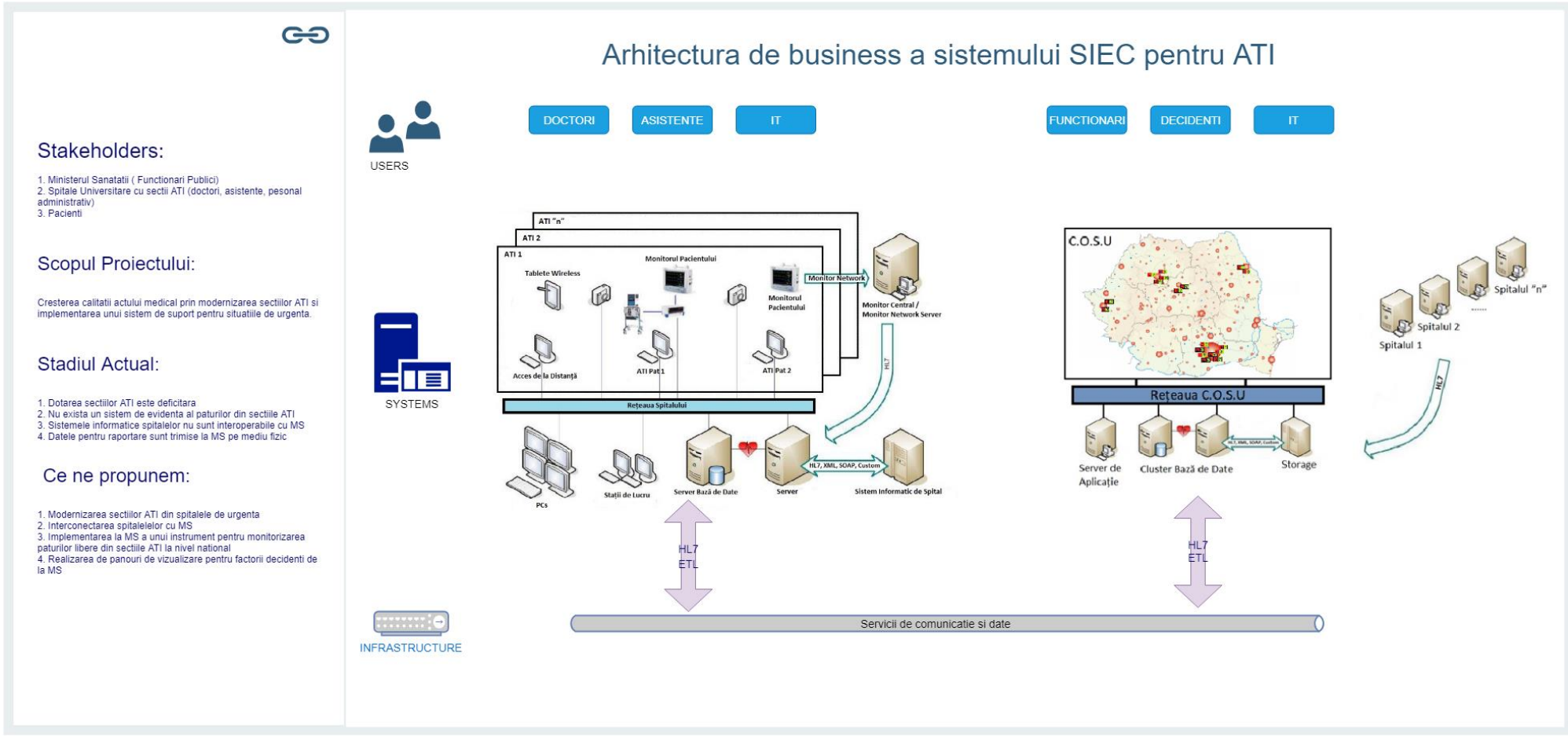


Fig. 1 . - Arhitectura de Business a sistemului SIEC - ATI

Toate aceste cerințe vor fi dezvoltate la nivel de detaliu in cadrul documentației de atribuire/caietul de sarcini. In același timp cerințele nu sunt limitative, furnizorul putand oferta conform soluției pe care o are in vedere in conditiile asigurarii superioritatii fata de specificatiile minime din caietul de sarcini. Este așadar necesar ca Furnizorul să propună soluții complete si integrate, care să îndeplinească în totalitate cerințele beneficiarului.

Față de cerințele tehnice si funcționale ale sistemului informatic, furnizorii au obligativitatea de a include in propunerea tehnica si comerciala orice alte componente hardware, software si de servicii pe care le considera necesare pentru asigurarea funcționalității sistemului si cu justificarea tehnica a solutiei adoptate, chiar daca acestea nu au fost solicitate sau explicitate in proiectul tehnic.

Sunt avute in vedere doua modalitati de comunicare si transport de date intre componentele software locale si componenta software centrala:

- Comunicare in timp real prin servicii web intre spitale si HUB-ul central pentru popularea Componentei Dashboard Disponibilitate paturi ATI

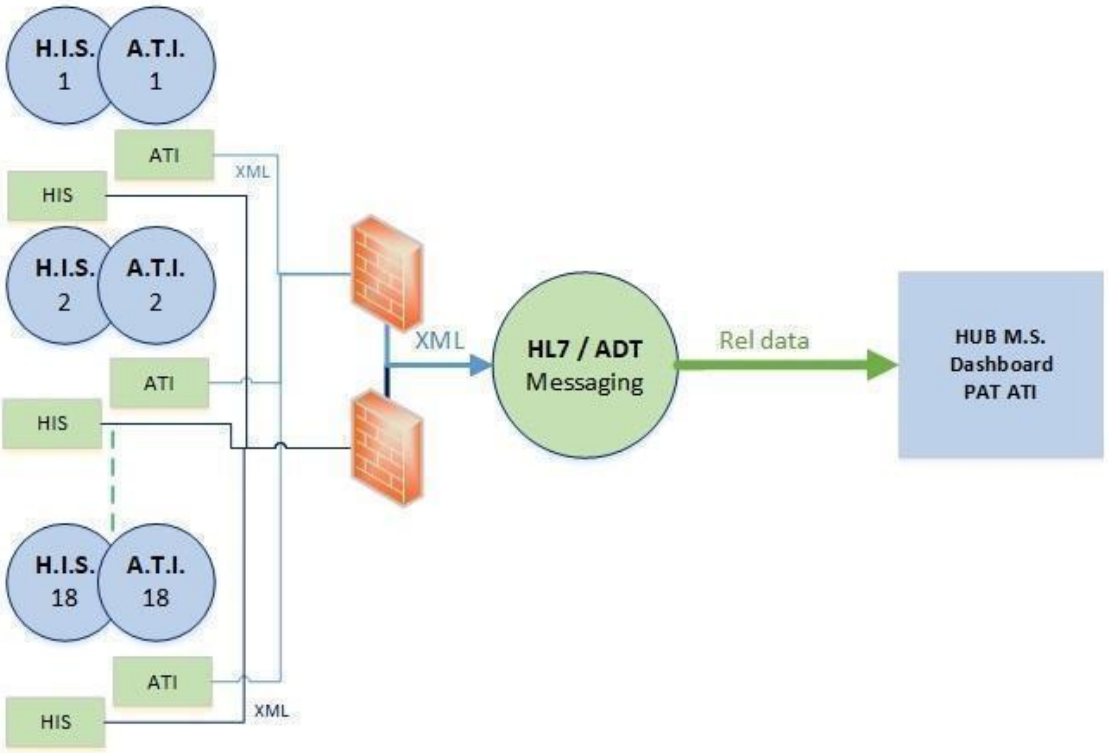


Fig: Fig. 2. - Diagrama transport de date in timp real

- Comunicare asincrona pentru raportare si date statistice

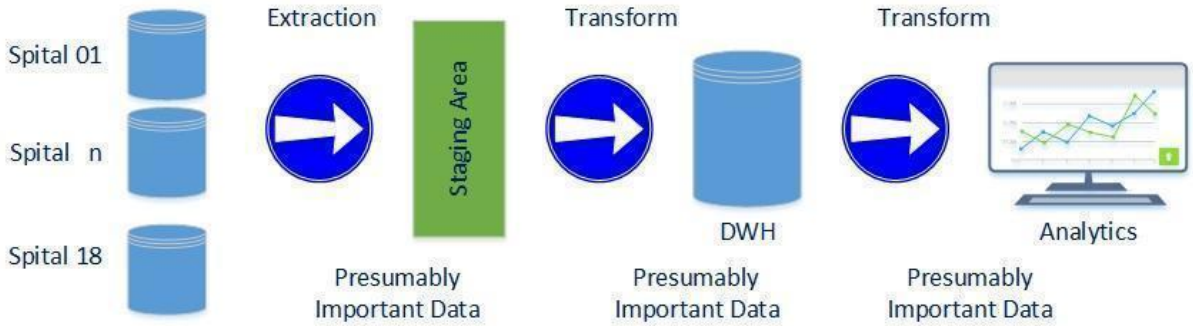


Fig.3. - Diagrama pentru raportare si date statistice

Ministerul Sănătății în calitate de Autoritate Contractantă va achiziționa un sistem integrat cu următoarele componente functionale principale:

(a) Componenta informatică pentru secțiile de Terapie Intensivă și Bloc Operator / Săli Operație (SO) la nivelul fiecărui spital partener în proiect (din lista de mai jos)
(b) Componenta HUB MS:

- Componenta Dashboard Disponibilitate paturi ATI, integrată cu aplicațiile ATI din spitalele de implementare din cele 5 regiuni/orașe – lista de mai jos. Aplicația va permite vizualizarea în timp real a situației din cele 18 spitale și va permite initierea procesului de rezervare a paturilor ATI
- Componenta Business Intelligence – BI de raportare la nivelul Ministerului Sănătății pentru analiza datelor din sistem la nivel istoric: zilnic, săptămânal, lunar, anual sau ad-hoc ca suport în luarea deciziilor

Locațiile de implementare a proiectului sunt:

Nr.	Denumire entitate
0	HUB Min. Sanatatii / HUB-MS
București	
1	Spitalul de Urgenta "Bagdasar Arseni" București
2	Spitalul de Urgenta "Sf. Ioan" București
3	Spitalul de Urgenta "Sf. Pantelimon" București
4	Spitalul Clinic de Urgenta București
5	Spitalul Universitar de Urgenta București
6	Spitalul de Chirurgie Plastică Reparatorie și Arsuri București
7	Spitalul de Urgente Pediatrice "M.S. Curie" București
8	Spitalul de Urgenta pentru Copii "G. Alecsandrescu" București
Cluj-Napoca	
9	Institutul Inimii de Urgență pentru Boli Cardiovasculare "Nicolae Stăncioiu" Cluj-Napoca
10	Institutul Oncologic "Prof. Dr. I. Chiricuța" Cluj-Napoca
11	Institutul Regional de Hepatologie si Gastroenterologie " O. Fodor" Cluj-Napoca
12	Spitalul Clinic Județean de Urgenta Cluj-Napoca
Iași	
13	Institutul Regional de Oncologie Iași
14	Spitalul Județean de Urgenta "Sf. Spiridon" Iași
Târgu Mureș	
15	Institutul de Urgență pentru Boli Cardiovasculare și Transplant Târgu Mureș
16	Spitalul Județean de Urgentă Târgu Mureș
Timișoara	
17	Institutul de Boli Cardiovasculare Timișoara
18	Spitalul Clinic Județean de Urgenta Timișoara

Mai jos, enumeram elemente de vocabular si acronime specifice proiectului

- BPM Business Process Model;
- HL7 Health Level Seven;
- HL7 RIM Reference Information Model;
- HL7 CTS Common Terminology Service;
- HL7 FHIR Fast Healthcare Interoperability Resource;
- ETL Extract, Transform, Load Service;
- DW Data Warehouse;
- DM Data Mart;

- WS W3C Web Services;
- SOAP Simple Object Access Protocol.

Număr beneficiari servicii (estimat vs. capacitate)

Beneficiile proiectului sunt trei categorii mari de beneficiari direcți ai proiectului:

(a) 20 angajați ai Ministerului Sănătății care vor beneficia de un instrument de suport documentat (având posibilitatea urmăririi actelor medicale efectuate, pe baza unor date precum morbiditate, mortalitate, gravitate inițială) in luarea deciziilor in privința alocării de resurse financiare către spitalele cărora li se adresează cazurile cele mai grave, aplica cele mai eficiente metode de tratament (inclusiv din punct de vedere financiar) și au cea mai buna performanță medicală

(b) 25 angajați ai instituțiilor subordonate Ministerului Sănătății care vor avea la dispoziție un sistem informatic ce îi va sprijini în cadrul unui centru operativ din cadrul Ministerul Sănătății la distribuirea marilor urgențe medico-chirurgicale (urgențe chirurgicale cardiace, vasculare, neurochirurgicale etc.) și controlul direcționării corecte, pe criterii bine stabilite a acestor pacienți către sălile de operație și secțiile ATI ale marilor spitale de urgență.

(c) 980 cadre medicale (180 medici și 800 asistente medicale) din cele 18 spitale vor avea la dispoziție un instrument informatic care va permite creșterea vitezei de reacție a acestora în cazurile cu evoluție negativă bruscă, prin emiterea automată de alarme pe baza analizei parametrilor medicali monitorizați de sistem. Cadrele medicale își vor putea configura emiterea de rapoarte și statistici în mod automat, privind: evoluția bolnavilor, rezultatele obținute etc., cu scopul eficientizării activităților specifice.

Totodată prin facilitarea accesului cadrelor medicale la o baza de date și informații într-un format coerent și unitar va duce la creșterea activității de cercetare dezvoltare și inovare clinică prin:

- Stimularea dezvoltării de parteneriate cu entități publice (universități și spitale) și particulare (firme medicale) naționale și internaționale pentru desfășurarea de activități de dezvoltare și inovare precum: studii clinice multicentrice, dezvoltarea și experimentare de noi tehnologii medicale, datorită existenței/obținerii de date cu ajutorul sistemului informatic de date clinice trasabile, nealterate și neinfluențate de factori externi;
- Creșterea vizibilității activităților de cercetare medicală din spitalele universitare prin creșterea numărului de articole (subiecte: ATI, infecții nozocomiale, specializări chirurgicale) bine documentate publicate în prestigioase reviste medicale, datorită facilității oferite de sistem, de a extrage date cu caracter medical necesare redactării și documentării articolelor.

Beneficiarii indirecți ai implementării proiectului sunt cetățenii prin creșterea calității îngrijirilor medicale și facilitarea accesului la servicii medicale de calitate. Sistemul va permite monitorizarea continuă, completă, precisă și trasabilă (inclusiv din punct de vedere medico-legal şi al arhivării informațiilor) a parametrilor vitali ai pacienților îngrijiți în secțiile de anestezie-terapie intensivă (ATI), a procedurilor executate si a medicației administrate în aceste secții precum şi a stării bolnavilor îngrijiți în aceste secții, având drept efecte: reducerea semnificativă a numărului de erori, creșterea productivității actului medical și a eficienței personalului medical prin reducerea încărcării cu operații administrative şi birocratice. Estimăm un număr de minim 30.000 de pacienți unici vor fi introduși în baza de date aferenta sistemului SIEC.

HUB MS va permite interoperabilitatea cu alte sisteme din domeniul sanatatii existente/viitoare – cum ar fi de exemplu: DES, 112 etc. in masura existentei unui acord inter-institutional care sa reglementeze interoperabilitatea acestora.

Soluția va permite distribuția seturilor de date către alte instituții guvernamentale pe baza permisiunea de acces. Seturile de date disponibile terților vor fi stabilite în perioada de analiză.

Cerinţele funcţionale minime obligatorii pe care soluţia tehnică pentru realizarea sistemului informatic trebuie să le îndeplinească sunt:

Pentru funcționarea sistemului integrat se vor achiziționa echipamentele TIC necesare:
- pentru sistemul central HUB MS: servere, echipamente de stocare, echipamente de securizare și de comunicații, echipamente UPS și rack, accesorii
- pentru fiecare spital partener de implementare: servere, echipamente de stocare, echipamente de securizare a rețelei, echipamente de comunicații rețea, PC-uri pentru pat terapie intensivă și pentru anestezie sala operatii, terminale digitizare semnale medicale, echipamente wi-fi de tip acces point (AP), echipamente UPS și rack-uri, accesorii

Ministerul Sanatatii este singurul responsabil de a intreprinde toate demersurile necesare pentru ca fiecare spital partener de implementare sa puna la dispoziția implementării proiectului spațiul necesar montării echipamentelor TIC cu care vor fi dotate în cadrul proiectului.

Pentru adopția facilă a sistemului integrat, se vor realiza sesiuni de instruire cu personalul din secțiile de Terapie Intensivă și Săli Operație (SO) din spitalele de implementare, cu personalul de la nivel central și cu personalul IT în administrarea cărora vor intra echipamentele TIC și soluțiile software din cadrul implementării proiectului.

Sistemul, odata finalizat, va deveni proprietatea Beneficiarului (inclusiv codul sursa pentru aplicatiile dezvoltate) urmand legislatia in vigoare privind respectarea drepturilor de autor (licentele COTS si infrastructura ce urmeaza a fi livrata).

2.2.CERINTE FUNCTIONALE

Proiectul se va constitui într-un sistem informatic modern care vine atat în întâmpinarea nevoilor pacientului cat si a cadrelor medicale din sectiile ATI si Salile de Operatie, precum si a angajatilor din sistemul decizional de sanatate (Ministerul Sanatatii si HUB-MS) prin punerea la dispozitie a unor unelte informatice moderne si dashboard-uri pentru optimizarea deciziilor in situatii critice si imbunatatirea politicilor publice in domeniul sanatatii.

Mai jos conturam principalele funcționalități ale celor doua componente ale sistemului informatic.

2.2.1. Principalele funcționalități ale sistemelor informatice ATI si SO

- Monitorizarea permanenta a starii pacientului
- Inregistrarea/transmiterea/consolidarea permanenta a datelor pacientului
- Interconectarea cu sistemele informatice de gestiune (din HIS)
- Interconectarea cu sistemele HIS
- Gestionarea dosarului pacientului aflat in sectiile ATI
- Generarea de rapoarte specializate /customizate in cazul in care este necesar (medico-legale)

2.2.2. Principalele funcționalități ale sistemului informatic HUB - MS

- Functionalitati de dashboard care permit monitorizarea in timp real a disponibilitatii paturilor de ATI+SO din lista de spitale afiliate proiectului
- Instrumente informatice pentru suportul decizional in gestionarea situatiilor de urgenta
- Colectarea/interpretarea/consolidarea/extragerea a unor seturi de date anonimizate ale pacientilor din sistem pentru consolidarea politicilor publice
- Servicii de tip API web service pentru interfațare cu sisteme terțe (posibilitatea interfațării este condiționată de existența unor protocoale interinstituționale)

Întreg ansamblul de componente ale sistemului informatic trebuie să funcționeze integrat și să ofere o experiență unitară tuturor actorilor participanți în proiect, respectiv sectiilor ATI si SO, angajatilor din spitale, precum si decidenților din MS (inclusiv din entități subordonate MS cu personalitate/fără personalitate juridică).

2.3.CERINTE DE ACCES SI SECURITATE

Sistemul trebuie să asigure confidenţialitatea şi securitatea informaţiilor, atât în cadrul proceselor de transfer de date cât şi pentru monitorizarea accesului utilizatorilor la toate resursele sistemului, personalizat în funcţie de responsabilităţile şi drepturile specifice, asigurate printr-un sistem de drepturi şi parole de acces la nivel de: utilizator, funcţie, modul.

Fiecare componenta va include functionalități administrare, spre exemplu:

- întreținere management utilizatori pentru aplicatiile din cadrul fiecarei componente;
- optimizare/indexare si gestiune dimensiuni tabele din baza de date, in cazul bazelor de date;
- administrarea backupului pentru salvari recurente a datelor si pastrarea lor pentru recuperarea după erori severe datorate unor evenimente deosebite

Sistemul nu trebuie să permită ştergerea de date dacă acestea sunt folosite în diverse tranzacţii, altele decât cele curente.
De asemenea, sistemul trebuie să asigure integritatea şi nealterarea datelor şi a aplicaţiilor software.
Datorită atacurilor cibernetice tot mai sofisticate din perioada recentă care au avut loc la nivel global, sistemul trebuie să fie securizat pe mai multe nivele: nivel firewall, nivel de comunicații criptate prin VPN, acces wi-fi securizat, securizarea bazei de date, antivirus la nivel de servere

Securitatea reprezintă o preocupare de bază atunci când este furnizat un serviciu public.
In cadrul proiectului se vor respecta următoarele principii:

- abordarea **securității prin concepție** pentru a asigura securitatea modulelor și a infrastructuriilor complete;
- serviciile **nu sunt vulnerabile la atacurile** care ar putea să le întrerupă funcționarea și ar putea provoca furtul sau deteriorarea datelor;
- integritatea, autenticitatea, confidențialitatea și nonrepudierea datelor.

2.3.1. Cerinte GDPR pentru componenta acces si securitate a sistemului central ATI HUB de servicii MS

Furnizorul va avea in vedere ca datele necesare sa fie colectate și raportate în același format standard pentru toate unitatile ATI.

Se va aplica principiul GDPR de colectare minimalizata a datelor necesare raportarii disponibilitatii paturilor din spitalele cu sectii ATI. Aceasta raportare va fi abordata in mod anonimizat, fara a fi transmise date despre pacienti, avand in vedere ca pentru raportarea numarului de paturi disponibile nu sunt necesare detalii precum numele, varsta, CNP, etnia, cetatenie etc.

Colectarea datelor necesare Componentei Business Intelligence se va face de asemeni in mod anonimizat, într-un asemenea mod încât datele transportate in HUB-ul MS să nu poată fi atribuite unui anumit pacient. În cadrul etapei de analiză se vor specifica datele colectate pentru componenta de Business Intelligence.

Abordarea propusa de anonimizare se va realiza în concordanță cu legislația națională de norme existente atit in legislatia nationala, cit si in cu cea europeana, dupa cum urmează:

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 (Regulamentul general privind protecția datelor)

Articolul 6 Legalitatea prelucrării

(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

...

Articolul 9 Prelucrarea de categorii speciale de date cu caracter personal

(1)Se interzice prelucrarea de date cu caracter personal care dezvăluie ... și prelucrarea ... de date privind sănătatea ... ale unei persoane fizice.

(2)Alineatul (1) nu se aplică în următoarele situații:

...

(b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

(d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

...

(g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

...

(i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional;

LEGE nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date

...

Art. 5: Condiţii de legitimitate privind prelucrarea datelor

...

(2) Consimţământul persoanei vizate nu este cerut în următoarele cazuri:

...

(b) când prelucrarea este necesară în vederea protejării vieţii, integrităţii fizice sau sănătăţii persoanei vizate ori a unei alte persoane ameninţate;

(c) când prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale a operatorului;

(d) când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sunt dezvăluite datele;

(e) când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate;

...

Art. 7: Prelucrarea unor categorii speciale de date

(1) Prelucrarea datelor cu caracter personal ..., precum şi a datelor cu caracter personal privind starea de sănătate ... este interzisă.

(2) Prevederile alin. (1) nu se aplică în următoarele cazuri:

...

b) când prelucrarea este necesară în scopul respectării obligaţiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanţiilor prevăzute de lege; o eventuală dezvăluire către un terţ a datelor prelucrate poate fi efectuată numai dacă există o obligaţie legală a operatorului în acest sens sau dacă persoana vizată a consimţit expres la această dezvăluire;

c) când prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii persoanei vizate ori a altei persoane, în cazul în care persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) când prelucrarea este efectuată în cadrul activităţilor sale legitime de către o fundaţie, asociaţie sau de către orice altă organizaţie cu scop nelucrativ şi cu specific politic, filozofic, religios ori sindical, cu condiţia ca persoana vizată să fie membră a acestei organizaţii sau să întreţină cu aceasta, în mod regulat, relaţii care privesc specificul activităţii organizaţiei şi ca datele să nu fie dezvăluite unor terţi fără consimţământul persoanei vizate;

e) când prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru persoana vizată ori de gestionare a serviciilor de sănătate care acţionează în interesul persoanei vizate, cu condiţia ca prelucrarea datelor respective să fie efectuate de către ori sub supravegherea unui cadru medical supus secretului profesional sau de către ori sub supravegherea unei alte persoane supuse unei obligaţii echivalente

2.3.2. Cerinte generale de securitate a sistemului

Formularea cerintelor de securitate are drept scop definirea cadrului general de securitate prin care sa se asigure confidentialitatea, integritatea si disponibilitatea informatiilor stocate, procesate sau transmise prin sistemele de comunicatii si informatice, destinate operationalizarii sistemelor ATI ale spitalelor si sistemului Central HUB MS.

Arhitectura solutiei trebuie sa respecte reglementarile legale privind GDPR ca si principiu de baza. In acest sens, securitatea datelor prelucrate de sistemul informatic, inclusiv din punct de vedere al comunicatiilor, dintre entitatile participante in sistem trebuie sa fie conforma normelor legale.

Sistemul informatic per ansamblu trebuie sa asigure mecanisme de protectie impotriva incercarilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le gestioneaza. Componentele de securitate trebuie sa asigure securitatea si confidentialitatea datelor. Sistemele SGBD ce vor fi utilizate trebuie sa asigure securitatea si confidentialitatea datelor cu caracter personal ale cetatenilor existente in bazele de date. La nivelul aplicatiilor utilizatorii vor putea accesa numai acele sectiuni si acel continut care le sunt permise prin apartenenta la un profil /Rol sau la o macheta de securitate.

Sistemul integrat va fi implementat si configurat astfel incat:
- sa nu permita persoanelor neautorizate sa modifice sau sa altereze informatiile din sistem;
- sa nu permita persoanelor neautorizate sa acceseze sistemul;
- sa asigure integritatea si autenticitatea datelor si sa permita identificarea sursei datelor initiale si a persoanelor care au accesat sau au inregistrat aceste date in sistem;
- sa asigure trasabilitatea actiunilor utilizatorilor si operatiunilor efectuate in sistem;
- nu va exista posibilitatea de acces pentru persoanele dintr-un mediu extern la date dintr-un mediu considerat intern;
- informatiile private care se transmit vor fi criptate pana la livrare, astfel incat sa nu poata fi interceptate si utilizate;
- informatiile vor putea fi protejate integral si in permanenta pentru acces neautorizat;
- grupurile de utilizatori vor putea fi setate pentru diferite niveluri de acces in sistem;
- sistemul va permite controlul complet al accesului utilizatorilor la aplicatii si la baza de date prin inregistrarea orei si datei la care a fost executata fiecare tranzactie, precum si identitatea utilizatorului care a initiat-o;
- la nivelul componentei de autentificare vor exista facilitati de generare parole, precum si stabilire de reguli specifice (lungime de parola, timp de expirare parola, numarul maxim de erori tolerate la introducerea parolei dupa care utilizatorul este automat blocat);
- va oferi posibilitatea de blocare facila si selectiva a utilizatorilor;
- va asigura securitatea tuturor interfetelor sistemului informatic prevenind accesul utilizatorilor neautorizati la sistem;
- accesul la baza de date il va avea doar administratorul de baze de date prin intermediul functiilor incluse in sistemul SGBD);

Accesul la date trebuie sa se faca doar prin intermediul serviciilor oferite de componentele informatice, pe baza drepturilor detinute de catre utilizatori, accesul direct la datele din tabele nefiind permis. De asemenea, accesul trebuie sa fie reglementat prin politicile de securitate, aferente fiecarui tip de utilizator.

Sistemul trebuie sa includa mecanisme pentru asigurarea urmatoarelor servicii de securitate:
- **confidentialitatea**, care asigura ca datele sunt accesibile, vizibile sau disponibile doar utilizatorilor autorizati atat pentru datele stocate cat si pentru cele care tranziteaza sistemul;
- **integritatea**, care asigura nealterarea datelor sau distrugerea acestora de catre o actiune neautorizata;
- **disponibilitatea**, asigura ca resursele de informatii sa fie accesibile si utilizabile la cererea personalului autorizat atunci cand le sunt necesare;
- **autentificarea**, este mecanismul prin care un utilizator demonstreaza ca este autorizat sa utilizeze sistemul;
- **nonrepudierea**, este un serviciu care nu permite unui utilizator participant la introducerea, modificarea sau manipularea datelor prin sistem sa decline faptul ca el a fost initiatorul unei anumite actiuni.

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.

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. Orice acces în aplicație, atât la nivelul utilizatorilor cât și la nivelul altor module de aplicație, este precedat de identificarea, autentificarea și autorizarea accesului;
- Credențialele de acces nu se transmit în clar prin rețea între componentele sistemului;
- Sesiunile de lucru inactive in aplicatia ATI trebuie să expire după o perioadă de timp configurabilă
- 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 pe sisteme care au aplicate ultimele patch-uri de securitate. În perioada de garanție, daca aplicarea de patch-uri impune modificări de soft acestea vor fi incluse în garanția sistemului, fără costuri adiționale.

Jurnalizare, monitorizare, auditare
Jurnalizarea evenimentelor semnificative legate de controlul accesului
- Înregistrarea în jurnal a autentificărilor cu succes (cel putin dată, oră, adresa IP)
- Înregistrarea în jurnal a autentificărilor fără succes (cel putin dată, oră, adresa IP)

Confidentialitatea 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.
- Toate activităţile utilizatorilor (între log-in şi log-out) sunt înregistrate în fişierul de loguri al sistemului şi sunt astfel clar şi complet trasabile (ce operaţie s-a efectuat, la ce moment de timp).
- Datele nu pot fi şterse complet din aplicație (din raţiuni medicale și legale). Datele introduse greşit se marchează ca atare, se scriu altele în loc, dar cele vechi nu sunt complet şterse. Astfel orice acţiune poate fi identificată la un moment ulterior efectuării ei deoarece toate modificările rămân în baza de date.
- După externarea pacientului sistemul permite 3 nivele de control acces:
    - **total interzis:** nici un fel de date nu mai pot fi adăugate, indiferent de drepturile de acces;
    - **parţial interzis:** după externare se pot adăuga formulare electronice la dosar, atât în baza de date curentă cât şi în baza de date arhivă;
    - **permis:** se pot adăuga orice fel de date în dosarul pacientului după externare, atâta timp cât pacientul figurează în baza de date de producţie (activă). Dacă dosarul este transferat în baza de date arhivă, orice acces este interzis.
- Aplicația pentru ATI și Săli Operație (SO) trebuie să respecte cerințele de regulamentului european GDPR și să conțină mecanisme de anonimizare a datelor cu caracter personal introduse în aplicație.

3. DESCRIEREA TEHNICĂ A PROIECTULUI

3.1.ARHITECTURA TEHNICA SI FUNCȚIONALĂ

Componentele sistemului informatic sunt dispuse in mai multe locatii: 18 spitale partenere aflate in subordinea Ministerului Sanatatii (lista de mai sus) si locatia desemnata de catre Ministerul Sanatatii.

La nivelul fiecarui spital:
Arhitectura fizica “high level” a componentei ATI la nivelul spitalului:

- Secția ATI

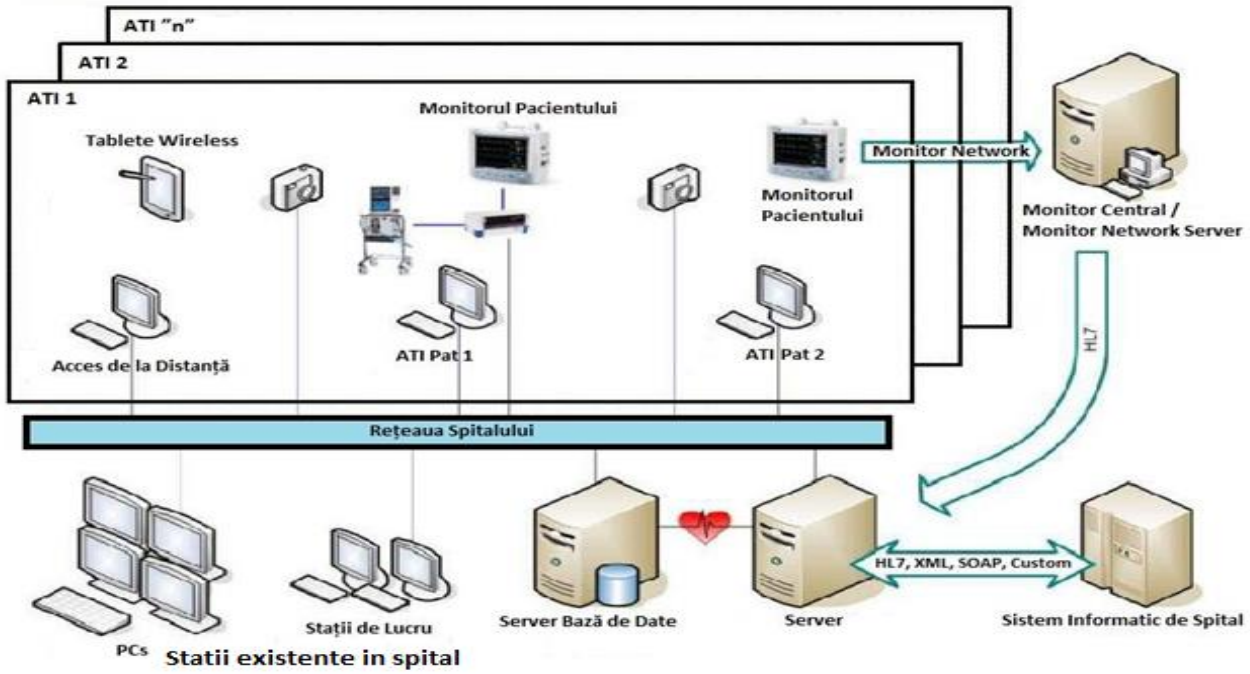


Fig. 4. - Arhitectura fizica "high level" a componentei ATI la nivelul spitalului

- Sali de operatie

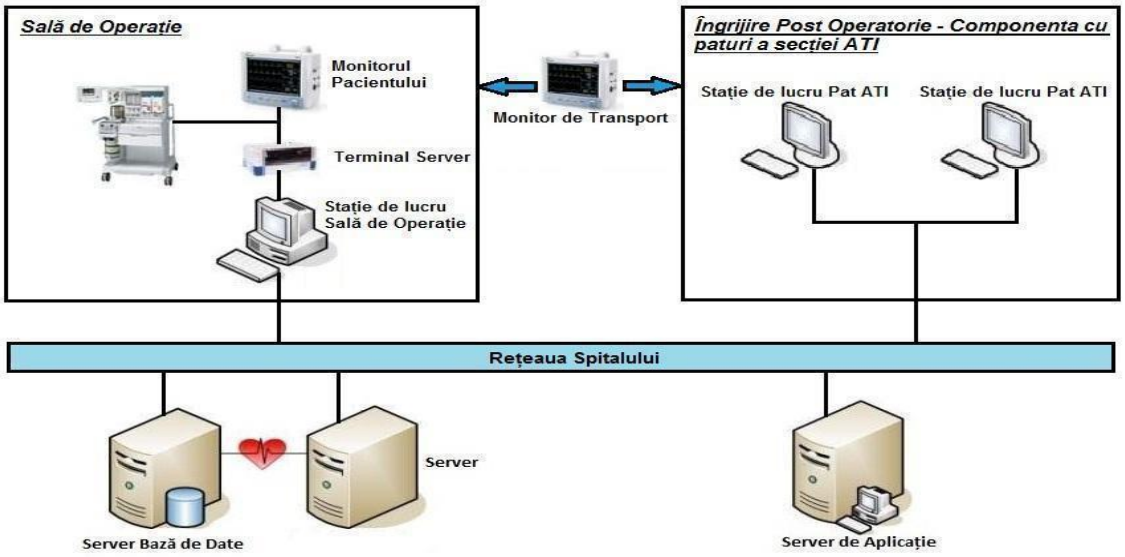


Fig. 5. - Arhitectura fizica "high level" a componentei S.O. la nivelul spitalului

- Arhitectura fizica "high level" a componentei Componenta HUB-MS:

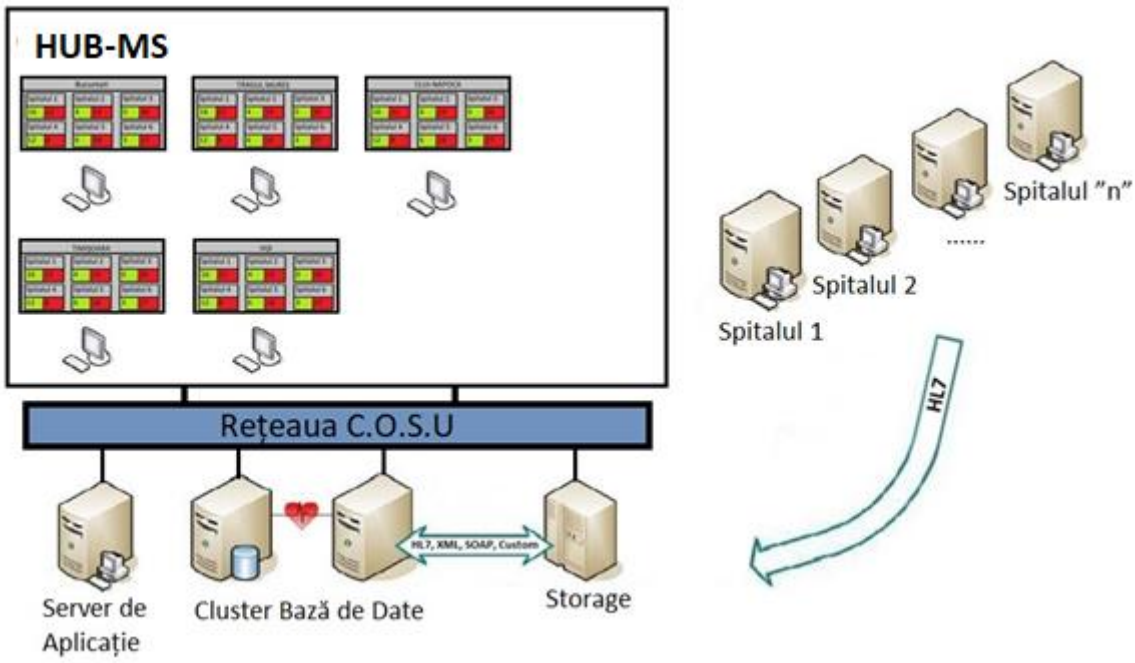


Fig. 6. - Arhitectura fizica "high level" a componentei HUB-MS

- Schema Conceptuala

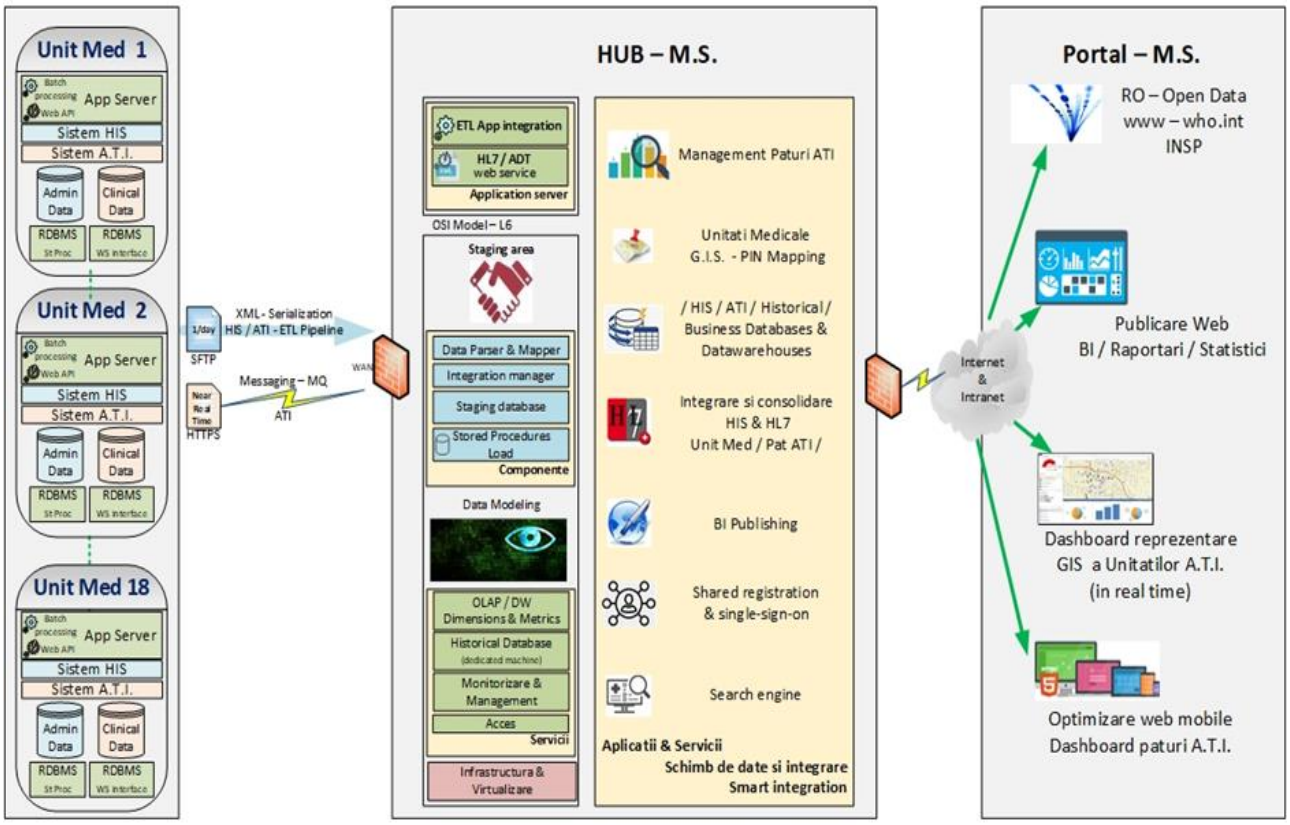


Fig. 7. – Schema Conceptuala – Centrul decizional si operational pentru A.T.I. – HUB-MS

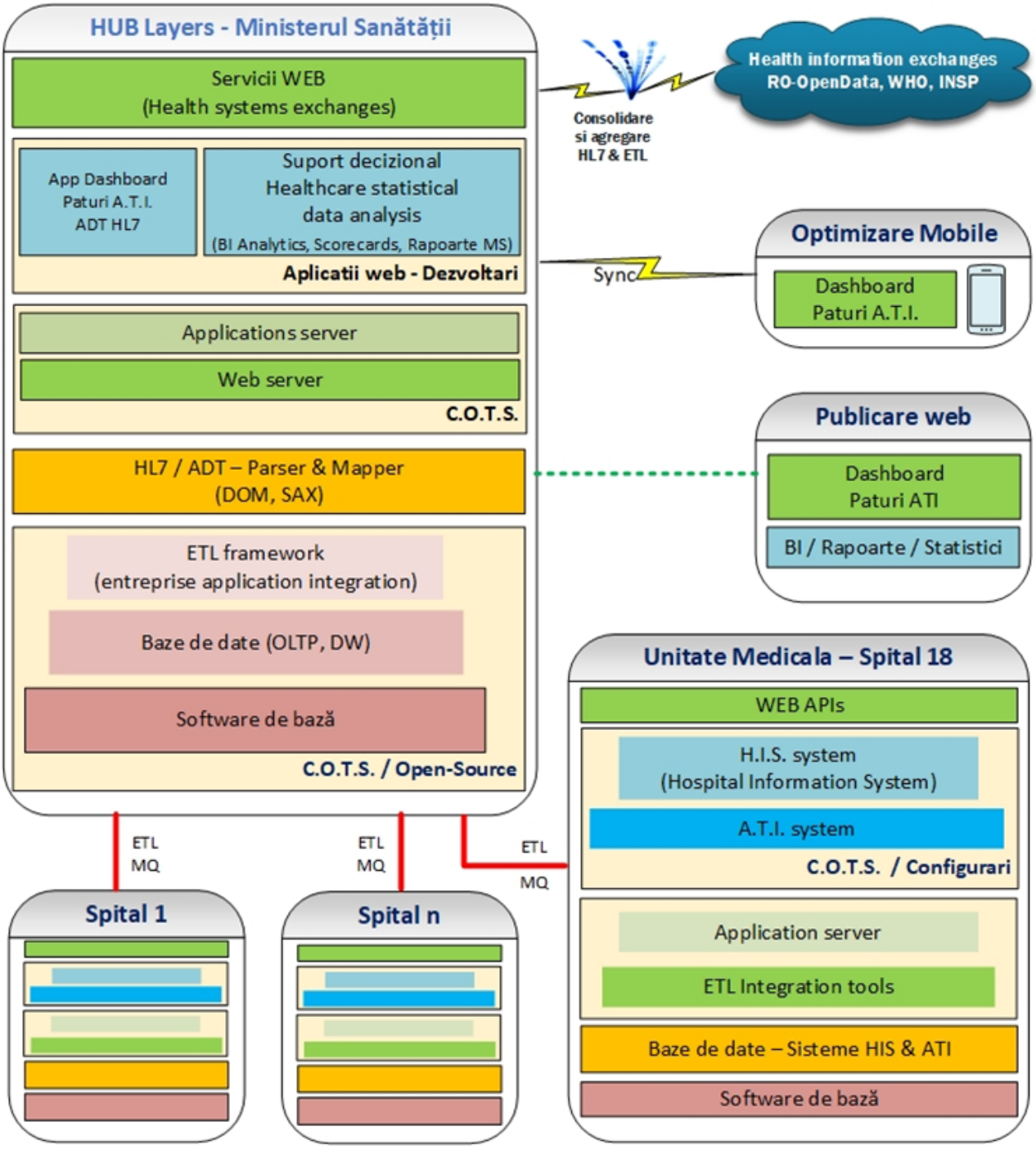


Fig. 8. - Arhitectura TOGAF sisteme (logic functionala)

Transferul de date de la unitățile medicale partenere în proiect se va face prin intermediul componentei de software aplicativ ATI (proces ETL cuplat direct la baza de date operațională și serviciu web).

Arhitectura TOGAF infrastructura

Pentru realizarea obiectivelor și implementarea funcționalităților, este necesară achiziția unui număr de echipamente hardware și licențe software de bază și software aplicativ care să ruleze în fiecare locație de implementare.

Dimensionarea componentelor **mediului de producție** va trebui sa asigure minimul de resurse de procesare dupa cum urmează.

Tabelul dotărilor (18 sectii ATI + sistemul central HUB MS) este prezentat mai jos, în mod centralizat pentru toate locațiile:

Nr. crt.	Articol TIC necesar Hardware	Cantitate totala
1.	Servere pentru baze de date – spital	36
2.	Servere pentru virtualizare - spital	54
3.	Echipament de stocare – spital	18
4.	Server backup – spital	18
5.	Firewall – spital	36
6.	Switch agregare model 1 – spital	72
7.	Switch model 2 – spital	36
8.	UPS – spital	36
9.	Rack- spital	18
10.	Climatizare – aer conditionat – total spitale + HUB MS	38
11.	Access point	446
12.	PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată	924
13	Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă	36
14.	Echipament monitorizare spitale centrul HUB MS	5
15.	Platforma interconectare infrastructura convergenta - centrul HUB MS	1
16.	Server aplicatie backup - HUB MS	1
17.	Firewall - HUB MS	2
18.	Switch agregare model 1 - HUB MS	2
19.	UPS - centrul HUB MS	2
20.	Rack - centrul HUB MS	1
21.	Data Terminal Server	924

Tabel rol masini fizice

Nr.crt.	Locatie	Tip server	Serviciu gazduit	Nr. Core	Memorie (GB)	Stocare locala	Necesar stocare storage (TB)
1	Spital	FIZIC	Baze de date	1 x 8	96	2x 240 (GB) SSD	2.5 de tip SSD
2	Spital	FIZIC	Baze de date	1 x 8	96	2x 240 (GB) SSD	
3	Spital	FIZIC	Virtualizare	2 x 14	256	2x 240 (GB) SSD	6.5 de tip SSD
4	Spital	FIZIC	Virtualizare	2 x 14	256	2x 240 (GB) SSD	
5	Spital	FIZIC	Virtualizare	2 x 14	256	2x 240 (GB) SSD	
6	Spital	FIZIC	Sistem backup	2 x 8	96	2x 240 (GB) SSD	48 de tip HDD

Nr.crt.	Locatie	Tip server	Serviciu gazduit	Nr. Core	Memorie (GB)	Stocare locala	Necesar stocare storage (TB)
1	Centru	FIZIC	Virtualizare	2 x 10	96	2x 480 (GB) SSD	55 de tip HDD
2	Centru	FIZIC	Virtualizare	2 x 10	96	2x 480 (GB) SSD	
3	Centru	FIZIC	Sistem backup	1 x 10	32	2x 600 (GB) HDD 10k	48 de tip HDD
4	Centru	FIZIC	Platforma interconectare convergenta / Baze de date	n.a.	n.a.	n.a.	minim 20 TB hibrid

Tabel rol masini virtuale

Nr.crt.	Locatie	Tip server	Aplicatie/functionalitate gazduita	vCore	Memorie (GB)	Disk virtual SO (GB)	Disk virtual suplimentar (GB)
1	Spital	Virtual	Directory	2	8	128	
2	Spital	Virtual	Directory	2	8	128	
3	Spital	Virtual	Aplicatie ATI	16	32	128	3000
4	Spital	Virtual	Aplicatie SO	16	32	128	250
5	Spital	Virtual	Comunicare cu statii centrale echipamente existente	16	32	128	250
6	Spital	Virtual	Comunicare cu statii centrale echipamente existente	16	32	128	250
7	Spital	Virtual	Comunicare cu statii centrale echipamente existente	16	32	128	250
8	Spital	Virtual	Comunicare cu statii centrale echipamente existente	16	32	128	250
9	Spital	Virtual	Comunicare cu statii centrale echipamente existente	16	32	128	250
10	Spital	Virtual	Raportare/BI nivel spital	16	32	128	500
11	Spital	Virtual	Comunicare cu HUB MS (HL7/ETL)	16	32	128	2000
12	Spital	Virtual	Comunicare cu sisteme de tip HIS (HL7)	16	32	128	2000

Nr.crt.	Locatie	Tip server	Aplicatie/functionalitate gazduita	vCore	Memorie (GB)	Disk virtual SO (GB)	Disk virtual suplimentar (GB)
1	Centru	Virtual	Comunicare cu spitale (HL7/ETL)	16	16	128	250
2	Centru	Virtual	Dashbord	16	32	128	250
3	Centru	Virtual	BI	8	16	128	250
4	Centru	Virtual	Consola management echipamente	4	8	128	250
5	Centru	Virtual	Consola antivirus	8	8	128	250
6	Centru	Virtual	Analiza SIEM	16	16	128	4000

3.2.COMPONENTELE SOFTWARE ALE SISTEMULUI

- Componenta informatică pentru secțiile de Terapie Intensivă și Bloc Operator / Săli Operație (SO) la nivelul fiecărui spital partener în proiect (din lista de mai jos)
- Componenta HUB MS:
    - Componenta Dashboard Disponibilitate paturi ATI, integrată cu aplicațiile ATI din spitalele de implementare din cele 5 regiuni/orașe – lista de mai jos. Aplicația va permite vizualizarea în timp real a situației din cele 18 spitale și va permite initierea procesului de rezervare a paturilor ATI
    - Componenta Business Intelligence – BI de raportare la nivelul Ministerului Sănătății pentru analiza datelor din sistem la nivel istoric: zilnic, săptămânal, lunar, anual sau ad-hoc ca suport în luarea deciziilor

Cerinte generale pentru componentele software de tip COTS:

- Oferta tehnica va contine in clar denumirea comerciala si codul comercial (part numberul) a licentelor software ofertate conform catalogului de produse al producatorului acestora precum si cantitatea ofertata.
- Licentele software ofertate vor fi conforme schemei de licentiere a producatorului acestora, vor asigura licentierea completa a puterii de calcul a serverelor din fiecare locatie si vor permite definirea unui numar nelimitat de masini virtuale.
- Licentele software ofertate vor fi non-OEM, licente perpetue, putand a fi utilizate de catre beneficiar pe orice server functie de cerintele de procesare si stocare date.
- Licentele software ofertate vor asigura administrarea serverelor in configuratie cluster, la nivelul fiecarei locatii, administrarea fiind realizata in consola pe baza de conturi cu drepturi de acces
- Furnizorul solutiei trebuie sa asigure garantie 3 ani si suport software 24x7 de la producatorul licentelor software, de la data receptiei cantitative in locatia de instalare.

3.2.1. Componente software la nivel spital

I.2.1.1. Componente software de baza la nivelul fiecarui spital

I.2.1.1.1. Software pentru baze de date relationale

Sistemul de gestiune al bazelor de date relationale trebuie sa fie disponibil comercial (COTS – Commercial off the Shelf) si sa ofere posibilitatea de a rula pe diverse platforme hardware precum si pe sistemele de operare majore existente pe piata (Windows, Linux si Unix). Pentru a raspunde cerintelor de functionalitate si performanta cerute, sistemul de baze de date relationale trebuie sa prezinte urmatoarele capabilitati:

- trebuie să asigure nivelurile de izolare ANSI SQL si sa ofere suport pentru functionalitatile de baza pentru limbajul SQL asa cum sunt ele stabilite in standardele SQL:2008 si SQL:2011;
- sa ofere suport Unicode UTF-8 sau echivalent;
- sa ofere suport pentru date de tip multimedia si geo-spatiale;
- sa permita nativ stocarea si gestiunea de structuri de date de tip XML;
- sa ofere suport pentru proceduri stocate si triggeri;
- sa permita, folosind o singura comanda de tip DML, introducerea datelor pe mai multe tabele simultan;
- sa permită faciliteze accesul cat mai rapid la informatii prin utilizarea diferitelor tipuri de indecşi, cum ar fi B-Tree, function based, domain sau similari;
- sa permita definirea de tabele de tip index pentru acces rapid la anumite tabele;
- să ofere suport complet pentru folosirea de expresii regulate si functii analitice;
- sa permita criptarea datelor in baza de date folosind oricare din algoritmii AES (minim 256 bit) si 3DES;
- sa permita criptarea transparenta, fara a necesita modificarea aplicatiilor, a informatiile vehiculate in timpul sesiunilor intre utilizatori/applicatii si baza de date folosind atat algoritmii criptografici AES si 3DES cat si protocoale criptografice specifice - SSL/TLS;
- sa ofere posibilitatea autentificarii utilizatorilor pe baza de certificate digitale;
- sa permita restrictionarea accesului la nivelul obiectelor bazei de date si sa ofere o lista cu operatiile pe care un grup sau o clasa de utilizatori le poate executa;
- sa permita realizarea online (fara oprirea bazei de date) de operatiuni de backup si restaurare, inclusiv pentru datele de tip BLOb (Binary Large Object) stocate in baza de date;
- să permită efectuarea de backup atât complet, cât si partial (incremental) iar pentru optimizarea spatiului aferent datelor de backup sa includa posibilitatea de compresie a datelor de backup;
- trebuie să ofere posibilitatea de a marca anumite fisiere de date sau tablespace-uri ca fiind de tip read-only, in vederea excluderii pe viitor a acestora din operatiile automate de backup (atat backup complet dar si incremental) ale bazei de date;

- sa ofere mecanisme integrate in baza de date pentru recuperarea datelor modificate de o tranzactie care a fost comisa, fara a fi necesara intreruperea activitatii pe baza de date, restaurarea datelor dintr-un backup sau intretinerea prin proceduri de utilizator a unor copii ale datelor;
- trebuie să ofere nativ mecanisme care sa permita interogarea istoricului modificarilor unei tabele, indiferent de tipul activitatilor (DDL sau DML), fara a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvarea periodica sau utilizarea functiei de audit
- trebuie sa permita functionarea intr-o arhitectura de disponibilitate inalta de tip cluster activ-activ asigurandu-se toleranta la defecte hardware sau nefunctionare planificata, scalabilitatea si disponibilitatea crescuta a sistemului. 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.
- trebuie să ofere posibilitatea de a aduga la nevoie noduri suplimentare in cluster, noduri care vor fi active imediat si vor prelua din incarcarea bazei de date, fara a necesita oprirea serviciilor la nivel de cluster;
- balansarea incarcarii intre noduri la nivelul cererilor si executiilor pe baza de date cluster, oferind astfel o incarcare uniforam a nodurilor dar si posibilitatea de a accesa memoria de pe celelalte noduri ;
- trebuie să includă propriul software de clustering si management al discurilor, astfel incat să permita rularea pe diferite platforme hardware si sisteme de operare, fara achizitionarea de soft aditional de la producatorul sistemului de operare, asigurandu-se totodata scalabilitatea orizontala a bazei de date si usurinta in administrare;
- sa ofere o consola/interfata unica, integrata, care sa permita administrarea si monitorizarea usoara a bazei de date sens in care va oferi:
    - un editor SQL inteligent cu functie de completarea automata a frazelor prin sugestii în functie de context;
    - posibilitatea editarii tabelelor bazelor de date intr-o fereastra interactiva în care se pot edita parametrii de interogare sau executie, valida sau calcula diverse valori etc.;
    - posibilitatea reformatarilor interogarilor SQL în functie de nevoie sau de utilizator;
    - posibilitatea proiectarii structurii bazelor de date precum si vizualizarea și editarea în mod grafic a structurii bazelor de date;
    - posibilitatea compararii datelor din doua tabele și reuniunea acestora intr-una singura
    - modelarea relaţională şi dimensională a datelor inclusiv raportare, precum si vizualizarea grafica a obiectelor de tip BLOb.

Suport software asigurat pentru minim 3 ani de la data receptiei cantitative.

I.2.1.1.2. Solutie virtualizare

Pe nodurile de virtualizare se va folosi o solutie de virtualizare cu management centralizat care trebuie sa aiba urmatoarele functionalitati:

- Să nu depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea şi funcţionalitatea serverelor, respectiv a maşinilor virtuale care rulează pe serverele respective;
- Amprenta pe disc a hypervisor-ului să fie cat mai mică (sub 300MB) astfel încât instalarea hypervisor-uIui să fie facuta foarte rapid (direct pe server) chiar și din rețea, oferind totodata posibilitatea de boot-are de pe stick USB;
- Suport pentru USB 3.0 (client atasat la masini virtuale cu sistem de operare Linux);
- Să permită conectarea peste rețea printr-un concentrator de porturi seriale la consola serială a oricarei mașini virtuale (exemplu: Linux);
- Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalitati disponibile în noile versiuni de procesoare;
- Să ofere o scalabilitate crescuta prin configurarea în clustere de înaltă diponibilitate;

- Să dispună de capacitati de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster;
- Să dispună de capacitati de failover astfel încât, în cazul defectării parțiale a unui host, mașinile virtuale care rulau pe acel host să poata fie migrate online pe celelalte host-uri din cluster iar host-ul degradat sa fie trecut in mentenanță după evacuarea mașinilor virtuale;
- Să dispună de capacitati de failover astfel încât, în cazul blocarii sistemului de operare instalat intr-o mașina virtuală, respectiva mașina virtuală să fie restartată automat pe acelasi host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor;
- Să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster;
- Să permită identificarea și evitarea situatiilor de split-brain prin monitorizarea stării host-urilor atât la nivelul retelei de management cat și la nivelul storage-ului comun;
- Să permită replicarea mașinilor virtuale la nivel de host, independent de tipul stocării folosite la sursă și destinatie, asigurand un RPO (recovery point objective) de minimum 5 minute;
- Să permită stabilirea unei politici de retentive a replicărilor cu peste 20 de replici în timp (exemplu: 4 replici pe zi, timp de 6 zile), care vor permite refacerea sistemului replicat prin procedura de recuperare, solutie utila pentru refacerea în cazul coruperii datelor sau virusarii;
- Să ofere posibilitatea mutarii simultane a mașinilor virtuale (minim 4, pe legaturi Gigabit/10 Gigabit) în funcționare de pe un host pe altul/altele fără afectarea funcționarii acestora pentru a se putea executa activitati de mentenanta pe host-ul respective;
- Să asigure rate mari de consolidare a mașinior virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memoriei (ex “Memory BalIooning”, ”Transparent Page Sharing”, “Memory Compression”, “Swap to disk”) pentru reducerea costurilor asociate infrastructurii fizice (exemplu: număr host-uri, număr porturi de rețea/switch-uri);
- Să poată rula pe host-uri echipate cu până Ia 576 de CPU-uri logice și 12TB memorie RAM;
- Sisteme de operare suportate pe mașinile virtuale: Windows (Server: 2016, 2012 R2, 2008 R2, 2003 R2, Desktop: 10, 8.1, 7), Red Hat, SuSE, Ubuntu, FreeBSD, CentOS, Solaris, Oracle Linux, Mac OS X Server;
- Aplicatia de virtualizare să permită configurarea și rularea unor mașini virtuale cu până la 128 procesoare virtuale și 6TB RAM;
- Să suporte diverse tipuri de storage (SAN, NAS, iSCSI) și protocoale de access (FC, FCOE, ISCSI, NFS) la nivel de cluster;
- Suport larg din partea ISV (Independent Software Vendors) terti pentru aplicațiile Tier 1 și nu numai – exemplu: Microsoft – SQL, Exchange, SharePoint, Oracle – RAC, SAP – HANA;
- Posibilitatea utilizării unui echipament de stocare extern pentru mai multe host-uri. Storage-ul trebuie să poată stoca atât mașina virtuală cât și hard disk-urile virtuale asociate acesteia;
- Accesul către sistemul de stocare extern să poată fi făcut pe mai multe căi (muItipathing), asigurându-se suport pentru failover și load balancing, oferind și posibilitatea de alegere a politicii de stabilire a căii de acces (exemplu: fixă, MRU, Round Robin);
- Sistemul de fişiere va permite accesul concurent a mai multor servere fizice (host) şi a mai multor maşini virtuale la aceeaşi resursă de stocare;
- Sistemul de fişiere trebuie să asigure că o maşină virtuală este accesată doar de pe un singur host (sistem de blocarea accesului); în caz de defectare a host-ului maşina virtuală trebuie să poată fi restartată de pe alt server fizic;
- Sistemul de fişiere va asigura posibilitatea migrării în timp real (fără intreruperea funcţionării) unei maşini virtuale de pe un host pe altul;
- Sistemul de fişiere tebuie să suporte expansiunea dinamică a volumelor şi LUN-urilor la capacitati mai mari de 2TB;
- Aplicatia de virtualizare trebuie să permită crearea de grupuri de maşini virtuale care să impartă aceleaşi resurse puse Ia dispozitie în comun (memorie şi timpi de procesor);
- Software-ul instalat pe host trebuie să poată crea echipamente de reţea virtuale (switch-uri) Ia care să se conecteze maşiniIe virtuale şi interfetele de rețea fizice de pe host;

- Aplicatia de virtualizare trebuie să permită managementul salvărilor contextuale (snap-shot) ale maşinilor virtuale fără afectarea stării de funcționare, astfel încât o maşină virtuală se va putea restaura din orice salvare anterioară;
- Interfata unica de management bazata pe interfata web, accesibila de pe browser-e Firefox (Windows, Mac OSX), Google Chrome (Windows, Mac OSX) și IE (Windows) pentru simplificarea managementului;
- Soluția de management centralizat aferente fiecarei locatii să fie disponibilă ca appliance virtual pentru simplificarea instalarii, actualizării și administrării precum și pentru reducerea costurilor asociate (exemplu: licenta windows, licenta baza de date SQL sau Oracle).
- Solutia de management trebuie sa ofere informatii privind intregul inventar al mediului virtual administrat din locatia respectiva, incluzand masini virtuale, gazde, medii de stocare si rețele de date;

Suport software de la producatorul licentelor software pentru minimum 3 ani de la data receptiei cantitative in locatia de instalare.

I.2.1.1.3. Solutie de backup

- Aplicatia de backup furnizata va trebuie sa fie capabila sa gestioneze dintr-o singura consola de administrare, atat serverele fizice cat si cele virtuale.
- Administrarea aplicatiei de backup se va realiza prin intermediul unei console de administrare centralizata pentru mai multe servere de backup, indiferent de platformele pe care ruleaza acestea (Windows, Linux).
- Aplicatia de backup trebuie sa puna la dispozitie si o interfata de management de tip “command line”, atat pentru platforme Windows, dar si pentru Linux.
- Aplicatia de backup trebuie sa permita instalarea unei console de administrare pe statia de lucru a administratorului.
- Solutia de backup trebuie sa puna la dispozitie, pe langa setarile si configurarile standard, un set de “wizard-uri” care sa permita administratorilor sa configureze cat mai usor device-urile utilizate pentru salvarea datelor, volumele, job-urile de backup pentru salvarea catalogului, precum si crearea usoara de politici de backup folosind aceste “wizard-uri”.
- Solutia de backup trebuie sa aiba capabilitatea de a seta limitari la nivelul benzii de retea si de a aplica restrictii de banda in timpul procesului de backup.
- Solutia de backup oferita va trebui sa dispuna de capabilitati de retentie a backup-urilor pentru diverse perioade de timp: saptamanal, lunar, anual si infinit.
- Aplicatia de backup trebuie sa fie capabila sa descopere masinile virtuale nou create pentru a le putea include in procesul de backup.
- Aplicatia de backup va oferi posibilitatea automatizarii, bazata pe politici, ale proceselor de backup si restaure.
- Aplicatia de backup va permite efectuarea backup-ului doar pentru fisierele care au suferit schimbari de la ultimul backup si pentru fisierele nou create.
- Aplicatia de backup va putea pune la dispozitie (la cerere) un model de administrare flexibil, permitand accesul mai multor utilizatori (administratori si operatori), fiecare cu nivel de autorizare diferit.
- Aplicatia de backup va putea oferi facilitatea de criptare a datelor schimbate intre client si server in timpul procesului de backup/restore.
- Aplicatia de backup va permite setarea perioadelor de pastrare a datelor salvate, in functie de timpul la care a fost realizat backup-ul.
- Aplicatia de backup va oferi mecanisme de “Data reduction” (compresie si deduplicare) pentru eficientizarea utilizarii retelei si a spatiului de stocare.
- Aplicatia de backup trebuie sa aiba suport nativ pentru serviciul director inclus in arhitectura propusa

- Abilitatea de a restaura obiecte individuale ale serviciului director pana la nivelul de atribute individuale fara a restaura intreg serviciul director.
- Abilitatea de a restaura articole individuale ale serviciului director, in timp ce acesta este in activitate (nu necesita restartare), incluzand:
    - conturi individuale de utilizator
    - Organizational Units (OU's)
    - Obiecte printer
    - Chiar atribute individuale ale serviciului director si valori incluzind nume, adrese, numere de telefon, adrese de posta electronica, etc. toate dintr-un singur pas la nivel de copie de siguranta a serviciului director
- Solutia de backup trebuie sa suporte backup pe disc si pe banda magnetica.
- Solutia de backup trebuie sa se integreze cel putin cu urmatoarele aplicatii si baze de date: Microsoft SQL, Microsoft Active Directory, Oracle, IBM DB2, MySQL, PostgreSQL.
- Aplicatia de backup ofertata trebuie sa suporte urmatoarele sisteme de operare: Windows Server, Windows Client, Linux (Red Hat, SUSE, Oracle, Debian/CentOS/Ubuntu).
- Serverul de backup trebuie sa suporte instalarea pe cel putin urmatoarele platforme: Windows, Linux Red Hat, Oracle Linux si SUSE.
- Solutia de backup trebuie sa se integreze cu principalele medii de virtualizare cum ar fi VMware si Microsoft Hyper-V.
- Solutia furnizata nu trebuie sa necesite instalarea de Proxy VM pentru a realiza backup la medii virtuale ce folosesc hipervizori VMware sau Microsoft Hyper-V.
- Aplicatia de backup trebuie sa fie capabila sa restaureze la nivel granular (file si folder) din interiorul unei masini virtuale (Hyper-V sau VMware), fara a fi nevoie de o restaurare integrala a masinii virtuale si fara a fi nevoie sa se instaleze vreun agent in masina virtuala.
- Solutia de backup trebuie sa poata pune la dispozitie API-uri cum ar fi interfata de tip XBSA ce permite furnizorilor de aplicatii sa dezvolte propriile solutii care sa se integreze cu clientii/aplicatia de backup.
- Licente perpetue pentru backup-ul a 4TB de date din fiecare locație de implementare (18 spitale).

I.2.1.1.4. Solutie serviciu director

Sistemul director trebuie să aibă următoarele funcționalități:
- să permită utilizarea structurii director constând din servicii director pentru gestionarea identităților și servicii meta-director pentru îmbunătățirea administrării;
- serviciul director pentru gestionarea identităților trebuie să suporte protocolul tip LDAP;
- serviciul director va permite definirea de politici de securitate;
- să suporte RFC 1823, ADSI, și JNDI API;
- serviciul director al gestionării identităților trebuie să suporte replicarea conținutului;
- Monitorizarea, diverse operații și restaurarea directorului de gestionare al identităților pot fi delegate;
- directorul trebuie să permită posibilitatea modificării topologiei infrastructurii, procedurilor de configurare si de operare printr-un proces de gestionare a modificărilor, iar modificările pot fi delegate;
- directorul de gestionare al identităților trebuie să aibă o singură rădăcină;
- spațiul de nume al serviciului director de gestionare al identităților poate fi partiționat într-un fel care să reflecte structura organizațională sau organizația;
- convenția numelui organizației va identifica indivizii folosind un identificator numeric unic ca valoare a unui atribut specific;
- serviciul director va permite adăugarea sau modificarea definițiilor claselor de obiecte și spațiul de nume al topologiei;
- să furnizeze posibilitatea auditării accesului pentru serviciul director și pentru modificările acestuia;
- serviciul director va avea abilitatea să stocheze certificate și CRL-uri;

- va permite integrarea cu serviciul DNS;
- va permite reproducerea și stocarea zonelor DNS găzduite în aplicația director;
- suportă dezactivarea atributelor și definițiilor claselor în schema director, astfel încât atributele și clasele pot fi redefinite dacă apar erori în definirea inițială.

Se vor asigura în cadrul proiectului toate licențele necesare, perpetue, pentru realizarea sistemului director pentru managementului utilizatorilor și al accesului în sistem in fiecare din locațiile de implementare a proiectului.

I.2.1.2. Componenta software aplicativ pentru sectiile ATI cu paturi si Sali de Operatii (SO)

A.1.1 Soluţia trebuie să fie compatibilă cu cerinţele specifice sistemului de sănătate din România (Ordinul Ministrului Sănătăţii Nr. 1500 / 24 Noiembrie 2009 privind aprobarea Regulamentului de organizare şi funcţionare a secţiilor şi compartimentelor de anestezie şi terapie intensivă din unităţile sanitare, publicat în Monitorul Oficial Nr. 873 / 15 decembrie 2009), şi confirmată prin referinţe internaţionale solide în domeniu.

A.1.2 Soluţia propusă trebuie să fie certificată produs medical clasa IIa, în conformitate cu următoarele reguli:
- DIN EN ISO 13485:2016
- DIN EN ISO 14971:2012
- EN 62366:2008
- EN 62304:2006/AC2008

A.1.3 Soluţia trebuie să poată fi utilizată în toate tipurile de secţii de anestezie - terapie intensivă, inclusiv: Generală, Chirurgie, Chirurgie Cardio-vasculară, Chirurgie Reparatorie - Arși, Unitate de Terapie Intensivă Pediatrică, Unitate de Terapie Intensivă Neonatală. Soluția trebuie să aibă câte o referinţă funcţională pentru fiecare din secţiile mai sus menţionate.

A.1.4 Soluţia trebuie să asigure colectarea şi înregistrarea automată precum şi afişarea informaţiilor şi datelor privind activitatea de anestezie care să acopere tot fluxul activităţilor, începând cu istoricul şi continuând cu etapele pre-operator, intra-operator, post-operator şi externare respectiv transfer al pacientului. Toate informaţiile provenind din internările precedente sau externări, vor fi de asemenea disponibile într-o bază de date unică. Soluția trebuie să aibă minim o referinţă funcţională care să ateste utilizarea soluţiei într-o unitate spitalicească.

A.1.5 Soluţia trebuie să fie flexibilă, pentru o implementare uşoară a procedurilor, protocoalelor şi practicilor medicale.

A.1.6 Soluţia trebuie să fie implementată de către personal cu experienţă dovedită prin documente, atestări, etc.

A.1.7 Implementarea soluţiei trebuie să fie bazată pe metodologii standard, iar experienţa specifică a echipei de proiect a ofertantului trebuie probată prin certificări relevante şi experienţă în proiecte similare.

A.1.8 Soluţia trebuie să beneficieze de o interfaţă utilizator în limba română şi trebuie să folosească limba română pentru toate meniurile, ecranele, rapoartele etc.

A.1.9 Soluția trebuie să ofere o interfaţă utilizator intuitivă, cu accent pe modul în care se completează, accesează, vizualizează şi asociază datele.

A.1.10 Soluția software trebuie să suporte folosirea ecranelor senzitive („touch screen”).

A.1.11 Soluția software trebuie să fie ergonomică și să contribuie la reducerea timpului necesar introducerii datelor. În plus, în sala de operație, în scopul diminuării riscului de contaminare microbiană, soluția nu trebuie să necesite folosirea mouseului și a tastaturii.

A.1.12 Soluţia trebuie să asigure suport/monitorizare continuă pentru îngrijirea pacientului între toate secţiile ATI din cadrul fiecărui spital în parte.

A.1.13 În funcţie de nivelul de acces al utilizatorului, trebuie să fie posibilă parcurgerea tuturor procedurilor medicale şi informaţiilor relevante ale sejurului pacientului în spital (parcursul complet al pacientului între: sala de operaţie, perioada de transport monitorizat şi unitatea cu paturi a secţiei de Terapie Intensivă), pe o singură fişă a pacientului.

A.1.14 Soluţia trebuie să monitorizeze în permanenţă statusul fiecărui dosar medical electronic.
A.1.15 Soluţia trebuie să asigure accesul uşor şi rapid la istoricul consultaţiilor, intervenţiilor şi tratamentelor pentru fiecare pacient în parte.
A.1.16 Soluţia trebuie să permită căutarea unei fişe de pacient după o combinaţie de criterii precum:

- ID-ul pacientului
- Nume
- Prenume
- Gender
- Data nastere
- Date de contact (adresa, tel, email)
- Persoana Ruda cu pacientul/Membru familie
- Date de contact Rude pacient
- Medic specialist
- Medic de familie
- Număr pat
- Data internării
- Data externării
- Alergii
- Proceduri medicale

A.1.17 Soluţia trebuie să permită trasabilitatea datelor pacientului de la internare până la momentul interogării.
A.1.18 Soluţia trebuie să permită salvarea şi stocarea datelor obţinute automat de la echipamentele medicale sau alte servicii care furnizează informaţii (alte sisteme informatice din spital) în baza de date, fără a fi necesară intervenţia utilizatorilor, doar interconectarea echipamentelor/serviciilor.
A.1.19 Soluţia trebuie să permită validarea ulterioara de către utilizator a informaţiilor obţinute automat de la echipamente.
A.1.20 Soluţia trebuie să permită stocarea şi salvarea datelor introduse de către utilizatori fără a fi nevoie de a fi semnate şi salvate elementele de date individuale cu posibilitatea de validare ulterioara a informatiilor.
A.1.21 Soluţia trebuie să asigure disponibilitatea unor interfeţe (API) care să accepte date în timp real de la diferite alte surse de date (de exemplu: sisteme de laborator, imagistică etc.);
A.1.22 Soluţia trebuie să pună la dispoziţia spitalului datele statistice necesare pentru pregătirea continuă a personalului medical şi non-medical;
A.1.23 Soluţia trebuie să aibă un modul de documentare inteligent care să îndrume/asiste utilizatorii prin scenarii de flux de lucru specifice.
A.1.24 Soluția trebuie să funcționeze concomitent pe mai multe secții ATI din același spital și să folosească aceeași bază de date, iar utilizatorii să poată fi restricționați pe secția ATI sau bloc operator de care aparțin (să poată vedea doar pacienții de care au grijă, medicația acestora etc.)
A.1.25 Soluţia trebuie să permită: afişarea disponibilităţii paturilor pentru fiecare salon/secţie ATI, semnalarea problemelor de ocupare, afişarea alocării pacienţilor pe pat, menţinerea datelor pacientului la schimbarea patului.
A.1.26 Soluţia trebuie să permită utilizarea de diagnostice principale şi secundare.
A.1.27 Soluţia trebuie să permită supravegherea pacienţilor de către medicii situaţi la distanţă. Supravegherea trebuie să includă informaţiile clinice complete, prescrieri medicale etc.
A.1.28 Soluția trebuie să permită extragerea datelor din echipamentele medicale de transport (ex: monitoare de semne vitale mobile, pompe de infuzie, seringi electrice, etc.), acolo unde acestea permit modul de stocare a datelor offline, astfel încât datele înregistrate pe perioada transportului pacienților (între: diversele secții ATI, blocul operator, UPU, chiar și între centre medicale), să poată fi integrate automat de către sistem.
A.1.29 Soluţia trebuie să opereze pe o arhitectură clasică client-server şi o bază de date relaţională.

A.1.30 Arhitectura soluţiei trebuie să fie deschisă pentru a facilita comunicarea cu o orice fel de echipament de pat de ATI, sală de operaţie şi paturi mobile (spitalele participante dispun de o structură foarte eterogenă de astfel de echipamente achiziţionate neunitar şi conform cu alocările bugetare), cât şi comunicarea cu sistemul informatic al spitalului;

A.1.31 Soluţia trebuie să aibă și o componentă mobilă, aceasta permițând accesul de la distanță (din orice locație cu acces la internet), prin orice dispozitiv mobil (laptop, telefon inteligent, tabletă etc) indiferent de marcă/sistem de operare, la informațiile pacienților din secțiile de ATI (pașaportale, medicație, analize de laborator, semne vitale, proceduri medicale, raportul intervențiilor chirurgicale). Această componentă trebuie să permită modificarea prescripțiilor de medicație și a procedurilor mediale cât și adăugarea unora noi.

A.1.32 Atât datele referitoare la ATI cât şi cele referitoare la SO trebuie să aibă aceeaşi bază de date şi aceeaşi arhitectură astfel încât se fie posibilă realizarea unui flux continuu și coerent de date pentru pacienţii critici care necesită monitorizare şi terapie specifică.

A.1.33 Soluţia trebuie să permită introducerea mai multor secţii într-o bază de date, pe un singur server. Structura aferentă fiecărei secţii trebuie să fie independent configurabilă;

A.1.34 Soluţia propusă trebuie să permită următoarea arhitectură realizarea de arhitecturi cu o configurație de bază trebuie să fie aceeași pentru toate spitalele, dar să permită personalizare locală pe baza nevoilor spitalelor;

A.1.35 Soluţia trebuie să ofere o interfaţă-utilizator coerentă din punctul de vedere al elementelor de design (structură, fonturi, culori, meniuri etc.) la nivelul întregului sistem;

A.1.36 Soluţia trebuie să fie parametrizabilă de către utilizatori instruiţi şi certificaţi pentru aceasta, fără a necesita cunoştinţe avansate de programare.

A.1.37 Soluţia trebuie să nu permită existenţa datelor dublate, trebuie să sesizeze datele inconsistente, datele lipsă sau deteriorate;

A.1.38 Soluția trebuie să genereze vizualizarea în timp real a datelor financiare relevante pentru: consumuri de materiale sanitare, medicamente, proceduri medicale.

A.1.39 Soluţia trebuie să poată încorpora practic orice standard de codificare şi facturare. Odată selectate datele relevante din sistemul de coduri (de exemplu: DRG) acestea vor fi importate şi memorate în baza de date a sistemului ca parte a dosarului de pacient. Informaţiile importate din DRG împreună cu alte informatii (de exemplu: timp de ventilaţie, scor APACHE, prescripţii medicale, etc.) trebuie să poată fi exportate către sistemul informatic de management al spitalului pentru calculele totale de costuri ale pacientului respectiv.

A.1.40 Soluţia trebuie să permită implementarea mai multor categorii uzuale de interfeţe, obligatoriu XML/JSON, HL7/FHIR standard şi Web services SOA environment fără a se limita la aceasta.

A.1.41 Soluţia trebuie să permită alocarea de coduri ICD-10 (sau ICD 11, daca se va trece la aceasta versiune) pacienţilor folosind nume (configurabile) de proceduri şi boli. Dacă lista de boli şi proceduri nu include o componentă, aceasta trebuie să poată fi adăugată imediat de un key-user.

A.1.42 Soluţia trebuie să permită crearea temporară a unei înregistrări a pacientului în eventualitatea indisponibilităţii sistemului informatic de gestiune pacient al spitalelor (sisteme informatice de tip HIS).

A.1.43 Soluţia trebuie să ofere posibilitatea de a înregistra informaţiile de contact ale rudelor apropiate, tutori, apartinatori.

A.1.44 Soluţia trebuie să asigure disponibilitatea funcţiilor integrate de administrare centralizată a sistemului, pentru definirea, controlul şi optimizarea funcţionării acestuia.

A.1.45 Formularele electronice trebuie să poată fi configurate pentru utilizarea de terminologii standard, specifice, conforme cu normele unităţii spitaliceşti sau secţiei cu scopul prevenirii erorilor şi facilitării statisticilor şi controlului de calitate.

A.1.46 Formularele electronice trebuie să poată fi configurate în ce priveşte culoarea, selecţia de parametri, mărimea şi localizarea textului şi câmpurilor.

A.1.47 Soluţia trebuie să permită crearea de secţiuni dependente de context în cadrul formularelor, astfel încât, de exemplu pe formularul de internare, pentru un pacient cu arsuri va apărea un anumit tip de informaţii, în timp ce pentru un pacient cu alt tip de urgenţă vor apărea alte tipuri de informaţii.

A.1.48 Soluţia trebuie să permită definirea unor câmpuri obligatorii de completat în fişa pacientului. Înainte de externarea (mutarea) unui pacient, soluţia trebuie să semnaleze toate câmpurile obligatorii care nu au fost completate;

A.1.49 Soluţia trebuie să permită configurarea de shortcut-uri, meniuri, butoane generatoare de activităţi, alarme şi mesaje de alertă de către utilizatori autorizaţi şi calificaţi.

A.1.50 Soluţia trebuie să permită plasarea unor astfel de butoane şi shortcut-uri în diferite formulare şi ecrane astfel încât diferite părţi ale soluţiei să fie legate între ele şi să facă parte dintr-un proces continuu şi să permită accesarea unor legături intranet sau internet sau să efectueze acţiuni precum prescrierea unor reţete – indicaţii medicale predefinite.

A.1.51 Soluţia trebuie să permită adăugarea de parametri în ecrane / diagrame de către utilizatorii sistemului.

A.1.52 Soluţia trebuie să permită configurarea parametrilor de semne vitale, ecranelor aferente, diagramelor, tendinţelor, şi a altor elemente solicitate de către utilizatori autorizaţi şi calificaţi în operarea soluţiei fără a necesita programare/dezvoltare.

A.1.53 Soluţia trebuie să permită adăugarea de parametri într-un grafic, precum şi configurarea acestuia (formă, culoare şi scara folosită) de către utilizatorii sistemului fără a necesita programare/dezvoltare.

A.1.54 Soluţia trebuie să permită accesarea neîntreruptă a dosarului (fişei) pacientului. Înregistrările vor fi arhivate numai după externarea (mutarea) pacientului din secţie. Soluţia trebuie să ofere capabilităţi de arhivare conform politicilor de retentie stabilite la nivel legal, iar arhiva trebuie să conţină un set de date predefinit şi relevant.

A.1.55 Colectarea datelor nu trebuie să fie dependentă de modelul aparaturii medicale din secţie, astfel încât înlocuirea unui echipament medical pe viitor să nu influenţeze în nici un fel funcţionarea soluţiei. În acelaşi timp însă, soluţia trebuie să fie compatibilă cu aparatura medicală existentă în secţie în momentul implementării soluţiei.

A.1.56 Soluţia trebuie să permită unui key-user să poată crea formulare solicitate de utilizatori conform cu necesităţile. Formularele vor putea fi deschise cu uşurinţă cu butoane şi meniuri shortcut (fără a trece prin meniuri succesive). Se vor putea configura diverse opţiuni pentru activarea formularelor pentru date specifice. Se vor putea crea formulare dinamice de către utilizatori, de exemplu: unei anumite prescripţii i se va putea ataşa un formular care să întrebe dacă un anumit medicament a fost administrat înainte de internarea la ATI. Dacă răspunsul este afirmativ, formularul dinamic va genera automat rubrici referitoare la tip, doză, durata administrării, etc. În plus, se vor putea adăuga legături la documente externe care să conţină informaţii privind medicamentele utilizate, dozaje maximale, interacţiuni cu alte medicamente, etc.

A.1.57 Soluţia trebuie să ofere utilizatorilor diferite tipuri de machete definite pe tip de utilizator sau procedură.

A.1.58 Soluţia trebuie să pună la dispoziţia utilizatorilor un tablou de ansamblu al secţiei care să ofere informaţii actualizate şi sincronizate despre toţi pacienţii secţiei şi posibilitatea de a afişa tabloul de ansamblu pe un ecran de dimensiuni mari.

A.1.59 Soluţia trebuie să permită o vizualizare a informaţiilor din cadrul unei secţii accesibilă pe web şi dispozitive mobile din spital sau din afara lui doar de catre medicul curant în conformitate cu politicile de securitate a datelor din spital, a respectării drepturilor pacientului şi a drepturilor utilizatorului.

A.1.60 Soluţia trebuie să ofere înregistrarea automată la un anumit interval de timp de maxim 90 de secunde (a tuturor parametrilor măsuraţi de către toate aparatele medicale existente conectate la pacientul din patul de terapie intensivă, de exemplu monitorul de funcţii vitale, ventilator, pompe volumetrice, seringi electrice, aparat de hemofiltrare / hemodializă, alte tipuri de monitoare). Toate aceste date vor fi afişate, analizate, raportate şi salvate în baza de date automat, fără intervenţia utilizatorului.

A.1.61 Soluția trebuie să ofere un modul de triaj astfel încât utilizatorul să poată să stabilească/prioritizeze urgența/gravitatea cazului. Acest modul trebuie să conțină:

- Un set predefinit de opțiuni (de exemplu: durere de cap, hemoragie, durere în piept, fractură etc..);

- Un flux predefinit care, după alegerea unei opțiuni (de exemplu: durere de cap), să genereze un alt set de opțiuni predefinite legate de afecțiunea ”durere de cap”.

Modulul de triaj trebuie să poată genera automat urgența/gravitatea cazului prin afișarea unei culori sau a unui număr (de exemplu: roșu/1 pentru cazurile grave) și să ofere posibilitatea de a personaliza atât setul de opțiuni cât și fluxul.

I.2.1.2.1. Cerinţe specifice componentei pentru secţiile ATI cu paturi

A.1.62 Soluţia trebuie să ofere managementul planului de tratament (order management) – medicaţie, fluide, tratamente (partea de comenzi de la faza de planificare, semnalizare, validare comandă, urmărire comandă). Soluţia trebuie să ofere documentaţia/înregistrarea medicaţiei primită de pacient înainte de internare (transfer din altă secţie, reinternare) şi vizualizarea ei într-un format optim pentru a fi luată în consideraţie la stabilirea conduitei terapeutice.

A.1.63 Soluţia trebuie să ofere realizarea înregistrării şi editării tratamentelor precum şi a modului de administrare. Trebuie să permită înregistrarea şi editarea tuturor detaliilor relevante: cale de administrare, dozaj, frecvenţa, când începe administrarea, precum şi alte atribute specifice.

A.1.64 Soluţia trebuie să ofere posibilitatea calculării automate a raportului între dozaj şi parametrii pompei volumetrice sau seringii electrice şi, în funcţie de prescripţia primită, să poată schimba automat formatul şi dirija personalul medical pentru adăugarea datelor lipsă.

A.1.65 Soluția trebuie să poată fi integrată cu seringile electrice și pompele de perfuzie (acolo unde aceste echipamente medicale din dotare, permit) astfel încât, prescripția sau modificările efectuate în sistem să apară direct în echipamentele medicale respective și vice versa.

A.1.66 Soluţia trebuie să ofere configurarea de metode de prescriere predefinite pentru fiecare medicament în parte. Configurarea trebuie să includă: doza, viteza de administrare, concentraţia, soluţia de diluare, setările pompei şi numărul de administrări zilnice.

A.1.67 Utilizatorii autorizați trebuie să poată vedea lista curentă de prescripţii a pacientului şi vor putea să modifice planul de tratament direct.

A.1.68 Soluţia trebuie să permită managementul dozelor zilnice administrate de medicamente şi alte substanţe (soluţii lichidiene, componente de sânge, etc.) prin afişarea acestora, informând/alertand utilizatorii de posibilele consecinţe asupra pacientului în cazul modificării dozelor, înainte de a opera aceste modificări.

A.1.69 Prescripţiile trebuie să poată fi selectate din meniuri tip drop-down care asigură claritatea necesară şi previn posibile erori cu consecinţe asupra pacientului. În plus, medicamentele şi dozajele uzuale pot fi înregistrate cu un simplu buton (pe ecran) iar dozajele mari sau neobişnuite pot fi separate şi eventual blocate.

A.1.70 Pentru anumite situaţii (circumstanţe clinice speciale) trebuie să poată fi pre-definite protocoale de tratament şi, la nevoie, activate (înregistrate) cu un simplu click de mouse.

A.1.71 Soluţia trebuie să ofere o funcţionalitate, de tip jurnal electronic de prescripţii, care să permită informarea permanentă a utilizatorilor asupra stadiului prescripţiei. Trebuie să poată fi utilizat pentru a vedea fazele următoare ale prescripţiei (medicaţie, proceduri, doze etc.) şi a valida ce s-a executat deja. Prescripţiile vor fi afişate în culori diferite, în funcţie de momentul la care trebuie executate. Trebuie să permită afişarea tuturor prescripţiilor planificate (ce urmează a fi executate) într-o listă uşor de urmărit, iar momentul administrării unei prescripţii trebuie să fie semnalat, de exemplu, printr-o imagine pulsând pe ecran (atenţionare).

A.1.72 Soluţia trebuie să permită configurarea listelor de medicamente pe necesităţi, de exemplu, lista de medicamente prescrisă de medic, diagrama zilnică, predarea-primirea la schimbarea turei asistentelor, etc..

A.1.73 Soluţia trebuie să aibă posibilitatea de a prescrie tratamente standard complexe în care componentele individuale sunt dependente de timp. Tratamentele standard trebuie să fie customizabile.

A.1.74 Soluţia trebuie să permită prescrierea de medicamente care nu există în gestiunea spitalului (se va interconecta cu solutiile informatice de gestionare a stocurilor de medicamente).

A.1.75 Soluţia trebuie să permită accesarea de informaţii despre medicamentele prescrise urmărind un link intern sau extern direct din lista de prescriere.

A.1.76 Soluţia trebuie să ofere suport pentru stabilirea dozajului medicaţiei unui pacient.

A.1.77 Soluția trebuie să aibă funcționalitatea de a configura prescripţiile predefinite şi mecanisme de prevenire a erorilor umane.

A.1.78 Soluţia trebuie să permită evidenţa pacienţilor alergici la medicamente sau alte ingrediente. La înregistrarea în sistem a unei prescripţii, trebuie ca user-ul să fie notificat dacă pacientul este alergic la produsul administrat, care poate fi o substanţă sau un grup de substanţe (de exemplu: latex, penicilină, sulfamide). Modul de notificare trebuie să fie parametrizabil şi să poată fi configurat pentru a reflecta severitatea eventualei reacţii alergice. În acest fel, personalul va putea lua decizii bine documentate, evitând potenţiale riscuri.

A.1.79 Soluţia trebuie să permită alertarea prescrierii unui medicament dacă este înregistrată o alergie la acest medicament. Soluţia trebuie să aibă funcţionalitatea de a oferi diferite opţiuni de răspuns la atenţionarea unei alergii precum: prevenţia completă şi necesitatea co-semnăturii.

A.1.80 Soluţia trebuie să permită aprobarea (validarea) prescripţiilor în mod centralizat. Astfel, se permite farmacistului sau unui alt medic să vizualizeze toate prescripţiile ce urmează a fi executate în unitatea de ATI. Trebuie să permită aprobarea retroactivă sau aprobarea prescripţiilor de către medici care nu sunt prezenţi în secţie la momentul respectiv. Personalul cu drepturi de acces (asistente, medici) vor introduce în sistem (înregistra) aceste prescripţii împreună cu numele medicului care le-a emis (semnat). Soluţia trebuie să ofere funcţionalitatea de configurare a prescripţiilor ce necesită dublă semnătură (de exemplu: medic curant şi şeful de secţie), inclusiv funcţionalitatea de configurare a co-semnăturilor obligatorii pentru anumite prescripţii specifice.

A.1.81 Trebuie să existe o listă de prescripţii disponibilă permanent pentru vizualizare, analiza şi luarea de decizii terapeutice pentru prescripţiile înregistrate şi modificarea planului de tratament. Lista va conţine detaliile prescripţiei, filtre şi va permite sortarea după diverse criterii pentru a oferi o imagine de ansamblu asupra tuturor medicaţiilor şi procedurilor executate la un pacient. Prescripţiile în derulare sau deja executate vor putea fi afişate, fie tabelar, fie în formă grafică (diagrama Gantt) şi vor putea fi grupate în categorii pre-definite de unitatea ATI respectivă.

A.1.82 Soluţia trebuie să permită crearea unei liste de probleme multidisciplinare pentru urmărirea problemelor pacientului pe etape cronologice. Lista va fi completată de tot personalul spitalului implicat în cazul respectiv şi trebuie să aibă 2 secţiuni: probleme active şi probleme de fond, identificate distinct. Problemele noi, ce nu au fost încă introduse pe listă, vor putea fi adăugate pe măsură ce apar în lista permanentă.

A.1.83 Soluţia trebuie să permită configurarea unei liste de activităţi per pacient pentru fiecare secţie sau utilizator. Lista de activităţi pe secţie trebuie să poată fi configurată, de exemplu: să includă toate sarcinile uzuale secţiei sau numai cele dorite, pentru toţi pacienţii din secţie sau doar pentru anumiţi pacienţi. De asemenea, soluţia trebuie să afişeze o notificare către utilizatori referitor la necesitatea unei acţiuni ce trebuie întreprinsă.

A.1.84 Soluţia trebuie să permită calcularea automată a unor scoruri uzuale simple gen Glasgow şi afişarea lor la intervale regulate.

A.1.85 Soluţia trebuie să permită calcularea automată a unor scoruri complexe destinate în special pacienţilor de anstezie-terapie intensivă (APACHE II, SAPSII, OMEGA-RO, TISS, etc.).

A.1.86 Soluţia trebuie să permită generarea de documente în format text uzual, pentru diverse observaţii asupra pacientului. Se vor putea crea note de progres, note din discuţiile cu familia, diverse rapoarte periodice etc.

A.1.87 Soluţia trebuie să permită crearea de documente standard (templates) ce vor putea fi utilizate în scopuri ce necesită formate des utilizate.

A.1.88 Soluţia poate să permită generarea unui plan de îngrijire care să ghideze pe toţi cei implicaţi în îngrijirea pacientului în cauză, să permită identificarea de posibile probleme şi să permită documentarea simptomelor şi cauzele acestora. Se vor putea defini scopurile urmărite în cazul

fiecărei probleme, intervenţiile în caz de apariţie a problemei şi de asemenea se va putea defini un moment de evaluare.

A.1.89 Soluția trebuie să aibă un modul de îngrijire a plăgilor/rănilor și a cateterelor/drenajelor cu afișaj grafic al pacientului, al plăgilor/rănilor și al cateterelor/drenajelor.

A.1.90 Soluția trebuie să aibă modul de calculare a balanței fluidelor configurabil ca timp și componente.

A.1.91 Soluția trebuie să conțină în cadrul soluției de ATI un modul de Neonatologie.

A.1.92 Soluția trebuie să aibă integrat modulul de neonatologie în aceeași bază de date și să folosească aceeași interfața.

A.1.93 Soluția trebuie să permită utilizatorului după autentificare (login) să vizualizeze vârsta gestațională, zilele de spitalizare și varsta în zile. Privirea de ansamblu (ecranul principal) trebuie să poată fi reconfigurată/personalizată în funcție de cerințele utilizatorului și /sau ale unui grup de utilizatori.

A.1.94 Soluția trebuie să permită definirea și directionarea proceselor, cum ar fi de exemplu: internarea, date relevante financiare, stocarea procedurilor standard de operare (clinice și interne).

A.1.95 Soluția trebuie să permită stocarea schemelor standard pentru diagnostice, terapii și fluxuri de lucru specifice.

A.1.96 Soluția trebuie să permită introducerea datei ultimei menstruații și să poată calcula data probabilă de naștere, dar și vice versa.

A.1.97 Soluția trebuie să aibă un instrument pentru prescripția medicației/protocoalelor și a nutriției neonatale zilnice. Cu acest instrument trebuie să se poată introduce diferite dozaje/diferite viteze (ml / h, ml / kg / d, mcg / kg / min, etc).

A.1.98 Soluția trebuie să aibă un instrument care să conțină modele (template-uri) și să păstreze un istoric.

A.1.99 Soluția trebuie să permită folosirea diferitelor unități de greutate/masură per pacient.

A.1.100 În procesul de prescripție soluția trebuie să indice cantitățile substanțelor active cu o valoare țintă (exactă).

A.1.101 Soluția trebuie să permită customizarea vizualizării ecranelor, specifice neonatologiei.

A.1.102 Soluția trebuie să permită crearea liberă a balanțelor fluidice și a componentelor.

A.1.103 Soluția trebuie să includă un instrument pentru generarea automată de rapoarte neonatologice.

A.1.104 Soluția trebuie să includă percentilele (sex, varsta, inaltime, greutate etc) pentru diferitele gupe de vârstă în conformitate cu standardul WHO (World Health Organization/Organizația Mondială a Sănătății). Integrarea percentilelor naționale sau specifice spitalelor, să fie posibilă.

A.1.105 Soluția trebuie să aibă modul de îngrijire a plăgilor/rănilor pentru neonatologie.

I.2.1.2.2. Cerinţe specifice SO (Sala Operatie)

Funcţionalităţi necesare etapei pre-operator:

A.1.106 Personalul medical trebuie să poată introduce date clinice, personale, demografice ale pacientului şi să poată planifica medicaţia pre-operatorie folosind formulare online;

A.1.107 Documentaţia pre-operator trebuie să poată fi completată din orice loc cu acces la internet intranet, aplicaţie web-based. Astfel colectarea de informaţie din mai multe locuri trebuie făcută simplu şi rapid, iar toate datele medicale ale pacientului înregistrate anterior operaţiei trebuie să fie disponibile în timpul anesteziei;

A.1.108 Soluția trebuie să utilizeze câmpuri obligatorii predefinite pentru valorile importante (ex: alergii).

A.1.109 Soluția trebuie să poată transfera/genera fără probleme fluxul de informații (toate valorile, observațiile și parametrii) atunci când se efectuează transferul pacientului din secția de ATI în camera de inducție și apoi în sala de operație.

Funcţionalităţi necesare etapei intra-operator

A.1.110 Soluția trebuie să furnizeze un concept de flux de lucru pentru a predefini diverse proceduri astfel încât să ușureze pornirea intervenției.

A.1.111 Pentru siguranța pacientului, soluția trebuie să furnizeze standardele de siguranță WHO (Organizația Mondială a Sănătății) în materie de personal, timp, activități. Utilizatorii trebuie să fie obligați de către sistem să completeze acești pași.

A.1.112 Să permită monitorizarea şi afişarea în diverse modalităţi configurabile după necesităţi, a parametrilor necesari utilizatorului (de exemplu: medicului anestezist, asistente) în diversele etape ale operaţiei.

A.1.113 Să permită configurarea şi crearea de diverse modele pentru afişarea celor mai relevante date pentru procedura în desfăşurare.

A.1.114 Soluţia trebuie să permită monitorizarea şi înregistrarea medicamentelor şi fluidelor administrate importante pentru un utilizator (de exemplu: medicul anestezist, asistentă). Urmărirea trebuie să fie posibilă cu un singur click şi să se poată alege modul afişarii: tabelar sau sub formă grafică.

A.1.115 Soluţia trebuie să permită vizualizarea pe un ecran principal de stări şi faze cu informaţie vitală, în permanenţă. Maniera de afişare, tipurile de parametri, gruparea acestora pe display, formularele şi tabelele toate trebuie să fie configurabile, astfel încât fiecare utilizator să îşi poată crea un mod propriu de utilizare a datelor din sistem.

A.1.116 Soluţia trebuie să permită determinarea cu precizie a momentului efectuării unei manevre printr-un cursor de timp (electronic) vertical care apare la atingerea unui obiect sau fereastră de pe ecran. Din acest moment orice manevră efectuată (administrare de medicaţie, fluide, evenimente, alţi parametri) va fi înregistrată împreună cu momentul (ora) exact al producerii.

A.1.117 Soluţia trebuie să permită vizualizarea pe un ecran principal a următoarelor obiecte pre-definite: tabel, grafic, medicamente-fluide şi evenimente. Fiecare din aceste obiecte va dispune de un mod de prezentare a informaţiilor şi selectare a parametrilor, configurabil şi variabil. Pentru acces rapid fiecare obiect va putea fi manevrat grafic (de exemplu: stoparea administrării unui fluid să se poată face prin indicarea fluidului şi apăsarea unui buton de tip stop).

A.1.118 Soluţia trebuie să permită vizualizarea şi analiza evoluţiei valorilor unor parametri configuraţi de utilizatori pentru o perioadă de timp aleasă. Trebuie să se poată face comparaţii între parametri. Vor fi posibile o multitudine de opţiuni grafice, scale, culori, statistici pre-definite sau configurate local etc.

A.1.119 Soluţia trebuie să permită monitorizarea administrării de substanţe şi medicamente, precum şi intervenţia rapidă pentru schimbarea dozelor, a vitezei de administrare etc. Trebuie să se poată afişa fie grafic, fie tabelar, medicamentele şi fluidele administrate deja sau care se administrează la un moment dat şi să existe şi opţiunea să fie grupate pe categorii specifice unităţii medicale.

A.1.120 Soluţia trebuie să permită configurarea, la alegere, a structurii bilanţului fluidic, a celui energetic sau nutriţional şi a oricăror alte echilibre de către utilizatori calificaţi şi autorizaţi. Toate aceste configurări trebuie să fie posibile fără dezvoltări de software sau programări suplimentare.

A.1.121 Soluţia trebuie să permită calcularea şi afişarea echilibrului nutrienţilor, precum: glucoză, sodiu, potasiu etc.

A.1.122 Soluţia trebuie să permită vizualizarea continuă sau la cerere a unor evenimente specifice SO. Vor exista mai multe opţiuni de vizualizare, de exemplu: oprirea vizualizării continue a unui eveniment pentru a i se ataşa un formular electronic pentru documentarea evoluţiei unui caz. Trebuie să permită prezentarea de evenimente din timpul operaţiei, de exemplu: începutul sau terminarea anesteziei.

A.1.123 Soluţia trebuie să permită vizualizarea, de exemplu, sub formă de listă, unor acţiuni şi documentări efectuate, cum ar fi: date colectate de la aparatele medicale, documentarea procedurilor în formulare, documentarea evenimentelor clinice (de exemplu: începutul şi sfârşitul intervenţiei chirurgicale).

A.1.124 Soluţia trebuie să permită configurarea datelor prezente pe ecran, care va putea fi făcută după tipuri de operaţii sau tipuri de utilizator (medic anestezist, asistentă etc.).

Funcţionalităţi necesare etapei post-operator

A.1.125 Soluţia trebuie să se asigure continuarea coerentă a urmării evoluţiei pacientului după operaţie în oricare dintre subunităţile secţiei ATI cu paturi.

A.1.126 Soluția trebuie să furnizeze continuu informațiile (venite din sala de operație) de la seringile electrice, pompele de infuzie pornite și de la noile catetere/drenaje, în secția cu paturi ATI. Valorile balanței fluidelor și a parametrilor vitali trebuie să fie și ele disponibile în același mod.

I.2.1.2.3. Cerinţe pentru solutia de gestiune şi securitate acces utilizatori

A.1.127 Soluţia trebuie să poată interfaţa cu Microsoft Active Directory sau alte servicii similare, pentru autentificare utilizatori.

A.1.128 Soluţia trebuie să asigure navigarea facilă în şi între toate modulele şi accesarea tuturor funcţiilor şi comenzilor la care utilizatorul are acordate drepturi în cadrul aceleiaşi sesiuni de lucru, adică fără să fie necesară deconectarea şi reconectarea ca utilizator al aplicaţiei.

A.1.129 Soluţia trebuie să includă un mecanism de auto-logout.

A.1.130 Soluţia trebuie să permită urmărirea accesărilor în sistem şi generarea de rapoarte automate cu privire la acestea.

A.1.131 Soluția trebuie să permită anonimizarea unor pacienți specifici, pentru toți utilizatorii sau pentru un anumit grup de utilizatori/medici.

A.1.132 Soluţia trebuie să asigure posibilitatea ca orice utilizator din cadrul spitalului să poată accesa orice informaţie conform cu autorizarea de securitate, în funcţie de necesităţi şi de procedurile interne ale spitalului.

A.1.133 Soluţia trebuie să ofere posibilităţi de interogare a datelor printr-o interfaţă user-friendly care să permită utilizarea/accesul facil şi de către utilizatori fără experienţă în programare.

A.1.134 Soluţia trebuie să ofere posibilitatea ca toate configurările şi personalizările să poată fi făcute de către utilizatori autorizaţi şi instruiţi, fără a fi necesare cunoştinţe de programare.

A.1.135 Soluţia trebuie să ofere posibilitatea unui key-user să adauge noi parametri, să reconfigureze diagramele sau graficele (adăugare parametri, formă, culori, scală). Această configurare trebuie să revină la setările iniţiale la ieşirea utilizatorului din sistem.

A.1.136 Soluţia trebuie să ofere posibilitatea utilizatorilor fără cunoştinţe speciale de programare să folosească modulul de configurare al soluţiei.

A.1.137 Soluţia trebuie să ofere posibilitatea utilizatorilor prin modulul de configurare să definească plauzibilitatea sau completitudinea valorilor pentru diferite câmpuri. Trebuie să se poată defini câmpuri obligatorii pentru completarea unui formular şi câmpuri care trebuie completate în fişa pacientului până la externare.

A.1.138 Soluţia trebuie să asigure confidenţialitatea şi securitatea informaţiilor, atât în cadrul proceselor de transfer de date cât şi pentru monitorizarea accesului utilizatorilor la toate resursele sistemului, personalizat în funcţie de responsabilităţile şi drepturile specifice, asigurate printr-un sistem de drepturi şi parole de acces la nivel de: utilizator, funcţie, modul. În acest sens, soluţia trebuie să integreze funcţionalităţi de administrare, şi anume:

- întreţinere utilizatori;
- optimizare;
- acces de la distanţă la sistem în scopul recuperării datelor după erori severe datorate unor evenimente deosebite.

A.1.139 Key-userii trebuie să poată personaliza soluţia pentru diverse situaţii specifice.

A.1.140 Soluţia trebuie să asigure accesul în sistem, diferenţiat pentru fiecare utilizator, în funcţie de categoria din care face parte, pe baza unui nume unic şi a unei parole, de exemplu: utilizator de tip X care poate prescrie medicament A, dar nu şi medicament B, utilizatorul Y poate co-semna numai un anumit grup de medicamante, în timp ce utilizator Z nu poate decat să prescrie medicamentaţie. Sistemul va permite utilizarea de tehnologii de autentificare moderne.

A.1.141 Soluţia trebuie să asigure administrarea centralizată şi securizată a informaţiilor de acces;

A.1.142 Soluţia trebuie să conţină aplicaţiile necesare pentru asigurarea accesului personalului autorizat la informaţiile puse la dispoziţia acestora de către spital;

A.1.143 Soluţia trebuie să permită definirea unei perioade standard de inactivitate a unui utilizator logat, după care va face logout automat.

A.1.144 Soluţia nu trebuie să permită marcarea pentru ştergere a unor date dacă acestea sunt folosite în diverse tranzacţii, altele decât cele curente. Sistemul nu va permite ştergerea datelor, ci doar marcarea acestora ca şterse şi păstrarea lor în logurile aplicaţiei.

A.1.145 Soluţia trebuie să asigure respectarea protecţiei informaţiilor cu caracter personal şi confidenţial conform actelor normative în vigoare şi recomandărilor naționale cât și ale Uniunii Europene;

A.1.146 Key-userii trebuie să poată limita accesul neautorizat al anumitor utilizatori la date ale unui pacient (pentru cazurile sensibile: persoane publice etc.).

A.1.147 Soluţia trebuie să permită anonimizarea datelor pacientului.

A.1.148 Soluţia trebuie să permită 3 (trei) niveluri de acces:

- **acces total**: orice dosar de pacient poate fi vizualizat şi editat;
- **acces read-only**: datele pacientului pot fi văzute, dar nu pot fi editate;
- **no access**: un pacient poate cere restricţionarea accesului unui anumit utilizator la datele sale.

A.1.149 Soluţia trebuie să includă mecanisme care să permită accesul la date şi informaţii pentru personalul autorizat din mai multe secţii, pe 3 niveluri:

- **secţie-secţie:** pacientul transferat de la o secţie la alta (în cadrul aceluiași spital). Personalul din secţia primitoare va putea să vadă parţial sau integral în funcție de permisiunile primite de acesta din partea pacientului, dosarul electronic cu datele pacientului (de exemplu: personalul ATI poate vedea datele colectate atunci când pacientul a fost operat);
- **medic-secţie:** medicii vor putea să vadă dosarul unui pacient transferat succesiv la mai multe secţii ale spitalului. Dacă de exemplu un pacient tratat la ATI este trimis la operaţie (altă secţie) medicul să poată vedea dosarul de la SO chiar dacă nu există acces secţie-secţie;
- **permisiune pacient:** pacientul va putea să ceară limitarea accesului la datele sale, nivelul de prioritate să fie deasupra celor 2 anterioare (chiar dacă există acces secţie-secţie, dreptul pacientului prevalează). Key-userii vor putea să stabilască ce personal are acces la dosar şi niciun alt utilizator să nu îl poate accesa, indiferent de drepturile sale generale de acces.

A.1.150 Soluţia trebuie să permită 3 opţiuni de configurare pentru controlul accesului la datele pacientului, după externarea pacientului din secţiile gestionate de soluţia de ATI +SO:

- **total interzis**: nici un fel de date nu mai pot fi adăugate, indiferent de drepturile de acces;
- **parţial interzis**: după externare se pot adăuga formulare electronice la dosar, atât în baza de date curentă cât şi în baza de date arhivă;
- **permis**: se pot adăuga orice fel de date în dosarul pacientului după externare, atâta timp cât pacientul figurează în baza de date de producţie (activă). Dacă dosarul este transferat în baza de date arhivă, orice acces este interzis.

A.1.151 Soluţia trebuie să permită acordarea de niveluri diferite de acces pentru grupuri diferite de utilizatori pentru acţiuni specifice, sau pentru a prescrie anumite categorii de medicamente.

A.1.152 Soluţia trebuie să permită adăugarea de noi utilizatori, precum şi controlul drepturilor fiecărui utilizator de către utilizatori autorizaţi şi calificaţi.

A.1.153 Soluţia trebuie să permită mai multor utilizatori să se conecteze şi să introducă date simultan pentru acelaşi pacient.

A.1.154 Soluţia trebuie să ofere posibilitatea monitorizării intrărilor în sistem şi acţiunilor efectuate, de exemplu: ce utilizator a accesat datele cărui pacient, când, pentru cât timp, care sunt utilizatorii care au vizualizat datele pacientului x, datele căror pacienţi au fost accesate de utilizatorul y, etc. Toate activităţile utilizatorilor (între log-în şi log-out) vor putea fi înregistrate în fişierul de loguri al sistemului şi sunt astfel clar şi complet trasabile (de exemplu: ce operaţie s-a efectuat, la ce moment de timp). Datele nu vor putea fi şterse complet din sistem (din raţiuni medico-legale). Datele introduse greşit de către utilizatori se vor marca ca atare, se vor scrie altele, dar nu vor fi complet şterse. Astfel orice acţiune va putea fi identificată la un moment ulterior efectuării ei deoarece toate modificările vor rămâne în baza de date.

A.1.155 Soluţia trebuie să asigure integritatea şi nealterarea datelor şi a aplicaţiilor software.

A.1.156 Soluţia trebuie să asigure aplicaţiile necesare pentru a preveni atacurile electronice asupra sistemului spitalului;

I.2.1.2.4. Cerinţe de raportare operationala in aplicatie

A.1.157 Sistemul trebuie să realizeze nu numai procesarea datelor ci şi generarea de informaţii – suport pentru luarea deciziilor şi fundamentarea politicilor.
A.1.158 Soluţia trebuie să permită generarea de rapoarte periodice pe baza informaţiilor din baza de date
A.1.159 Soluţia trebuie să ofere posibilitatea accesării de informaţii sintetice, de exemplu: datele pacientului, necesare pentru cercetare, statistici, suport decizie, auditare. Datele obţinute să poată fi prelucrate în formate uzuale (de tip: Word, Excel, Access, sau echivalent) pentru statistici, grafice, situaţii. Sistemul trebuie să ofere o modalitate de emitere de rapoarte în formate care nu permit editarea (read-only) şi să permită exportul rapoartelor către aplicaţii externe.
A.1.160 Soluţia trebuie să permită crearea/tiparirea de rapoarte personalizabile pe baza datelor din sistem, de exemplu, date din sistemul informatic general al spitalului, datele pacientului, istoricul acestuia, imagini, date demografice, poate extrage date din dosarul electronic al pacientului (dacă există) cum ar fi: parametri, evenimente, tratamente, scoruri etc.
A.1.161 Soluţia trebuie să aibă capabilităti de tip „point and click" pentru accesare de rapoarte.
A.1.162 Soluţia trebuie să ofere posibilitatea semnalării de evenimente, posibilitatea adăugării unei componente de management al evenimentelor configurabile de către utilizator. Trebuie să poată emite o notificare (alertă) când un set de condiţii este îndeplinit, de exemplu: puls mai mare de 120 bătăi pe minut şi tensiune sistolică mai mică de 90 mmHg simultan. Fiecare eveniment este constituit dintr-un set de condiţii extrase din parametrii măsuraţi de aparatura de la pat, rezultate de laborator, diagnostice şi medicaţia pacientului. Odată un astfel de eveniment identificat, un mesaj detaliat (configurabil de către un key-user) apare pe ecran sau se poate trimite pe e-mail, SMS sau alte suporturi de comunicaţii.
A.1.163 Soluţia trebuie să includă un modul centralizat de comunicaţii şi management care să pună la dispoziţia utilizatorilor informaţii clare şi de încredere dintr-o sursă centrală. Va include funcţiile (configurabile după necesităţi):
- Căsuţă poştală pentru comunicarea cu ceilalţi utilizatori ai sistemului;
- Atenţionare pentru semnalizare prescripţiilor în aşteptare, imediate sau întârziate;
- Laborator –anunţă utilizatorul asupra intrării în sistem a datelor de laborator;
- Notificare evaluare – în cazul planurilor de îngrijire personalizate, utilizatorii sunt atenţionaţi asupra momentelor de evaluare prestabilite în planul de îngrijire.

Datorită aplicabilității critice a aplicației ATI+SO, aplicația trebuie să aibă referințe de implementare naționale/internaționale în medii de ATI și Săli de Operație. Nu vor fi acceptate soluții care se dezvoltă custom specific pentru acest proiect. Se va face dovada existenței aplicației prin organizarea unei sesiuni demo în cadrul perioadei de evaluare a ofertelor.

I.2.1.2.5. Modulul de transfer de date între aplicații (integrare ATI-HIS)

1) Soluția trebuie să conțină un sistem independent de mesagerie între aplicații care să permită interoperabilitatea cu aplicațiile medicale deja existente în cadrul spitalelor acolo unde există această funcționalitate.
2) Sistemul de mesagerie trebuie să permită interoperabilitatea aplicațiilor informatice prin abonarea acestor aplicații la anumite mesaje sau tipuri de mesaje.
3) Soluția trebuie să prezinte un sistem de mesagerie între aplicații care să fie independent, deschis, scalabil, bazat pe standarde și protocoale de comunicație internaționale (de exemplu HL7) specifice domeniului medical, care să fie capabil să transmită mesaje între sisteme medicale.
4) Soluția trebuie să asigure, prin sistemul independent de mesagerie, transferul mesajelor între aplicații. Datele de interes care se vor transfera între aplicații prin sistemul de mesagerie independent sunt reprezentate de datele de identificare și demografice ale pacientului, informațiile privind medicația și consumul de materiale sanitare, informațiile referitoare la analizele de laborator, informații privind procedurile efectuate în cadrul spitalului.
5) Sistemul independent de mesagerie între aplicații va permite implementarea unor seturi predefinite de reguli pentru validarea mesajelor.

6) Sistemul independent de mesagerie între aplicații trebuie să aibă o interfață de administrare intuitivă și prietenoasă cu key-userii.
7) Sistemul independent de mesagerie între aplicații, având în vedere natura informațiilor pe care le gestionează, va trebui să implementeze un mecanism de securitate care să permită transmiterea mesajelor doar către aplicațiile care trebuie să le receptioneze. Toate operațiunile desfașurate la nivelul sistemului independent de transmitere a mesajelor se înregistrează într-o componentă de jurnalizare a sistemului, astfel încât să fie posibilă auditarea ușoară de către key-useri.
8) Soluția trebuie să conțină un sistem de stocare, gestionare și publicare a nomenclatoarelor.
9) Sistemul trebuie să prezinte o arhitectură software bazată pe servicii de acces.
10) Sistemul de stocare, gestionare și publicare a nomenclatoarelor va dispune de o interfață de administrare intuitivă și prietenoasă cu key-userii. Acest sistem va fi capabil să funcționeze independent de sistemele informatice deservite și va avea capacitatea de deservire în paralel a unuia sau mai multor sisteme informatice.
11) Gestionarea nomenclatoarelor în cadrul sistemului trebuie să permită:
    - Adăugarea, stocarea, editarea/actualizarea și inactivarea nomenclatoarelor și/sau a valorilor stocate în cadrul nomenclatoarelor;
    - Versionarea nomenclatoarelor și/sau a valorilor stocate în cadrul nomenclatoarelor;
    - Popularea/actualizarea nomenclatoarelor prin metode diverse: import, adăugare manuală etc;
    - Gestionarea diferitelor tipuri de nomenclatoare: nomenclatoare cu structură publică (publicate de către diverse instituții din domeniul sanatatii etc.), nomenclatoare specifice unuia sau mai multor sisteme deservite etc.
12) Sistemul trebuie să includă funcționalități de abonare a sistemelor de actualizare a diferitelor nomenclatoare ale altor sisteme externe la date și un mecanism de verificare, autorizare și furnizare a datelor în funcție de permisiunile de acces stabilite.
13) Sistemul de stocare, gestionare și publicare a nomenclatoarelor trebuie să includă un mecanism de securitate atât în ceea ce privește publicarea datelor către mediul extern, cât și autorizarea accesului la conținut. Mecanismul de securitate va include funcționalități referitoare la:
    - - Asigurarea securității de acces la nomenclatoare
    - - Configurarea nivelului de acces a sistemelor abonate la nomenclatoare
    - - Configurarea nivelului de acces a fiecărui abonat la nivel de valoare/item din cadrul nomenclatoarelor
14) Toate operațiunile desfășurate în cadrul sistemului de stocare, gestionare și publicare a nomenclatoarelor se vor înregistra într-o componentă de jurnalizare a sistemului, astfel încât să fie posibilă auditarea ușoară de către key-userii.

Notă: Pentru o implementarea optimă a sistemului se va folosi un mecanism standardizat de subscrieri la resursele corespunzătoare secțiilor de Terapie Intensivă și Sălilor de Operație. Odată ce o subscriere este înregistrată la serverele locale ale spitalelor, serverul local verifică fiecare resursă creată sau actualizată, iar dacă resursa corespunde criteriilor de subscriere, trimite un mesaj pe „canalul securizat” definit, astfel încât sistemul HUB - MS poată lua măsuri adecvate .
Din punct de vedere tehnic, Modulul de transfer de date între aplicații va implementa o versiune a standardului HL7 sau un standard echivalent.
Standardele de mesagerie HL7 sunt aplicate pe scară largă de către soluțiile software din sistemul medical. HL7 Versiunea 2 („v2”) este în prezent cea mai populară alegere pentru schimbul de informații medicale, incluzând informații despre registrele medicale electronice. HL7 Versiunea 3 („v3”) a fost concepută pentru a fi succesorul versiunii 2, abordând deficiențele versiunii 2. Datorită inconsecvenței documentației, dar și datorită complexității acesteia, această versiune nu se bucură de o mare popularitate. Standardele HL7 FHIR (Fast Healthcare Interoperability Resource) sunt cea mai nouă versiune de implementare a standardului HL7. Implementate în aplicațiile software se face pe o arhitectură modernă de tip RESTful, cu resurse care pot fi consumate direct sau prin mesagerie, cu o specificație simplificată, cu un număr mic de tipuri de mesaje (aproximativ 30, față de peste 400 in HL7 v3).Oricare din cele 3 versiuni ale HL7 corespund funcțional cerințelor proiectului. Furnizorul va trebui să abordeze dezvoltarea

modulului de integrare al componentei HUB – MS în același mod cu Modulul de transfer de date între aplicații.

3.2.2. Componentele software la nivel central HUB MS

3.2.2.1. Software de baza la nivel central HUB MS

3.2.2.1.1. Solutie virtualizare – centru HUB MS

Pe nodurile de virtualizare se va folosi o solutie de virtualizare cu management centralizat care trebuie sa aiba urmatoarele functionalitati:

1) Să nu depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea şi funcţionalitatea serverelor, respectiv a maşinilor virtuale care rulează pe serverele respective;
2) Amprenta pe disc a hypervisor-ului să fie cat mai mică (sub 300MB) astfel încât instalarea hypervisor-ului să fie facuta foarte rapid (direct pe server) chiar și din rețea, oferind totodata posibilitatea de boot-are de pe stick USB;
3) Suport pentru USB 3.0 (client atasat la masini virtuale cu sistem de operare Linux);
4) Să permită conectarea peste rețea printr-un concentrator de porturi seriale la consola serială a oricarei mașini virtuale (exemplu: Linux);
5) Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalitati disponibile în noile versiuni de procesoare;
6) Să ofere o scalabilitate crescuta prin configurarea în clustere de înaltă diponibilitate;
7) Să dispună de capacitati de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster;
8) Să dispună de capacitati de failover astfel încât, în cazul defectării parțiale a unui host, mașinile virtuale care rulau pe acel host să poata fie migrate online pe celelalte host-uri din cluster iar host-ul degradat sa fie trecut in mentenanță după evacuarea mașinilor virtuale;
9) Să dispună de capacitati de failover astfel încât, în cazul blocarii sistemului de operare instalat intr-o mașina virtuală, respectiva mașina virtuală să fie restartată automat pe acelasi host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor;
10) Să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster;
11) Să permită identificarea și evitarea situatiilor de split-brain prin monitorizarea stării host-urilor atât la nivelul retelei de management cat și la nivelul storage-ului comun;
12) Să permită replicarea mașinilor virtuale la nivel de host, independent de tipul stocării folosite la sursă și destinatie, asigurand un RPO (recovery point objective) de minimum 5 minute;
13) Să permită stabilirea unei politici de retentive a replicărilor cu peste 20 de replici în timp (exemplu: 4 replici pe zi, timp de 6 zile), care vor permite refacerea sistemului replicat prin procedura de recuperare, solutie utila pentru refacerea în cazul coruperii datelor sau virusarii;
14) Să ofere posibilitatea mutarii simultane a mașinilor virtuale (minim 4, pe legaturi Gigabit/10 Gigabit) în funcționare de pe un host pe altul/altele fără afectarea funcționarii acestora pentru a se putea executa activitati de mentenanta pe host-ul respective;
15) Să asigure rate mari de consolidare a mașinior virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memoriei (ex “Memory BalIooning”, ”Transparent Page Sharing”, “Memory Compression”, “Swap to disk”) pentru reducerea costurilor asociate infrastructurii fizice (exemplu: număr host-uri, număr porturi de rețea/switch-uri);
16) Să poată rula pe host-uri echipate cu până la 576 de CPU-uri logice și 12TB memorie RAM;
17) Sisteme de operare suportate pe mașinile virtuale: Windows (Server: 2016, 2012 R2, 2008 R2, 2003 R2, Desktop: 10, 8.1, 7), Red Hat, SuSE, Ubuntu, FreeBSD, CentOS, Solaris, Oracle Linux, Mac OS X Server;
18) Aplicatia de virtualizare să permită configurarea și rularea unor mașini virtuale cu până la 128 procesoare virtuale și 6TB RAM;

19) Să suporte diverse tipuri de storage (SAN, NAS, iSCSI) și protocoale de access (FC, FCOE, ISCSI, NFS) la nivel de cluster;
20) Suport larg din partea ISV (Independent Software Vendors) terti pentru aplicațiile Tier 1 și nu numai – exemplu: Microsoft – SQL, Exchange, SharePoint, Oracle – RAC, SAP – HANA;
21) Posibilitatea utilizării unui echipament de stocare extern pentru mai multe host-uri. Storage-ul trebuie să poată stoca atât mașina virtuală cât și hard disk-urile virtuale asociate acesteia;
22) Accesul către sistemul de stocare extern să poată fi făcut pe mai multe căi (muItipathing), asigurându-se suport pentru failover și load balancing, oferind și posibilitatea de alegere a politicii de stabilire a căii de acces (exemplu: fixă, MRU, Round Robin);
23) Sistemul de fişiere va permite accesul concurent a mai multor servere fizice (host) şi a mai multor maşini virtuale la aceeaşi resursă de stocare;
24) Sistemul de fişiere trebuie să asigure că o maşină virtuală este accesată doar de pe un singur host (sistem de blocarea accesului); în caz de defectare a host-ului maşina virtuală trebuie să poată fi restartată de pe alt server fizic;
25) Sistemul de fişiere va asigura posibIitatea migrării în timp real (fără intreruperea funcţionării) unei maşini virtuale de pe un host pe altul;
26) Sistemul de fişiere tebuie să suporte expansiunea dinamică a volumelor şi LUN-urilor la capacitati mai mari de 2TB;
27) Aplicatia de virtualizare trebuie să permită crearea de grupuri de maşini virtuale care să impartă aceleaşi resurse puse Ia dispozitie în comun (memorie şi timpi de procesor);
28) Software-ul instalat pe host trebuie să poată crea echipamente de reţea virtuale (switch-uri) Ia care să se conecteze maşiniIe virtuale şi interfetele de rețea fizice de pe host;
29) Aplicatia de virtualizare trebuie să permită managementul salvărilor contextuale (snap-shot) ale maşinilor virtuale fără afectarea stării de funcționare, astfel încât o maşină virtuală se va putea restaura din orice salvare anterioară;
30) Interfata unica de management bazata pe interfata web, accesibila de pe browser-e Firefox (Windows, Mac OSX), Google Chrome (Windows, Mac OSX) și IE (Windows) pentru simplificarea managementului;
31) Soluția de management centralizat aferente fiecarei locatii să fie disponibilă ca appliance virtual pentru simplificarea instalarii, actualizării și administrării precum și pentru reducerea costurilor asociate (exemplu: licenta windows, licenta baza de date SQL sau Oracle).
32) Solutia de management trebuie sa ofere informatii privind intregul inventar al mediului virtual administrat din locatia respectiva, incluzand masini virtuale, gazde, medii de stocare si rețele de date;
33) Oferta tehnica va contine in clar denumirea comerciala si codul comercial (part numberul) a licentelor software ofertate conform catalogului de produse al producatorului acestora precum si cantitatea ofertata.
34) Licentele software ofertate vor fi conforme schemei de licentiere a producatorului acestora, vor asigura licentierea completa a puterii de calcul a serverelor din fiecare locatie si vor permite definirea unui numar nelimitat de masini virtuale.
35) Licentele software ofertate vor fi non-OEM, licente perpetue, putand a fi utilizate de catre beneficiar pe orice server functie de cerintele de procesare si stocare date.
36) Licentele software ofertate vor asigura administrarea serverelor in configuratie cluster, la nivelul fiecarei locatii, administrarea fiind realizata in consola pe baza de conturi cu drepturi de acces.

Suport software de la producatorul licentelor software pentru minimum 3 ani de la data receptiei cantitative in locatia de instalare.

3.2.2.1.2. Solutie de backup – centru HUB MS

1) Aplicatia de backup furnizata va trebuie sa fie capabila sa gestioneze dintr-o singura consola de administrare, atat serverele fizice cat si cele virtuale.
2) Administrarea aplicatiei de backup se va realiza prin intermediul unei console de administrare

centralizata pentru mai multe servere de backup, indiferent de platformele pe care ruleaza acestea (Windows, Linux).

3) Aplicatia de backup trebuie sa puna la dispozitie si o interfata de management de tip "command line", atat pentru platforme Windows, dar si pentru Linux.
4) Aplicatia de backup trebuie sa permita instalarea unei console de administrare pe statia de lucru a administratorului.
5) Solutia de backup trebuie sa puna la dispozitie, pe langa setarile si configurarile standard, un set de "wizard-uri" care sa permita administratorilor sa configureze cat mai usor device-urile utilizate pentru salvarea datelor, volumele, job-urile de backup pentru salvarea catalogului, precum si crearea usoara de politici de backup folosind aceste "wizard-uri".
6) Solutia de backup trebuie sa aiba capabilitatea de a seta limitari la nivelul benzii de retea si de a aplica restrictii de banda in timpul procesului de backup.
7) Solutia de backup oferita va trebui sa dispuna de capabilitati de retentie a backup-urilor pentru diverse perioade de timp: saptamanal, lunar, anual si infinit.
8) Aplicatia de backup trebuie sa fie capabila sa descopere masinile virtuale nou create pentru a le putea include in procesul de backup.
9) Aplicatia de backup va oferi posibilitatea automatizarii, bazata pe politici, ale proceselor de backup si restaure.
10) Aplicatia de backup va permite efectuarea backup-ului doar pentru fisierele care au suferit schimbari de la ultimul backup si pentru fisierele nou create.
11) Aplicatia de backup va putea pune la dispozitie (la cerere) un model de administrare flexibil, permitand accesul mai multor utilizatori (administratori si operatori), fiecare cu nivel de autorizare diferit.
12) Aplicatia de backup va putea oferi facilitatea de criptare a datelor schimbate intre client si server in timpul procesului de backup/restore.
13) Aplicatia de backup va permite setarea perioadelor de pastrare a datelor salvate, in functie de timpul la care a fost realizat backup-ul.
14) Aplicatia de backup va oferi mecanisme de "Data reduction" (compresie si deduplicare) pentru eficientizarea utilizarii retelei si a spatiului de stocare.
15) Aplicatia de backup trebuie sa aiba suport nativ pentru serviciul director inclus in arhitectura propusa
16) Abilitatea de a restaura obiecte individuale ale serviciului director pana la nivelul de atribute individuale fara a restaura intreg serviciul director.
17) Abilitatea de a restaura articole individuale ale serviciului director, in timp ce acesta este in activitate (nu necesita restartare), incluzand:
    - conturi individuale de utilizator
    - Organizational Units (OU's)
    - Obiecte printer
    - Chiar atribute individuale ale serviciului director si valori incluzind nume, adrese, numere de telefon, adrese de posta electronica, etc. toate dintr-un singur pas la nivel de copie de siguranta a serviciului director
18) Solutia de backup trebuie sa suporte backup pe disc si pe banda magnetica.
19) Solutia de backup trebuie sa se integreze cel putin cu urmatoarele aplicatii si baze de date: Microsoft SQL, Microsoft Active Directory, Oracle, IBM DB2, MySQL, PostgreSQL.
20) Aplicatia de backup ofertata trebuie sa suporte urmatoarele sisteme de operare: Windows Server, Windows Client, Linux (Red Hat, SUSE, Oracle, Debian/CentOS/Ubuntu).
21) Serverul de backup trebuie sa suporte instalarea pe cel putin urmatoarele platforme: Windows, Linux Red Hat, Oracle Linux si SUSE.
22) Solutia de backup trebuie sa se integreze cu principalele medii de virtualizare cum ar fi VMware si Microsoft Hyper-V.
23) Solutia furnizata nu trebuie sa necesite instalarea de Proxy VM pentru a realiza backup la medii virtuale ce folosesc hipervizori VMware sau Microsoft Hyper-V.
24) Aplicatia de backup trebuie sa fie capabila sa restaureze la nivel granular (file si folder) din

interiorul unei masini virtuale (Hyper-V sau VMware), fara a fi nevoie de o restaurare integrala a masinii virtuale si fara a fi nevoie sa se instaleze vreun agent in masina virtuala.

25) Solutia de backup trebuie sa poata pune la dispozitie API-uri cum ar fi interfata de tip XBSA ce permite furnizorilor de aplicatii sa dezvolte propriile solutii care sa se integreze cu clientii/aplicatia de backup.
26) Licente perpetue pentru backup-ul a 4TB de date din locația de implementare (HUB MS).

3.2.2.1.3. Solutia de gestiune Data warehouse – centru HUB MS

Solutia de Data warehouse va avea in vedere colectarea si consolidarea datelor de la bazele de date ale unitatilor spitalicesti din teritoriu si trebuie sa aiba urmatoarele caracteristici tehnice minime:

1) să fie un sistem de administrare a bazelor de date de tip relational si sa fie disponibil comercial (COTS – Commercial off the Shelf) si sa ofere posibilitatea de a rula pe diverse platforme hardware precum si pe sistemele de operare majore existente pe piata (Windows, Linux si Unix). Pentru a raspunde cerintelor de functionalitate si performanta cerute, sistemul de baze de date relationale trebuie sa prezinte urmatoarele capabilitati minime si obligatorii:
2) trebuie să asigure nivelurile de izolare ANSI SQL si sa ofere suport pentru functionalitatile de baza pentru limbajul SQL asa cum sunt ele stabilite in standardele SQL2008 si SQL2011;
3) suspendarea temporara a operatiilor consumatoare de resurse cu reluarea ulterioara a acestora in momentul cand sistemul permite, precum si posibilitatea de a implementa scheme de prioritate in modul de accesare a resurselor 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 ;
4) interogarea direct din baza de date a fisierelor text externe, fara a necesita in prealabil o operatiune de incarcare intr-o tabela din baza de date inclusiv posibilitatea de a rula anumite scripturi la momentul interogarii acestor fisiere din interiorul bazei de date ;
5) reorganizarea, mutarea si redefinirea de tabele si indecsi fara blocarea activitatii utilizatorilor la datele aflate in curs de modificare, indiferent de dimensiunea acestora;
6) sa permita accesul cat mai rapid la informaţii prin utilizarea diferitelor tipuri de indecşi, cum ar fi B-Tree, bitmap, function based, domain sau similari dar si a tabelelor de tip index in care datele sa fie ordonate dupa o anumita coloana;
7) sa ofere suport pentru proceduri stocate, triggeri si tranzactii autonome ;
8) sa permita paralelizarea operatiilor de tip DML si DDL (insert, update, delete, merge, creare indecsi, creare tabele, interogari, etc) pentru o reducere semnificativa a timpului de raspuns pentru aceste operatii ;
9) sa ofere nativ mecanisme care sa permita interogarea istoricului modificarilor unei tabele, indiferent de tipul activitatilor (DDL sau DML), fara a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvarea periodica sau utilizarea functiei de audit ;
10) sa permita recuperarea rapida in urma erorilor umane prin posibilitatea de a recupera online randuri sau tabele sterse de utilizatori fara a utiliza proceduri complicate si date de backup
11) Baza de date trebuie sa permita functionarea intr-o arhitectura de disponibilitate inalta de tip cluster activ-activ asigurandu-se toleranta la defecte hardware sau nefunctionare planificata, scalabilitatea si disponibilitatea crescuta a sistemului. 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 perspectiva administrarii si monitorizarii, solutia de baza de date trebuie sa ofere o unealta cu interfata grafica accesibila web care sa ofere minim urmatoarele functionalitati:gestionarea obiectelor bazei de date si a proceselor uzuale ;

12) administrare utilizatori, roluri si privilegii ;
13) monitorizarea performantei si sanatatii bazei de date precum si vizualizarea fisierelor de tip log si trace ;

14) vizualizarea incarcarii bazei de date, a activitatii utilizatorilor si a operatiilor mari consumatoare resurse .

Din perspectiva operatiilor de backup, baza de date trebuie sa permita:

15) operatiuni de backup si restaurare a datelor in regim de lucru online, salvarea totala si/sau partiala a bazei de date;
16) 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 ;
17) efectuarea de backup-uri complete si partiale (incrementale) pentru optimizarea spatiului aferent datelor de backup, indiferent de tipul de date stocate in baza de date, inclusiv pentru cele binare de tip BLOb (*Binary Large Object*) ;
18) posibilitatea de a marca anumite fisiere de date sau tablespace-uri ca fiind de tip READ-ONLY in vederea excluderii pe viitor a acestora din operatiile automate de backup (atat backup complet dar si incremental) ale bazei de date
19) pe baza datelor de backup, sa poata efectua restaurare la nivel de bloc de date, tabela, tablespace sau datafile precum si restaurarea partiala a bazei de date dar asigurandu-se o imagine consistenta a acesteia de la un moment de timp specificat de cel ce realizeaza operatia de restaurare ;

Pentru asigurarea trasabilitatii activitatii utilizatorilor, 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).

Ca mecanisme de securitate oferite, baza de date:

20) trebuie sa includa restrictionarea accesului la nivelul obiectelor bazei de date, aplicarea simultana a mai multor politici de securitate pe un acelasi obiect al bazei de date precum si mecanisme native de restrictionare a accesului utilizatorilor la nivel de inregistrare si coloana intr-o tabela
21) baza de date va trebui sa ofere si o functionalitate de afisare conditionata a informatiilor dintr-o anumita coloana, inclusiv posibilitatea de a afisa doar partial informatia din coloana, in functie de contextul de lucru al utilizatorului (statie de lucru, adresa IP, client folosit, ora din zi, zi din saptamana sau similar)
22) pentru sporirea securitatii procesului de autentificare la baza de date, aceasta va permite configurarea autentificarii utilizatorilor pe baza de certificate digitale si ii va informa pe acestia despre data si ora ultimei conectari in baza de date.
23) pentru sporirea sigurantei datelor baza de date va include mecanisme robuste de criptare a datelor stocate cat si a celor vehiculate in timpul sesiunilor dintre utilizatori si baza de date. Toate operatiile de criptare trebuie sa poata fi implementate intr-un mod transparent, fara a implica modificari la nivel de aplicatie de business sau client. In functie de nevoie, criptarea transparenta a datelor stocate trebuie sa poata fi facuta la nivel de coloana, tabela sau chiar la nivelul intregii baze de date si sa suporte cel putin urmatorii algoritmi de criptare : 3DES (minim 168 bit) si AES (minim 256 bit).

3.2.2.1.4. Solutie de raportare – centru HUB MS

Sistemul de raportare de la locatia centrala trebuie sa permită următoarele:

1) Să ofere posibilitatea de rulare pe diverse platforme hardware şi pe sistemele de operare majore de pe piaţă (Windows, Linux si Unix);
2) Să ofere posibilitatea prezentării datelor în formate variate (tabele, tabele pivot, grafice, texte derulante etc.);
3) Să ofere funcţionalităţi de navigare ghidată pentru utilizatorii finali, cu posibilităţi multiple de navigare dintr-un anumit punct, atât pentru rapoarte cat şi pentru grafice;

4) Să permită combinarea rezultatelor obţinute de pe platforme diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
5) Să permită salvarea rapoartelor în formate diferite (Excel, PDF, Word, HTML, etc.);
6) Să ofere posibilitatea includerii rapoartelor/graficelor în tablouri de bord pentru toţi utilizatorii finali, fără costuri de licenţiere suplimentare;
7) Să permită tuturor utilizatorilor finali modificarea tablourilor de bord sau a rapoartelor (fără costuri de licenţiere suplimentare);
8) Să nu necesite replicarea datelor pe un server separat, ci să folosească capabilităţile bazei de date sursa. Mediul de lucru pentru utilizatorii finali sau alţi dezvoltatori de rapoarte/analize sa fie în mediu web pur;
9) Să faciliteze accesul la informaţie printr-un nivel de metadate care să ascundă utilizatorilor finali complexitatea structurilor fizice de date;
10) Nivelul de metadate expus utilizatorilor să fie comun la nivelul tuturor modulelor sistemului de raportare şi analiză;
11) Utilizatorii să îşi poată crea singuri propriile rapoarte (analize ad-hoc) fără să fie nevoiţi să cunoască structurile fizice de date pe care le accesează;
12) Să permită accesarea datelor atât de pe platforme relaţionale, cât şi multidimensionale sau foi de calcul;
13) Să permită integrarea cu LDAP, oferind în acelaşi timp capabilităţi proprii de definire a rolurilor pentru restricţionarea accesului la rapoarte;
14) Interacţiunea utilizatorilor finali cu aplicaţia se va face într-o interfaţă de tip web, fără a necesita instalarea de componente software suplimentare pe maşinile utilizatorilor, prin operaţiuni de tip point-and-click şi drag-and-drop;
15) Să expună o interfaţă de administrare atât a drepturilor de acces la diferite zone cât şi a drepturilor de acces pe diferite tipuri de acţiuni;
16) Să fie scalabilă şi să dispună de mecanisme de clustering a componentelor (de prezentare sau la nivel de server de acces la date), astfel încât să poată fi adăugate ulterior resurse hardware suplimentare;
17) Să ofere posibilitatea prezentării simultane a aceleiaşi informaţii în formate diferite, printr-o singură execuţie a interogării: de exemplu tabel + grafic;
18) Să permită configurarea raportului astfel încât utilizatorii să poată selecta în tabloul de bord modul de reprezentare a informaţiei: tabel, grafic, etc.;
19) Să permită facilităţi avansate de formatare a rapoartelor;
20) Să ofere posibilitatea de a salva, organiza şi partaja rapoartele cu alţi utilizatori;
21) Să ofere capabilităţi de drill-down pe diferite nivele de agregate;
22) Generarea interogărilor către bazele de date să ţină seama de specificul bazei de date accesate si să genereze interogările ţinând cont de funcţii native, specifice fiecărei platforme în parte;
23) Produsul va oferi posibilitatea de a crea rapoarte înlănţuite, datele din raportul copil fiind filtrate pe baza rezultatelor din raportul părinte;
24) Accesul utilizatorilor la informaţie trebuie să se facă si pe criteriul domeniului de valori (de exemplu un utilizator să nu poată vedea decât rândurile la care acces);
25) Să ofere acces direct la surse de date multiple, de pe platforme diferite (Oracle ,SQL Server, DB2, SQL Anywhere, etc.), în mod transparent pentru utilizatorul final;
26) Să dispună de mecanisme de alertare pentru utilizatorii finali (cel puţin prin aplicaţie, email şi dispozitive mobile);
27) Accesul utilizatorului final să se facă dintr-o singura interfaţă web din care să aibă acces la toate componentele de analiză, raportare, alertare, notificare etc.
28) Să permită navigarea de la tablourile de bord la analizele relevante, care detaliază informaţiile din aceste tablouri de bord, în aceeaşi interfaţă utilizator;
29) Rapoartele analitice să poată fi construite pe un număr variabil de interogări analitice. Instrumentul de business intelligence nu trebuie să limiteze numărul de astfel de interogări (querry-uri);
30) Să ofere utilizatorilor finali posibilitatea subscrierii la alertele definite;

31) Să dispună de mecanisme de optimizare a accesului la informaţie (cu impact minim asupra bazei de date) asigurând minimal următoarele: mecanisme de multi-user shared caching, generarea optimizată a interogărilor;
32) Din punctul de vedere al arhitecturii sistemului de raportare, toate componentele sale trebuie să fie strâns integrate, să facă parte dintr-un mediu unitar de lucru si să împărtăşească un sistem de securitate comun;
33) Produsul trebuie să afişeze excepţiile/depăşirile sub forma de cod culori;
34) Să ofere utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât şi în aplicaţia de front-end.
35) Să asigure acces ODBC către layer-ul de metadate ce poate fi accesat direct de către orice altă aplicaţie astfel încât metadatele sistemului să fie accesibile aplicaţiilor externe în scopul consultării sau modificării definiţiilor şi algoritmilor de calcul şi includerea acestora în rapoarte
36) Să asigure posibilitatea de writeback în baza de date din layer-ul de raportare;
37) Să ofere posibilitatea de a copia obiectele din tablourile de bord şi de a le afişa în MS Office;
38) Să ofere posibilitatea de accesa obiectele de BI din MS Excel, cu posibilitatea reexecutării raportului direct din MS Excel.
39) Să ofere utilizatorului posibilitatea de a utiliza acelaşi set de parametrii către multiple rapoarte/ tablouri de bord;
40) Să ofere utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cat şi în aplicaţia de front-end;
41) Să ofere capabilităţi pentru salvarea filtrelor aplicate unui raport sau pentru salvarea template-urilor de formule;
42) Să dispună de vizualizări interactive, tranziţii animate între rapoarte, legături Master — Detail;
43) Să permită vizualizarea trasabilităţii unei componente dintr-un raport, şi dacă aceasta reprezintă o valoare calculată să permită vizualizarea formulei de calcul utilizate, integrând informaţiile de calcul din instrumentul de business intelligence cu regulile de transformare aplicate în instrumentul de ETL;
44) Să ofere un mecanism de programare a execuţiei rapoartelor sau a preîncărcării în serverul de BI a unui set de date astfel încât să minimizeze timpii de execuţie ai interogărilor analitice, în funcţie de sursele de date
45) Să ofere funcţionalităţi de navigare ghidată pentru utilizatorii finali, cu posibilităţi multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât şi pentru grafice; Implementarea mecanismului de navigare ghidată nu va implica scrierea de secvenţe de cod/programare, ci va folosi funcţionalităţile native ale sistemului.
46) Să permită salvarea tablourilor de bord sau a analizelor de business intelligence pentru a putea fi accesate offline, fără conexiune la serverul de BI.
47) Să permită navigarea în cadrul tablourilor de bord salvate offline.
48) Soluția trebuie să fie licențiată pentru accesul a 25 de utilizatori - licențe perpetue.

3.2.2.1.5. Solutie management centralizat echipamente comunicatii – centru HUB MS

Solutia trebuie sa indeplineasca minim urmatoarele functionalitati:

Functii generice de sistem

- Administrare bazata pe profile
- Interfata securizata Web
- Comunicare criptata si autentificare intre echipamentul de management si sistemele administrate
- Alerta Mail Server
- Baza de date relationala
- Lansare module management
- Lansare consola administrator
- Online Help în limba română
- Vizualizare Informatii Sistem / Resurse

- Vizualizare licenta
- Vizualizare istoric functionare
- Vizualizare informatii sesiune
- Configurare setari de baza sistem
- Vizualizare alerte
- Vizualizare Informatii Sistem / Resurse
- Vizualizare status conexiune echipamente conectate
- Backup / Restore
- Incarcare setari din fabrica
- Formatare discuri interne
- Schimbare Firmware
- Schimbare Host Name
- Conectare la Update Center
- Suport upgrade-ul de firmware, salvarea si restaurarea configuratiei de pe USB

Manager LOG & rapoarte
- Vizualizare log-uri
- Stocarea log-urilor in Central Data Repository
- Vizualizare si configurare log-uri de sistem, de evenimente de securitate, sumar de trafic, continut, arhive, carantina, rapoarte)
- Programare log-uri automate
- Integrare securizata cu echipamentele conectate

Echipamente si politici de management
- Adaugare/Schimbare/Stergere echipamente sau grupuri de echipamente
- Adaugare/Schimbare/Stergere liste filtre
- Parametri administrativi
- Proprietati de baza sistem
- Parametri antivirus
- Parametri Firewall
- Parametri HA
- Parametri preventie si detectie intruziuni
- Parametri filtrare continut
- Utilizatori/Grupuri Salvare/Restaurare configuratie IP virtual

Monitorizare in timp real
- Monitorizare stare echipament
- Monitorizare parametri de functionare
- Monitorizare echipamente/ grupuri de echipamente
- Filtre si vizualizari personalizate
- Setare limite grupuri
- Monitorizare serviciu High-Availability

Manager scripturi
- Vizualizare/Editare/Salvare scripturi
- Rulare scripturi
- Validare scripturi

Manager VPN
- Configurare / Monitorizare echipamente VPN, parametri si politici
- Management/ Monitorizare clienti VPN
- Creare de tunele VPN
- Configurare profile de trafic

- Configurare parametri autentificare IPSec
- Creare servicii personalizate

Manager update-uri
- Adaugare/Schimbare/Stergere echipamente
- Monitorizare stare echipamente conectate
- Conectare la reteaua de update-uri
- Update antivirus si definitii de atacuri
- Updateuri programabile sau manuale
- Vizualizare pachete si statistici pentru AV/IP
- Configurare filtru web si servicii Antispam
- Upload-uri manuale ale bazelor de date

Manager firmware
- Management imagini Firmware pentru echipamente
- Instalare imagini Firmware catre echipamentele conectate
- Upgrade/Downgrade Firmware echipamente

Capabilitati solutie management centralizat
- Management al tuturor access point-urilor solicitate si al firewall-urilor
- Sa ruleze in regim cluster pentru asigurarea disponibilitatii ridicate – solutia se va instala pe echipamentul server de virtualizare instalat in locatia centrala
- Capacitate log-uri pe zi de 25 GB minim
- Capacitate de stocare 5TB minim
- Solutia trebuie sa nu consume multe resurse, sa poata rula si pe masini virtuale VMWare, Hyper-V sau Open Source Xen, cu minim 4 GB memorie si minim 2vCPU.

Se va configura solutia in regim fail-over pentru a se asigura inalta disponibilitate.

3.2.2.2. Aplicatie centrala Dashboard Disponibilitate paturi ATI

1) Soluția trebuie să funcționeze în cadrul Ministerului Sanatatii HUB MS;
2) Soluția trebuie să fie integrată cu sistemul de ATI din cadrul celor 18 spitale (5 regiuni / 5 orașe), incluse în proiect.
3) Soluția trebuie să furnizeze din cadrul sistemului de ATI numărul de paturi libere și cele ocupate din secțiile de ATI pentru fiecare spital în parte, în timp real (maxim 60 de secunde).
4) Soluția trebuie să aibă modulul de triaj din cadrul sistemului ATI astfel încât operatorul HUB MS să poată să stabilească/prioritizeze urgența/gravitatea cazului.
5) Soluția trebuie să furnizeze paturile libere din secțiile de ATI așa cum sunt denumite în sistemul de ATI din cadrul spitalului. De exemplu, în Spitalul 6 există:
   - 5 secții de ATI (ATI 1, ATI 2…ATI 5);
   - În toate secțiile ATI sunt 3 paturi libere (ex: ATI 1 – 2 paturi, ATI 5 – 1 pat);
   - Denumirea acestora în sistemul de ATI este de exemplu ATI 1 - P3, P8 și ATI 5 - P13.

   Soluția din cadrul HUB MS trebuie să preia aceleași denumiri, respectiv ATI - P3, P8 și ATI - P13;
6) Soluția trebuie să aibă posibilitatea de a rezerva paturile libere, iar sistemul de ATI să poată prelua în timp real (maxim 60 de secunde) rezervarea acestora;
7) Soluția trebuie să funcționeze în cadrul HUB-MS pe 5 calculatoare și 5 monitoare cu diagonală mare pentru a fi ușor de vizualizat (de ex: minim 165 cm diagonala), unul pentru fiecare regiune/oraș;

Exemplu de ecrane pentru soluția din HUB:

a) Luăm exemplul de mai sus, respectiv cel al Spitalului 6 din orașul/regiunea București (Fig.1) unde avem disponibilitatea paturilor de ATI (3 libere, verde și 27 ocupate, roșu), acesta fiind ecranul principal al soluției din cadrul HUB MS;

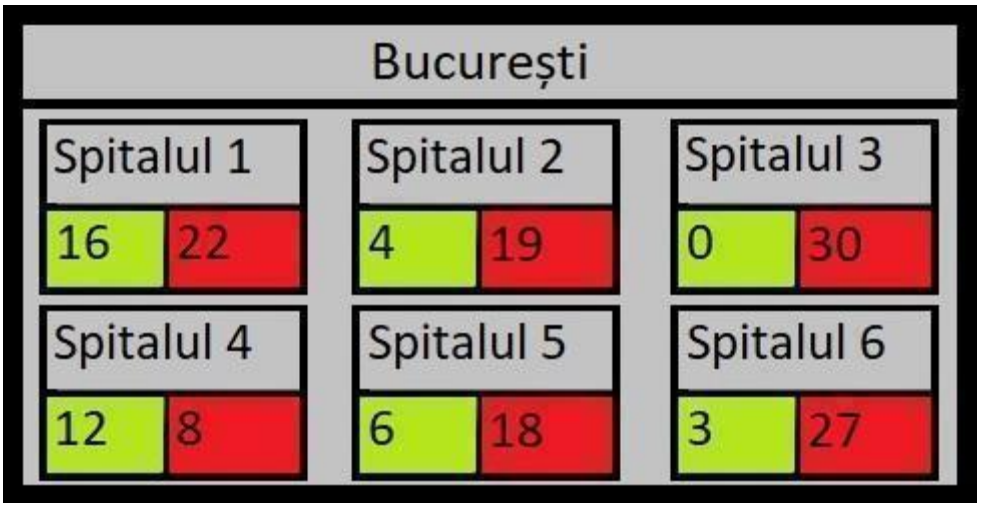


Fig.9. -

b) Dacă operatorul HUB MS trebuie să rezerve un pat, selectează Spitalul 6 din Fig.9. Soluția trebuie să îi afișeze Spitalul 6, secțiile ATI și gradul de ocupare al paturilor per secție (Fig.10). Din acest ecran își va alege secția ATI dorita (ATI 1 sau ATI 5)

Fig.10. -

c) Soluția trebuie să îi afișeze secția respectiva și paturile libere, așa cum sunt denumite în sistemul de ATI al Spitalului, în exemplul nostru, ATI 1 (Fig.11).

Fig.11 -

d) Din acest ecran (Fig.3), operatorul HUB MS poate rezerva patul (de exemplu, prin clic dreapta și alege opțiunea de rezervare). După rezervare, soluția va indica patul (ex: P3) ca fiind rezervat, modificând culoarea, din verde în roșu (Fig.12) și va transmite în timp real (maxim 60 de secunde) rezervarea și către sistemul de ATI din cadrul Spitalului 6.

Fig.12 -

e) După rezervare, în ecranul principal, soluția trebuie să indice numărul de paturi ATI ramase libere, respectiv Spitalul 6: 2 paturi libere (verde) și 28 paturi ocupate (roșu), fig.13.

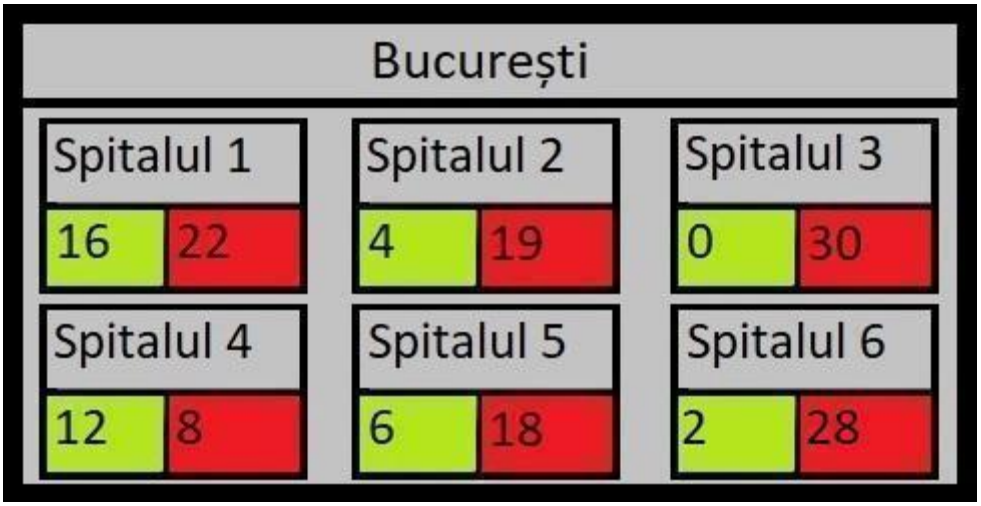


Fig.13 -

8) Sistemul ATI din cadrul spitalelor va prelua toate informațiile de mai sus de la soluția din cadrul C.O.S.U. și le va afișa în timp real (maxim 60 secunde).

Functia Layer GIS

Pe langa prezentarea tabelara a situatiei paturilor ATI disponibile prezentata mai sus, solutia va permite afisarea pe harta a coordonatelor de geolocatie ale spitalelor cu sectii ATI, cu prezentarea pe harta a locatiei spitalului si a paturilor disponibile, astfel incat pentru situatii de urgenta sa se poata oferi suport decizional pentru transferul pacientilor pe ruta optima (cel mai apropiat spital) de la nivel central HUB MS.

Sistemul va permite colectarea in timp real prin intermediul unui serviciu web a datelor continand coordonatele GPS ale ambulantelor/pacientilor. Integrarea sistemelor existente prin intermediul acestui serviciu web (ex. Serviciul 112) nu se afla in scopul acestui proiect si poate face obiectul unui protocol interinstitutional.

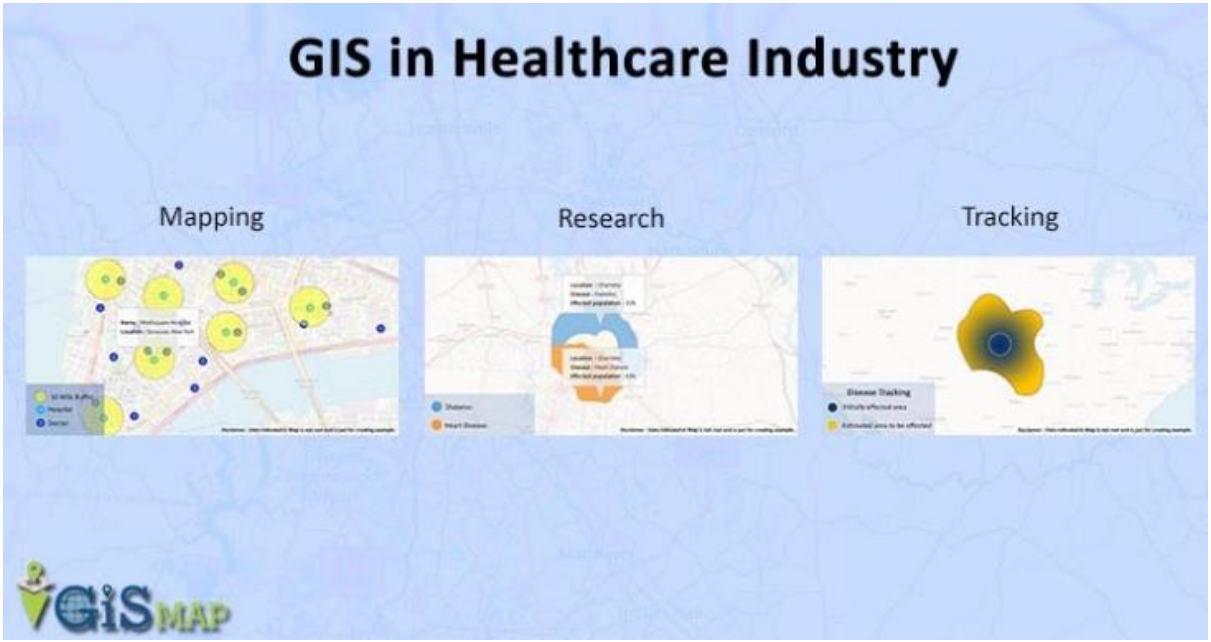


Fig. 14.

Prin selectarea unui spital de pe harta cu paturi disponibile, operatorul HUB MS va putea sa rezerve un pat, urmand acelasi proces ca si in vederea tabelara a paturilor disponibile.
In urma etapei de analiza se pot identifica impreuna cu Beneficiarul si alte tipuri de vizualizari (minim cele doua descrise, max.5).

3.2.2.3. Aplicație de BI si raportare pentru Ministerul Sănătății

Modulul de Business Intelligence, raportare, analiză statistică si urmărire tendințe asigură uneltele vizuale de înaltă performanță capabile să reflecte atingerea indicatorilor activităților din sectiile ATI . Platforma de tip enterprise trebuie sa contina un modul de raportare care va permite realizarea prin configurare a unor rapoarte, scorecard-uri si tablouri de bord care sa afiseze in format tabelar sau grafic (widgets) informatii agregate despre activitatile din sectiile ATI .

1) Aplicația va centraliza fluxurile informaționale din aplicația de ATI și Sali Operație din cele 18 spitale incluse în proiect și va pune la dispoziția utilizatorilor rapoarte care să poată reflecta în timp real diverși indicatori de performanță medicală și economică.
2) Aplicația trebuie să fie licențiată pentru un număr de 25 de utilizatori, care vor avea roluri diverse și drepturi diferite de vizualizare a datelor.
3) Modulul va asigura rapoarte diverse extrase dintr-un data warehouse, cu posibilitatea de efectuare a analizelor detaliate prin drill-down.
4) Aplicația va pune la dispoziția fiecărui nivel organizațional o situație centralizată de tip tablou de bord și un număr de rapoarte de analiză managerială, de complexitate medie și ridicată; acestea vor fi definite în etapa de analiză (exemple: scoruri, timp mediu de spitalizare ATI, grad de ocupare al paturilor ATI si alte informatii statistice depersonalizate)

Obiectivul componentei de analytics nu este acela de a exprima modelarea operațională a sectiilor ATI ci se concentrează pe a genera rapoarte "rezumative", agregate si statistici.

Rapoartele si analizele vor permite a fi clasificate pe diferite categorii. Sistemul trebuie sa permita definirea de grupuri de utilizatori si acordarea diferentiata a drepturilor de accesare a anumitor categorii de rapoarte.

III.3. Componentele hardware ale sistemului

III.3.1. Echipamente hardware necesare in locatii

3.3.1.1. PC certificat IP65 (protecție contra apei) sau echivalent și antibacteriană pentru sala de operații și terapie intensivă cu masă dedicată - 924 bucati

Procesor	Procesor de ultima generatie din clasa i5, minim 2.5GHz, minim 6MB cache, 4 nuclee, set instrucţiuni pe 64 biţi sau echivalent
Memorie	minim 8GB
Stocare	minim 120GB SATA SSD
I/O	2 x USB2.0, 4 x USB3.0, serial, 2 x HDMI, 2 x LAN
WLAN	802.11 a/b/c/g/n intern
Display	Touchscreen minim 24 inch TFT LED, sticla Anti Glare, Rezolutie 1920 x 1080 full HD, Marime pixel maxim 0.2715 x 0.2715 (unul pe triada)
Contrast	1000 (Typ)
Luminozitate	300 cd/m2
Timp raspuns	maxim 5ms
Webcam	2MP
Carcasa	tip All in One, integreaza unitatea centrala si monitorul intr-o singura carcasa certificata IP65 (protectie contra apei) si antibacteriana
Optiuni securitate	smart card securitate, RFID
Adaptor alimentare medical	12V DC (curent continuu)
Putere consumata	maxim 29W
Greutate	maxim 7 kg
Temperatura de functionare	0ºC to 40ºC
Temperatura de stocare	-20ºC to +60ºC
Conformitate	CE, FCC-B, RoHS, DICOM IEC 60601-1, IEC 60601-1-2, Class 2 izolare dubla, Energy Star sau echivalent;

Sistem de operare de tip profesional cu funcţionalităţi de securitate	Windows 10 Pro sau echivalent, preinstalat si preactivat
Garantie	3 ani
Accesorii incluse:	
Tastatura	Alba, compacta, cu Numpad integrat, protejata impotriva prafului si a apei (conform IP68), cu minim 104 taste plate cu membrana de silicon care permite dezinfectarea, existenta unui mod de dezactivare a tastelor, pentru curatare, găuri filetate pentru montare VESA, conector USB
Mouse	Alb, cu doua taste si senzor de scroll, protejat cu membrana de silicon (conform IP68), 1000dpi, durata de viata a tastelor de minim un milion de apasari, conform CE, conector USB
Stativ din inox	Cu sertar pentru tastatura si mouse, dimensiuni de minim H 100 cm x L 55 x A 40 cm.

3.3.1.2. Data Terminal Server – 924 bucati

Management	HTTP/HTTPS, CLI sau Telnet
Protocoale	UDP/TCP, DHCP, Extended Telnet RFC 2217, Telnet, Reverse Telnet, Rlogin & Auto Connect, TFTP
Securitate	Securitate SSL, SSL/TLS, SSHv2, FIPS 197 (serial ports), SNMPv2
Software	COM port redirector pentru COM/TTY porturi pentru Microsoft® Windows®, UNIX® şi Linux®, RFC 2217, Python scripting
LEDuri de Stare	Power, Locator, Serial şi Ethernet link/activity
Sisteme de operare	AIX, HP-UX, Solaris, Linux®, Windows® 2000, Windows® XP, Windows® 7, Windows® 8, Windows® 8.1, Windows® 10, Windows Server® 2003, Windows Server® 2008, Windows Server® 2012.
Interfeţe	
Seriale	
Porturi	4 RS-232 porturi cu izolare galvanică (2.5kV)
Rată de transmisie	Până la 230 Kbps
Protocoale	TXD, RXD, RTS, CTS, DTR, DSR, DCD
Ethernet	
Porturi	1 uplink, Optional 4-port switch
Nivel fizic	10/100 Base-T cu izolare galvanică (1.5kV)
Mod	Full sau half duplex
Cerinţe de alimentare	
Sursă de alimentare	Internă 100-240VAC, 50-60 Hz 0.2A max
Protecţie de vârf (ESD)	4 kV puls (EFT) pe EN61000-4-4, 2 kV conform standard EN61000-4-5 sau echivalent
	4 kV izolare galvanică intrări/ieşiri

	2 kV conform standardului EN61000-4-5 sau echivalent
Standarde respectate sau echivalente	
Emisii	EN 55011, EN 55022, CISPR 11, CISPR 22
Siguranţă	EN 60950-1, IEC 60950-1, EN 60601-1, EN 60601-1-2, IEC 60601-1
Protecţie individuală	EN 55024, CISPR 24

3.3.1.3. Echipamentele mobile de vizualizare soluție mobilă terapie intensivă – 40 bucati

CPU	Intel® Pentium® Silver N5000 (min quad core sau echivalent)
Memorie	minim 8GB LPDDR4
Stocare	minim 128GB SSD (M.2)
Display	minim 11" IPS HD 1366x768 multi-touch
I/O	1x USB 3.0 port (Type-A); 1 x USB 3.0 port (Type-C); 1x Combo audio jack; 1x MicroSD card reader
Audio	boxe incorporate 2 x 1W
Sensors	Fingerprint pe butonul de power
Securitate	TPM 2.0
Conectivitate	WiFi 802.11 ac; Bluetooth 4.2; LTE
Camera	cu rotatie de 180 grade 2.0 MP
Acumulator	3 celule 3250mAh (autonomie ~10 ore), 37W, cu incarcare rapida Ruggedness
Alte specificatii	rezistenta la cadere 76cm (conform MIL-STD-810G sau echivalent); rezistenta la lichid (330cc lichid), rezistenta la praf IP5X
Greutate maximă	1.4 Kg cu baterie standard
Tastatura	inclusa
GPS	inclus
Alte specificatii	Active Stylus Pen cu baterie
Sistem de operare de tip profesional cu funcţionalităţi de securitate	Windows 10 Pro sau echivalent, preinstalat si preactivat
Garantie	3 ani

3.3.1.4. Acces point - 446 bucati

Solutie de access wireless (access point-uri) cu capabilitati de securitate (Filtrare Web, Antispam, Antivirus/Antispyware/AntiMalware, Application Control si IDS/IPS) si integrare cu servere de autentificare, minim Active Directory.
Cerinte tehnice minime:

- minim doua interfete redundante GigabitEthernet RJ45
- un port USB
- un port consola RJ-45
- suport PoE, standard 802.3at
- suport Mesh wireless
- suport IEEE 802.11 a/b/g/n/ac
- minim 2 benzi radio (dual band, radio 1 2.4 - Ghz, radio 2 - 5 Ghz)
- suport pentru urmatoarele benzi de frecvente : 2.400 - 2.4835, 5.150 - 5.250, 5.250 -5.350, 5.470 - 5.725, 5.725 - 5.850
- suport MIMO 4x4 cu 4stream-uri spatiale
- rata de transfer Wi-Fi : pana 600 Mbps radio 1, pana la 1733 Mbps radio 2
- suport pentru 6 antene interne type (castig 4.5 dBi -2.4 Ghz, 6.5 dBi - 5 Ghz)
- suport pentru pana la 16 SSID-uri (14 pentru clienti si 2 pentru monitorizare)

- suport pentru minim 4 cozi de trafic cu suport WME Multimedia Extensions
- suport 802.11 Transmit Beam Forming TxBF
- suport 802.11 MPDU/MSDU aggregation
- suport 802.11 Dynamic MIMO Power Save
- suport 802.11 LDPC encoding
- suport 802.11 MLD
- suport 802.11 Max ratio combining (MRC)
- suport 802.11ac MU-MIMO Wave 2
- Suport pentru rogue AP scanning(dual band, background scan & full-time dedicated monitor)
- suport pentru on-wire MAC collector
- suport pentru management din cli si din controller-ul wireless
- suport pentru dicovery al AP-ului dupa DNS name, DHCP based, Multicast si Broadcast
- suport pentru client fast-roaming
- suport Automatic Radio Resource Provisioning
- suport pentru autentificare WPA, WPA2 bazat pe cele mai noi standarde de criptare inclusiv AES, TKIP, AES-TKIP, 802.1X atat pentru utilizatori cat si pentru portalul captiv.
- suport pentru urmatoarele metode de autentifficare IEEE 802.1X(EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA), RFC 2716 PPP EAP-TLS, RFC 2865 RADIUS authentication, RFC 3579 RADIUS support for EAP, RFC 3580 IEEE 802.1x RADIUS Guidelines, RFC 3748 Extensible Authentication Protocol, WPA (Wi-Fi Protected Access) Personal and Enterprise, WPA2 (Personal and Enterprise) – 802.11i standard
- suport remote AP (peste internet)
- suport split routing pentru remote AP
- suport pentru detectia device-urilor cu posibilitatea de clasificare a tipurilor de device-uri, a producatorului, a tipului de sistem de operare si a versiunii sistemului de operare.
- suport pentru detectia aplicatiilor la layer 7 cu peste 300 de semnaturi si posibilitatea de prioritizare sau blocare a aplicatiilor.
- injector POE inclus
- certificari si complianta FCC Part 15 Subpart B (Class B), Subpart C and Subpart E, UL 609550-1, UL 2043, CSA C22.2 No. 60950-1, IEC 60950-1, RSS-210, RSS-GEN, RSS-102, ICES-003, WiFi Alliance, DFS sau echivalente.

Solutia ce urmeaza a fi achizitionata trebuie sa aiba capabilitati de utilizare in medii critice spitalicesti. Managementul access point-urilor se va putea face printr-o solutie software.

Echipamentele vor beneficia de suport 24x7 de la producator pentru o perioada de 3 ani de la data receptiei in locatia de instalare.
In cazul defectarii unui echipament, acesta se va putea inlocui cu un altul in termen de 3 zile de la constatarea defectului.

Nr.	Spitale	Nr AP-uri
1	Spitalul de Urgenta “Bagdasar Arseni” **Bucureşti**	27
2	Spitalul de Urgenta “Sf. Ioan” **Bucureşti**	19
3	Spitalul de Urgenta “Sf. Pantelimon” **Bucureşti**	21
4	Spitalul Clinic de Urgenta **Bucureşti**	44
5	Spitalul Universitar de Urgenta **Bucureşti**	43
6	Spitalul de Chirurgie Plastică Reparatorie şi Arsuri **Bucureşti**	7
7	Spitalul de Urgente Pediatrice “M.S. Curie” **Bucureşti**	18
8	Spitalul de Urgenta pentru Copii “G. Alecsandrescu” **Bucureşti**	20
9	Institutul Inimii de Urgenţă pentru Boli Cardiovasculare "Nicolae Stăncioiu" **Cluj-Napoca**	11

10	Institutul Oncologic "Prof. Dr. I. Chiricuța" **Cluj-Napoca**	16
11	Institutul Regional de Hepatologie si Gastroenterologie " O. Fodor" **Cluj-Napoca**	15
12	Spitalul Clinic Județean de Urgenta **Cluj-Napoca**	48
13	Institutul Regional de Oncologie **Iași**	18
14	Spitalul Județean de Urgenta "Sf. Spiridon" **Iași**	38
15	Institutul de Urgență pentru Boli Cardiovasculare și Transplant **Târgu Mureș**	12
16	Spitalul Județean de Urgentă **Târgu Mureș**	34
17	Institutul de Boli Cardiovasculare **Timișoara**	7
18	Spitalul Clinic Județean de Urgenta **Timișoara**	48
	TOTAL	**446**

Pentru fiecare spital sunt prevazute echipamente de tip acces point, care sa asigure comunicatii de tip wireless in Salile de Operatii si Saloane ATI.

Numarul de acces point-uri care vor trebui livrate in fiecare locatie are in vedere alocarea pentru fiecare spital a:

- cate un acces point la fiecare 5 paturi din saloanele ATI
- cate un acces point la fiecare pat/masa din Sala de operatie

3.3.1.5. Servere pentru baze de date – 36 bucati

În fiecare spital de implementare va rula un cluster de 2 noduri cu baza de date a aplicației ATI si Sala Operație.

Caracteristica tehnica	**Cerinta tehnica minimala**
Form factor	Rackmount 1U echipat cu sine de montaj in rack incluse
Procesoare instalate	1 procesor din segmentul server cu urmatoarele specificatii minimale: - Intel Xeon Silver de ultimă generație, 8 core, min. 2GHz, 11MB cache sau echivalent
Memorie	128GB DDR4 2400 REG ECC; suport arhitectura six-channel, sparing, mirroring, chipkill, minim 24 sloturi DIMM cu suport pentru: - minim 1TB in configuratie maximala (upgrade-uri ulterioare);
Retea	2 x 10Gbps RJ45, 2 x 10Gbps SFP+
Alimentare	Sursă redundantă hot-plug minim 1000W, eficienta 80Plus Platinum
Racire	Ventilatoare redundante
Stocare	8 x bay-uri hot-plug 2.5"; SD slot intern, suport NVMe Serverul include: 2 x SSD 480GB SATA tip Enterprise cu circuit PLI sau echivalent Controller hardware RAID 0,1
Interfete I/O	2 x PCI-E X16 Gen 3.0
Interfete	3 x USB 3.0, 1 x serial, VGA
Video	Controler video integrat cu minim 16MB memorie dedicata
Management	Management acustic si termic. Modul Management IPMI cu port dedicat 1Gbps, suport KVM-over-IP. Se va furniza o aplicatie pentru monitorizarea granulara a componentelor serverului, analiza predictive la defectare cel putin pentru procesor, memorie, unitati de disc/ssd, alertare proactiva erori (inclusiv alertare prin email), obtinere date de performanta, configurare remote a serverului, inventariere hardware (inclusiv P/N componente) si generare rapoarte pentru componentele incluse. Aplicatia va furniza informatii despre senzorii integrati (temperaturi si turatii ventilatoare), log sistem/ audit securitate, unitati disc, procesor, memorie, configurare BMC. Suport SNMP, SSL.

	Va permite colectarea in timp real a informatiilor legate de temperatura si consum de putere al nodurilor din sistem (indiferent de producatorul acestora) cu functionalitati incluse de power-capping. Solutia permite vizibilitate completa a serverelor din retea inclusiv la nivel de rack si permite reducerea consumului de putere si optimizarea alocarii resurselor neutilizate de procesare.
Sisteme de operare certificate de producator	Microsoft Windows Server, Vmware (Vmware Ready).
Conformitate	CE, ISO9001, ISO14001sau echivalent, electrosecuritate si electrocompatibilitate Serverul trebuie sa fie marca inregistrata a producatorului acestuia si trebuie sa fie testat si validat/certificat sub aceasta marca.
Energie disipata	Se va prezenta un calcul al energiei disipate pentru configuratia propusa exprimata in BTU/h
Temperatura de functionare	10 °C - 35 °C
Sistem de operare instalat	minim Windows Server Standard 2016 sau echivalent
Garantie	36 luni

3.3.1.6. Servere pentru virtualizare – 54 bucati

În fiecare spital de implementare a proiectului se va folosi un cluster de 3 noduri pe care va rula mediul virtual al sistemului.

Caracteristica tehnica	**Cerinta tehnica minimala**
Form factor	Rackmount 1U echipat cu sine de montaj in rack incluse
Procesoare instalate	2 procesoare din segmentul server cu urmatoarele specificatii minimale: Intel Xeon de ultima generatie, 14 core, min. 2GHz, 22MB cache sau echivalent
Memorie	256GB DDR4 REG ECC 2400 mhz; suport arhitectura six-channel, sparing, mirroring, chipkill, minim 24 sloturi DIMM cu suport pentru: - minim 1,5TB in configuratie maximala (upgrade-uri ulterioare); - memorie persistenta tip optane (sau echivalent, module de minim 512GB);
Retea	2 x 10Gbps RJ45, 4 x 10Gbps SFP+
Alimentare	Sursă redundantă hot-plug minim 1000W, eficienta 80Plus Platinum
Racire	Ventilatoare redundante
Stocare	8 x bay-uri hot-plug 2.5”; SD slot intern, suport NVMe Serverul include: 2 x SSD 480GB SATA tip Enterprise cu circuit PLI sau echivalent Controller hardware RAID 0,1
Interfete I/O	2 x PCI-E X16 Gen 3.0
Interfete	3 x USB 3.0, 1 x serial, VGA
Video	Controler video integrat cu minim 16MB memorie dedicate
Management	Management acustic si termic. Modul Management IPMI cu port dedicat 1Gbps, suport KVM-over-IP. Se va furniza o aplicatie pentru monitorizarea granulara a componentelor serverului, analiza predictive la defectare cel putin pentru procesor, memorie, unitati de disc/ssd, alertare proactiva erori (inclusiv alertare prin email), obtinere date de performanta, configurare remote a serverului, inventariere hardware (inclusiv P/N componente) si generare rapoarte pentru componentele incluse. Aplicatia va furniza informatii despre senzorii integrati (temperaturi si turatii ventilatoare), log sistem/ audit securitate, unitati disc, procesor, memorie, configurare BMC. Suport SNMP, SSL. Va permite colectarea in timp real a informatiilor legate de temperatura si consum de putere al nodurilor din sistem (indiferent de producatorul acestora) cu functionalitati

	incluse de power-capping. Solutia permite vizibilitate completa a serverelor din retea inclusiv la nivel de rack si permite reducerea consumului de putere si optimizarea alocarii resurselor neutilizate de procesare.
Sisteme de operare certificate de producator	Microsoft Windows Server, Vmware (Vmware Ready).
Conformitate	CE, ISO9001, ISO14001, electrosecuritate si electrocompatibilitate Serverul trebuie sa fie marca inregistrata a producatorului acestuia si trebuie sa fie testat si validat/certificat sub aceasta marca.
Energie disipata	Se va prezenta un calcul al energiei disipate pentru configuratia propusa exprimata in BTU/h
Temperatura de functionare	Cel puțin în intervalul 10 °C - 35 °C
Garantie	36 luni

Pe nodurile de virtualizare se va folosi un sistem de operare compatibil cu aplicația de ATI și Sală Operație. Licența sistemului de operare va fi perpetuă, va acoperi toată capacitatea fizică (core-uri de procesare instalate) a fiecărui nod și nu va trebui să depindă de numărul de mașini virtuale care rulează pe fiecare nod – este necesar sistem de operare licențiat pentru un număr nelimitat de mașini virtuale care vor rula pe clusterul de virtualizare pentru asigurarea înaltei disponibilități a întregului sistem implementat în locație.

3.3.1.7. Echipamente de stocare – 18 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Controller/ CPU	Sistemul de stocare propus trebuie sa dispuna de minim doua controller-e Fiecare controller sa dispuna de 2 procesoare fiecare cu 6-core si 2.2Ghz. minim 20MB cache
Porturi instalate	Interfete de interconectare, astfel: minim 4 porturi 10 Gb Ethernet SFP+ per controller minim 2 porturi 10 Gb Ethernet RJ45 per controller minim 2 porturi 1 Gb Ethernet RJ45 per controller 1 port remote management (KVM-over-IP)
Memorie Cache	Minim 128GB memorie de tip RAM instalata pe fiecare controller
Sloturi de expansiune	Fiecare controller trebuie sa dispuna de minim 2 sloturi PCI-e pentru posibilitatea de suplimentare a porturilor de conectare.
Stocare	Sistemul va avea urmatoarea capacitate de stocare bruta instalata: 13x1.6TB SSD SAS 3DWPD server hot-swap Sistemul de stocare trebuie sa aiba suport pentru cel putin 1PB.
Fiabilitate, disponibilitate, mentenanta	Sistemul trebuie sa ofere metode de autodiagnosticare si izolare a defectelor Sistemul trebuie sa functioneze in configurate de cluster activ-activ sau activ-pasiv cu minim o pereche de noduri. In cazul in care un controller din perechile de noduri este scos din productie (din cauza unor defectiuni sau operatiuni de mentenanata), celalalt nod/pereche trebuie sa preia sarcinile si resursele asignate anterior nodului inactiv; Sistemul de stocare trebuie sa permita o diagnosticare si rezolvare in cel mai scurt timp a problemelor aparute (de exemplu, administratorul trebuie sa aiba vizibilitate si posibilitati de analiza in timp real asupra intregului Sistem de stocare de tip NAS/transport a datelor); Eventualele operatiuni de upgrade al sistemului de operare a nodurilor nu trebuie sa impacteze disponibilitate sistemului; Inlocuirea discurilor defecte trebuie sa se poata realiza cu sistemul de stocare in functiune, fara intreruperea accesului la date.

Caracteristici software si facilitati aditionale:	Sistemul trebuie sa suporte mecanisme de optimizare a procesului de stocare si protectie a datelor: compresie LZ4, deduplicare, thin provisioning; Sistemul trebuie sa suporte acces de tip fisier la informatiile stocate prin intermediul protocoalelor NFS, SMB si acces de tip bloc la informatiile stocate prin intermediul protocoalelor iSCSI, FC; Sistemul suporta standard caching/ tiering. Sistemul trebuie sa suporte functii de clonare si replicare. Sistemul include in mod standard numar nelimitat de clone si snapshot-uri. Sistemul include standard urmatoarele functionalitati de redundata si integritate a datelor: Data & metadata checksumming, self-healing, paritate tripla si suporta functionalitati de recovery tip on-site si off-site. Sistemul suporta functionalitati pentru disaster recovery. Certificare Vmware Ready Storage (include ESXi 6.5, 6.0 U3, 6.0 U2, 6.0 U1, 5.5 Pentru solutia de virtualizare de mai sus este inclusa nativ functionalitate de backup &recovery Sistemul trebuie sa fie compatibil cu urmatoarele medii: VMware, Microsoft Windows, Microsoft Hyper-V, Microsoft Active Directory, Citrix, Linux, RHEL, MacOS, XEN, OpenStack
Monitorizare si alerte	Sistemul trebuie sa permita monitorizarea in timp real si sa alerteze automat, inclusiv prin e-mail, administratorul de sistem. Configurarea si administrarea sistemului de stocare trebuie sa se poata realiza prin interfata web/ CLI. De asemenea sistemul de management trebuie sa includa functionalitatea de roll-back la o stare anterioara. Sistemul trebuie sa includa suport pentru: SNMP, REST API Sistemul de management trebuie sa ruleze integral pe controllerele unitatii de stocare.
Altele	Unitatea de stocare trebuie sa dispuna de redundanta la nivelul componentelor si facilitati hot-plug la nivel de: ventilatoare controllere, surse, unitati de disc/SSD, module I/O;
Format	Rackmount 19”, cu sine de montaj incluse
Suport si garantie	Sistemul de stocare va beneficia de 3 ani garantie. Serviciile de instalare ale echipamentului vor fi asigurate de personal autorizat din partea producatorului echipamentului.

3.3.1.8. Server de backup – 18 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Form factor	Rackmount -2U echipat cu sine de montaj in rack incluse
Procesoare instalate	2 procesoare cu urmatoarele specificatii minimale: - Procesor ultima generatie min. 8-core cu frecventa 2GHz, 11 MB cache, HT, VT;
Memorie	128 GB DDR4 REG ECC 2400; suport arhitectura six-channel, sparing, mirroring, chipkill, minim 24 sloturi DIMM cu suport pentru: - minim 1.5TB in configuratie maximala (upgrade-uri ulterioare);
Retea	2 x 10Gbps RJ45, 2 x 10Gbps SFP+
Alimentare	Sursă redundantă hot-plug minim 1000W, eficienta 80Plus Platinum
Racire	Ventilatoare redundante
Stocare	12 x bay-uri hot-plug 3.5” echipate cu HDD-uri de 8TB; SD slot intern, suport NVMe Serverul include: 2 x SSD 480GB SATA tip Enterprise cu circuit PLI sau echivalent Controller hardware RAID 0,1,5,6,10 cu 2GB si baterie de backup inclusa, fara mentenanta
Interfete I/O	2 x PCI-E X16 Gen 3.0

Interfete	3 x USB 3.0, 1 x serial, VGA
Video	Controler video integrat cu minim 16MB memorie dedicata
Management	Management acustic si termic. Modul Management IPMI cu port dedicat 1Gbps, suport KVM-over-IP. Se va furniza o aplicatie pentru monitorizarea granulara a componentelor serverului, analiza predictive la defectare cel putin pentru procesor, memorie, unitati de disc/ssd, alertare proactiva erori (inclusiv alertare prin email), obtinere date de performanta, configurare remote a serverului, inventariere hardware (inclusiv P/N componente) si generare rapoarte pentru componentele incluse. Aplicatia va furniza informatii despre senzorii integrati (temperaturi si turatii ventilatoare), log sistem/ audit securitate, unitati disc, procesor, memorie, configurare BMC. Suport SNMP, SSL. Va permite colectarea in timp real a informatiilor legate de temperatura si consum de putere al nodurilor din sistem (indiferent de producatorul acestora) cu functionalitati incluse de power-capping. Solutia permite vizibilitate completa a serverelor din retea inclusiv la nivel de rack si permite reducerea consumului de putere si optimizarea alocarii resurselor neutilizate de procesare.
Sisteme de operare certificate de producator	Microsoft Windows Server, Vmware (Vmware Ready).
Conformitate	CE, ISO9001, ISO14001, electrosecuritate si electrocompatibilitate, sau echivalente Serverul trebuie sa fie marca inregistrata a producatorului acestuia si trebuie sa fie testat si validat/certificat sub aceasta marca.
Energie disipata	Se va prezenta un calcul al energiei disipate pentru configuratia propusa exprimata in BTU/h
Temperatura de functionare	10 °C - 35 °C
Sistem de operare preinstalat	Minim Windows Server 2016 Standard sau echivalent
Garantie	36 luni

3.3.1.9. Cate 1 librarie de benzi pentru fiecare server de backup cu urmatoarele caracteristici:

Caracteristica tehnica	**Cerinta tehnica minimala**	
Format carcasa	Carcasa montabila in rack, maxim 1U	
Drive-uri	Libraria de benzi va avea minim 1 drive LTO8 instalat cu conectivitate SAS.	
Sloturi	min 8 sloturi pentru casete;	
Gestionarea casetelor	Libraria va include un cititor de coduri de bare si magazie de incarcare-descarcare cu minim 8 slot-uri;	
Siguranta datelor	Sa suporte criptare;	
Management	Panou de control LCD care ofera posibilitatea vizualizarii starii de sanatate si activitatii drive-urilor si permite configurarea hardware si software a acestora; Web based prin port RJ-45 dedicat care permite vizualizarea starii de sanatate si activitatii drive-urilor, configurarea hardware si software a acestora, upgraded firmware pt librarie si drive-uri;	
Temperatura de operare	10 - 35 grade C	
Umiditate	20% - 80%	
Casete incluse	Ofertantul va include 1 caseta de curatare si 8 de casete RW LTO8	

3.3.1.10. Firewall – 36 bucati

Cerinte tehnice minimale	
Descriere generala	Echipament integrat de protectie in retea cu capabilitati de scanare antivirus, scanare antispam, control la nivel de aplicatie si prevenirea intruziunilor destinat folosirii ca o solutie de securitate unificata. Se va livra o solutie de 2 echipamente configurate in cluster de inalta disponibilitate. Protectia sistemului este critica dpdv al infrastructurii retelei, asadar modulele de securitate nu trebuie sa contina componente mecanice. Se va avea in vedere utilizarea unor procesoare specializate pentru asigurarea unei viteze superioare de procesare a traficului de date pentru asigurarea functionalitatilor de baza. Datorita necesitatii protectiei investitiei si a suportului, se solicita ca toate modulele de filtrare si tehnologiile aplicate sa provina de la acelasi producator.
Specificatii hardware	Pentru a asigura acuratete si performanta, toate modulele de protectie ce alcatuiesc modulele de securitate trebuie sa functioneze avand la baza un sistem de operare dedicat, dezvoltat de catre producatorul echipamentului. Nu este permisa folosirea unui sistem de operare comercial, pentru uz general. - Montabil in rack, maximum 1U rack unit - Minim 16 interfete 10/100/1000 Base- T RJ-45 - Minim 2 interfete 10/100/1000 Base-T RJ-45 pentru management - Minim 16 interfete SFP GE - Minim 2 porturi USB - 1 x port consola RJ45 - Storage inclus 480 GB
Performanta sistemului	- Firewall Throughput IPv4/IPv6: 32 Gbps - Firewall Throughput (pachete pe secunda) : 30 Mpps - IPSec VPN Throughput: 20 Gbps - Threat Protection Throughput (enterprise mix, firewall, application control, malware protection): 3 Gbps - Tunele IPSec VPN concurente: 2.000 - SSL-VPN Throughput: 2.5 Gbps - Concurrent session: 4.000.000 - New Session/Sec: 300.000 - Policies(Maxim): 10.000 - Configuratii redundante posibile: Activ/Activ, Activ/Pasiv - Licente pentru un numar nelimitat de utilizatori
Parametrii echipament	- Alimentare alternativa 100-240V, 50-60Hz - Consum maxim de putere: 185 W
Protocoale si standarde	Rutare/Retea: - Suport WAN multiplu - Suport PPPoE - Client/Server DHCP - Policy-based routing - Rutare dinamica IPv4/IPv6- RIP, OSPF,BGP, IS-IS, Multicast(IPv4) - Suport multi-zone - Rutare intre zone - VLAN Tagging(802.1q) - Wan load balancing cu ECMP si redundanta - Link aggregation (802.3ad) - Rutare intre VLAN-uri - Suport IPv6(Firewall, AntiVirus, Web-Filtering, IPS, DNS,Transparent Mode,SIP,rutare dinamica, Admin access, Management) Traffic shaping : - Policy-based - Suport DiffServ

	- Banda Garantata/Maxima/Prioritara - Shaping per- IP, per-Account Domenii virtuale: - Domenii Firewall/Rutare separate - Interfete VLAN separate High Availability: - Activ/ Activ, Activ/Pasiv - Statefull Failover - Link status monitor - Link failover - Server Load balancing Firewall : - NAT,PAT,Transparent - Rutare dinamica-RIP,OSPF,BGP,Multicast Policy-based NAT - Domenii Virtuale (NAT/Transparent) - VLAN Tagging (802.1q) - SIP/H.323/SCCP NAT Traversal - Suport session helpers (DCE-RPC, DNS, FTP, H.245, H.323, MGCP, ONC-RPC, PPTP, RSH, RTSP, SIP, TFTP, TNS) - Profile granulare de protectie per-policy - Suport proxy explicit, optimizare WAN, caching - suport explicit proxy & FTP proxy - Suport pentru autentificarea userilor la nivel de politici firewall : ▪ baza locala ▪ Windows AD ▪ External RADIUS/LDAP/TACACS+ ▪ XAUTH over RADIUS (IPSEC) ▪ RSA Secure ID ▪ 2-factor authentication cu tokenuri hardware sau software dedicate VPN: - PPTP,IPSec,SSL - Suport criptare DES, 3DES, AES - Autentificare SHA-l *I* MD5/SHA-256/SHA-384/SHA-512 - PPTP,L2TP,VPN Client pass through - Suport VPN "Hub and Spoke" - Autentificare IKE cu Certificate(x.509 v1 si v2) - IPSec NAT Traversal - Producatorul trebuie sa aiba in portofoliu client de VPN propriu - USB entropy token support Prevenirea intruziunilor : - Suport Anomalii de protocoale - Suport Semnaturi definite de utilizator - Suport Ipv6 Antivirus : - Suport Antivirus si Antispyware - Worm Prevention - Inspectie HTTP/HTTPS; POP/POP3S; SMTP/SMTPS; IMAP/IMAPS; FTP/FTPS; IM - Blocarea fisierelor in functie de tip sau dimensiune - Suport Ipv6 Antispam : - Inspectie SMTP/SMTPS; IMAP/IMAPS; POP/POPS Application control : - Identificarea si controlul la nivel de aplicatie (control Layer 7 indiferent de port/protocol)

	- Traffic shaping (per aplicatie) - Diff Serv per aplicatie - Suport inspectie trafic SSL Suport Data Loss Prevention - Identificarea si controlul datelor sensitive - Suport actiuni configurabile (block/log/archive) - Suport document fingerprinting Suport optimizare Wan - Bi-Directional/Gateway-to-Client/Gateway - Caching integrat si optimizarea - Accelerare CIFS/FTP/MAPI/HTTP/HTTPS/Generic TCP Wireless controlller : - Posibilitatea de a functiona ca si controler wireless - Suport pentru management centralizat a pana la 256 access point-uri fizice (in mod tunel)
Management	Administrare: - Consola, Telnet, SSH, HTTP/HTTPS,CLI - Utilizatori/ Administratori cu drepturi configurabile - Syslog, SNMP, log-uri interne, grafice, notificari email - System software rollback - Posibilitatea de management centralizat prin intermediul unui echipament dedicat Autentificare : - Baza de date locala - Integrare Active Directory - Integrare LDAP/RADIUS/Tacacs+ - IP/MAC address binding
Software	- Licente pentru activarea actualizarilor serviciilor Antivirus, Antispam, Prevenirea intruziunilor, Web Filtering. Valabilitate licente: 3 ani (36 luni).
Certificate	- Acuratetea filtrarii componentelor trebuie sa fie demonstrata de urmatoarele certificate: - ICSA: Firewall, VPN - SSL/TLS, IPS, Antivirus, IPSec - FCC Class A Part 15 - ISO 9001 pentru producator
Service si garantie	Garanţia echipamentului este de 3 ani de la receptia in locatia de instalare. In perioada de garantie, dacă echipamentul defect nu este remediat în maxim 30 de zile, produsul va fi schimbat cu unul nou. Se vor livra din partea producatorului update-uri de firmware pentru o perioada de 3 ani si servicii securitate, actualizari semnaturi conform licentelor.

3.3.1.11. Switch de agregare model 1- spital – 72 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Porturi	48 x porturi 10/100/1000 BASE-T (RJ-45)
	4 x porturi 1GBASE-X SFP combo ports
	4 x porturi SFP+ (din care 2 pot fi folosite pentru stacking)
	2 x porturi 10GBASE-T copper combo ports
	Compatibil cu 10GBASE-SR SFP+, 10GBASE-LR SFP+, 10GBASE-ER SFP+, 1000BASE-SX SFP, 1000BASE-LX SFP, 1000BASE-ZX SFP, 1000BASE-LX SFP
	Port de management Out Of Band dedicat 10/100/1000 BASE-T

	1 port de consola seriala implementat ca si conector RJ-45
	Stack number indicator LED
	Sasiu rackabil maxim 1U
	1 port USB 2.0
Performanta	Capacitate Switch Bandwidth minim 174 Gbps
	Frame Forwarding Rate minim 130 Mpps
	Layer 2 MAC Addreses : 16.000
	Procesor 64 biti MIPS, minim 1 Ghz
	1 GB ECC DDR3 DRAM
	4 GB eMMC Flash
	Sistem de operare modular, care permite repornirea unui modul fara intreruperea proceselor
	suport stackare prin porturile SFP+ (minim 8 unitati per stack)
	SYN attack protection
	CPU DoS Protection with traffic rate-limiting to management CPU
	Suport pentru 2 versiuni diferite de firmware in locatii diferite ale memoriei flash, una primara si una pentru backup
	sa poata stoca mai multe fisiere de configurare
	suport IEEE 802.az Energy Efficient Ethernet (EEE)
	suport JSON-RPC pentru "machine-to-machine" configuration
	suport pentru rularea de script-uri Python, script-uri TCL, posibilitatea de a rula script-uri bazate pe reguli de tip ACL
	suport link flaping detection cu posibilitatea de a loga si de a dezactiva portul respectiv si de a rula un script
	protocol de detectie a buclelor layer 2 (fara a fi bazat pe Spanning Tree)
	sub 4 micro seconds latency (64-byte packet)
	9216 octeti marimea unui pachet (Jumbo Frame)
Surse	minim 1 sursa de putere interna (maxim 64 W consum de putere)
	Sursele externe redundante de putere de minim 90 de W
QOS	1024 ingress bandwidth meters
	8 QoS egress queues/port
	Rate Limiting Granularity : 8 Kbps
	Layer 2 Trusted Mode (IEEE 802.1p tagging)
	RFC 2598 DiffServ Expedited Forwarding (EF)
	RFC 2597 DiffServ Assured Forwarding (AF)
	RFC 2474 DiffServ Precedence
	RFC 2475 DiffServ Core and Edge Router Functions
Agregare	Suport pentru LACP IEEE 802.3ad si Multi-switch Link Aggregation Groups (M-LAG)
	Link Aggregation cu suport pentru cel putin 8 porturi pe fiecare link de agregare, 128 load sharing trunks
VLAN-uri	Minim 4000 VLAN-uri simultane (port, protocol, IEEE 802.1q)
Protocoale rutare Layer 3	Static Unicast Routes
	Static Multicast Routes

	Routing Information Protocol (RIP) v1/v2
	Classless Inter-Domain Routing (CIDR)
	Internet Control Message Protocol (ICMP)
	ICMP Router Discover Protocol (IRDP)
	Address Resolution Protocol (ARP)
	Internet Group Management Protocol (IGMP) v1/v2/v3
	DHCP – Helper/Relay and Server
Performanta rutare Layer 3	25000 IPv4 Routes
	minim 1000 IPv4 ARP entries in hardware
	Graceful protocol restart
Management	Kerberos snooping
	sFlow v5
	Unicast Reverse Path Forwarding prin intermediul ACL-urilor
	RFC 854 – Telnet
	Suport RADIUS (Authentication & Accounting) si TACACS+
	Suport pentru profilurile de securitate: - Alocare dinamică de ACL-uri pe baza răspunsului la autentificare - Alocare dinamică de QoS bazată pe răspunsul la autentificare - Asignare dinamică a Vlan-ului bazată pe răspunsul la autentificare - Executarea unui script dinamic pe baza răspunsului la autentificare cum ar fi setările duplex, setările de auto-negociere, setările LLDP, etc.
	RFC 1155 – SMI v1
	RFC 1157 – SNMPv1
	RFC 1212 – Concise MIB Definitions, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs
	RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
	RFC 2068 – HTTP web server
	SSL/TLS transport suport
	RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
	RFC 2576 – Coexistence between SNMP v1, v2 and v3
	RFC 2578 - RFC 2580 SMIv2
	RFC 3410 – 3415 SNMPv3, user based security, encryption and authentication
	RFC 1866 HTML – for Web-basedLogin and WebBased management
	Secure Shell (SSH-2), Secure Copy (SCP-2) client & server, and SFTP client/server with encryption/authentication
	IEEE 802.3ab – 1000 Base-T
	IEEE 802.3z 1000BASE-X
	IEEE 802.1Q VLAN Tagging
	IEEE 802.3ad – Link Aggregation si Multi-switch Link Aggregation Groups (M-LAG)
	IEEE 802.3ae – 10 GigE
	IEEE 802.1D – Spanning Tree

	IEEE 802.1S – Multiple Spanning Tree
	IEEE 802.1W – Rapid Spanning Tree
	IEEE 802.1Q – Virtual LANs with Port-based VLANs
	IEEE 802.1v – VLAN classification by Protocol and Port
	IEEE 802.1p – Ethernet Priority with User Provisioning and Mapping
	IEEE 802.1X – Port-based Authentication, Web and MAC-based mechanisms
	ITU-T G.8032 Ethernet Ring Protection Switching
	RFC 768 – UDP
	RFC 783 – TFTP
	RFC 791 – IP
	RFC 792 – ICMP
	RFC 793 – TCP
	RFC 826 – ARP
	RFC 951, 1542 – BootP
	RFC 2030 – Simple Network Time Protocol (SNTP) Version 4 for IPv4
	RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification
	RFC 2131 – BOOTP/DHCP relay agent and DHCP server
	RFC 2865 RADIUS Authentication
	RFC 2866 RADIUS Accounting
	RFC 3579 RADIUS EAP support for 802.1x
	RFC 3164 – The BSD Syslog Protocol
	IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
	IEEE 802.1AB – LLDP
	ANSI/TIA-1057 – LLDP-MED
Rutare	RFC 826 – Ethernet ARP
	RFC 894 – Transmission of IP Datagrams over Ethernet Networks
	RFC 1027 – Using ARP to implement Transparent Subnet Gateways (Proxy ARP)
	RFC 1256 – ICMP Router Discovery Messages
	RFC 1519 – CIDR
	RFC 1812 – Requirements for IP Version 4 Routers
	RFC 2131 – BOOTP/DHCP relay agent and DHCP server
	RFC 2453 – RIP v2
	RFC 3046 – DHCP Option 82 with port and VLAN ID
	RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
	RFC 2475 – DiffServ Core and Edge Router Functions
	RFC 2597 – DiffServ Assured Forwarding (AF)
	802.1p Packet Priority
	RFC 1112 – Host Extensions for IP Multicasting (IGMPv1)
	RFC 2236 – IGMPv2
	RFC 2710 – MLDv1
	RFC 3376 – Internet Group Management Protocol, Version 3 (IGMPv3)

	Data Center Bridging eXchange (DCBX) (IEEE P802.1Qaz)
Rutare iPv6	RFC 1981 – Path MTU for IPv6
	RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
	RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
	RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
	RFC 2462 – Stateless Autoconfiguration
	RFC 2464 – IPv6 over Ethernet
	RFC 3513 – Addressing Architecture for IPv6
	RFC 3587 – IPv6 Global Unicast Address Format
	RFC 2462, IPv6 Stateless Address Auto Configuration – Host Requirements
	RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
Accesorii	sinele si toate accesoriile necesare montarii in rack
	cablurile de stackare (2 pentru fiecare switch)
Garantie	3 ani garantie
Certificari ISO	Producatorul sa fie certificat ISO 9001
Conformitate cu standarde europene	EN60950-1:2007, EN 55022:2006+ A1:2007 Class A, EN 61000-3-2,8-2006 (Harmonics),ETSI EN 300 386 v1.4.1, 2008-04 (EMC Telecommunications) sau echivalente

Notă: In switch-urile de agregare din fiecare spital se vor conecta echipamentele data terminal server, echipamentele acces point din fiecare spital, porturi de management ale echipamentelor din camera serverelor.

Numarul mediu de switch-uri per spital luat in calcul este de 4 bucati, dar alocarea finala se va realiza dupa efectuarea site-survey-urilor in fiecare locatie, in cadrul etapei de analiza. Deoarece spitalele participante la proiect sunt de marimi diferite si complexitate a retelei diferită, numarul de switch-uri poate varia de la 2-7 bucati/locatie, iar alocarea finala va fi detaliata in etapa de proiectare.

3.3.1.12. Switch model 2 – spital – 36 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Porturi	24 x porturi 1Gb/10 Gb SFP+ ports (conectivitate de fibra optica cu 1 Gbps si 10 Gbps)
	1 x port 10Gb/40 Gb QSFP+ (disponibil pentru stacking)
	2 x porturi 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 (toate porturile trebuie sa functioneze atat ca porturi in modul 40 Gigabit Ethernet cat si in modul 4 x 10G Gigabit Ethernet)
	Compatibil cu 10GBASE-SR SFP+, 10GBASE-LR SFP+, 10GBASE-ER SFP+, 10GBASE-ZR SFP+, 1000BASE-SX SFP, 1000BASE-LX SFP, 1000BASE-ZX SFP, 10/100/1000BASE-T SFP,
	Port de management Out Of Band dedicat 10/100/1000 BASE-T
	1 port de consola seriala implementat ca si conector RJ-45
	Sasiu rackabil maxim 1U
	1 port USB sau micro-USB
Performanta	Capacitate Switch Bandwidth minim 880 Gbps
	Layer 2 MAC Addreses : 270.000
	Procesor quad core nimim 2.3 Ghz
	minim 4 GB ECC DDR3 RAM

	32 GB Flash storage
	Sistem de operare modular, care permite repornirea unui modul fara intreruperea proceselor
	suport stackare flexibil prin urmatoarele moduri: 2 din porturile SFP+, 2 din porturile QSFP+
	SYN attack protection
	CPU DoS Protection with traffic rate-limiting to management CPU
	Suport pentru 2 versiuni diferite de firmware in locatii diferite ale memoriei flash, una primara si una pentru backup
	sa poata stoca mai multe fisiere de configurare
	suport cut-through si store-and-forward switching
	suport pentru stackare prin porturile de 10G SFP+ sau porturile QSFP28
	suport JSON-RPC pentru "machine-to-machine" configuration
	suport pentru rularea de script-uri Python, script-uri TCL, posibilitatea de a rula script-uri bazate pe reguli de tip ACL
	suport link flaping detection cu posibilitatea de a loga si de a dezactiva portul respectiv si de a rula un script
	protocol de detectie a buclelor layer 2 (fara a fi bazat pe Spanning Tree)
	9216 octeti marimea unui pachet (Jumbo Frame)
Surse	minim 2 surse interne redundante de 770W AC PSU hot swap
Ventilatoare	Minim 4, de tip Hot swap
QoS	Layer 2 Trusted Mode (IEEE 802.1p tagging)
	RFC 2598 DiffServ Expedited Forwarding (EF)
	RFC 2597 DiffServ Assured Forwarding (AF)
	RFC 2474 DiffServ Precedence
	RFC 2475 DiffServ Core and Edge Router Functions
Agregare	Suport pentru LACP IEEE 802.3ad si Multi-switch Link Aggregation Groups (M-LAG)
	Link Aggregation cu suport pentru cel putin 32 porturi pe fiecare link de agregare, 128 load sharing trunks
VLAN-uri	Minim 4000 VLAN-uri simultane (port, protocol, IEEE 802.1q)
Protocoale rutare Layer 3	Static Unicast Routes
	Static Multicast Routes
	Routing Information Protocol (RIP) v1/v2
	Open Shortest Path First (OSPF) v2/v3
	Classless Inter-Domain Routing (CIDR)
	Internet Control Message Protocol (ICMP)
	ICMP Router Discover Protocol (IRDP)
	Virtual Redundant Routing Protocol (VRRP)
	Address Resolution Protocol (ARP)
	Internet Group Management Protocol (IGMP) v1/v2/v3
	DHCP – Helper/Relay and Server
	Suporta prin licentiere suplimentara ulterioara BGP4, External BGP(EBGP) si internal BGP (IBGP)
	Suporta prin licentiere suplimentara ulterioara MPLS si H-VPLS

Performanta rutare Layer 3	minim 130000 IPv4 Routes in hardware
	minim 10000 external OSPF routes
	minim 122000 IPv4 ARP entries in hardware
	Graceful protocol restart
	Bidirectional forwarding detection
Management	Kerberos snooping
	sFlow v5
	Unicast Reverse Path Forwarding prin intermediul ACL-urilor
	suport pentru arhitectura de switching extinsa bazat pe IEEE 802.1BR prin crearea unui switch virtual, astfel switch-ul va fi similar unui slot in sasiu si va permite management centralizat al topologiei dintr-un singur loc
	RFC 854 – Telnet
	Suport RADIUS si TACACS+
	RFC 1155 – SMI v1
	RFC 1157 – SNMP
	RFC 1212 – Concise MIB Definitions, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs
	RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
	RFC 2068 – HTTP server
	SSL/TLS transport suport
	RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
	RFC 2576 – Coexistence between SNMP v1, v2 and v3
	RFC 2578 - RFC 2580 SMIv2
	RFC 3410 – 3415 SNMPv3, user based security, encryption and authentication
	RFC 1866 HTML – used for Web-based Network Login and WebBased management
	Secure Shell (SSH-2), Secure Copy (SCP-2) and SFTP client/server with encryption/ authentication
	IEEE 802.3ab – 1000 Base-T
	IEEE 802.3z 1000BASE-X
	IEEE 802.3ae 10GBASE-X
	IEEE 802.3ba 40GBASE-X
	IEEE 802.1Q VLAN Tagging
	IEEE 802.3ad – Link Aggregation si Multi-switch Link Aggregation Groups (M-LAG)
	IEEE 802.1D – Spanning Tree
	IEEE 802.1S – Multiple Spanning Tree
	IEEE 802.1W – Rapid Spanning Tree
	IEEE 802.1Q – Virtual LANs with Port-based VLANs
	IEEE 802.1v – VLAN classification by Protocol and Port
	IEEE 802.1p – Ethernet Priority with User Provisioning and Mapping
	IEEE 802.1X – Port-based Authentication, Web and MAC-based mechanisms
	ITU-T G.8032 Ethernet Ring Protection Switching

	RFC 768 – UDP
	RFC 783 – TFTP
	RFC 791 – IP
	RFC 792 – ICMP
	RFC 793 – TCP
	RFC 826 – ARP
	RFC 951, 1542 – BootP
	RFC 2030 – Simple Network Time Protocol (SNTP) Version 4 for IPv4
	RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification
	RFC 2131 – BOOTP/DHCP relay agent and DHCP server
	RFC 2865 RADIUS Authentication
	RFC 2866 RADIUS Accounting
	RFC 3579 RADIUS EAP support for 802.1x
	RFC 3164 – The BSD Syslog Protocol
	IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
	IEEE 802.1AB – LLDP
	ANSI/TIA-1057 – LLDP-MED
Rutare	RFC 826 – Ethernet ARP
	RFC 894 – Transmission of IP Datagrams over Ethernet Networks
	RFC 1027 – Using ARP to implement Transparent Subnet Gateways (Proxy ARP)
	RFC 1256 – ICMP Router Discovery Messages
	RFC 1519 – CIDR
	RFC 1765 – OSPF Database Overflow
	RFC 1812 – Requirements for IP Version 4 Routers
	RFC 2131 – BOOTP/DHCP relay agent and DHCP server
	RFC 2328 – OSPF Version 2
	RFC 2453 – RIP v2
	RFC 3046 – DHCP Option 82 with port and VLAN ID
	RFC 1587 OSPF NSSA Option
	RFC 3768 – VRRP - Virtual Router Redundancy Protocol v2
	RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
	RFC 2475 – DiffServ Core and Edge Router Functions
	RFC 2597 – DiffServ Assured Forwarding (AF)
	802.1p Packet Priority
	RFC 1112 – Host Extensions for IP Multicasting (IGMPv1)
	RFC 2236 – IGMPv2
	RFC 2710 – MLDv1
	RFC 3376 – Internet Group Management Protocol, Version 3 (IGMPv3)
	RFC 2362 PIM-SM (Edge-mode)

	Mrinfo, the multicast router information tool based on Appendix-B of draft-ietf-idmr-dvmrp-v3-11
	Data Center Bridging eXchange (DCBX) (IEEE P802.1Qaz)
	Priority Flow Control (IEEE 802.1Qbb)
	IGMPv1, v2, v3
Rutare iPv6	RFC 1981 – Path MTU for IPv6
	RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
	RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
	RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
	RFC 2462 – Stateless Autoconfiguration
	RFC 2464 – IPv6 over Ethernet
	Suport pentru RFC 2740 – OSPFv3 (prin licentiere suplimentara ulterioara)
	RFC 3513 – Addressing Architecture for IPv6
	RFC 3587 – IPv6 Global Unicast Address Format
	RFC 2462, IPv6 Stateless Address Auto Configuration – Host Requirements
	RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
Accesorii	Trebuie sa includa sinele si toate accesoriile necesare montarii in rack
Garantie	3 ani de la data receptiei in locatia de instalare
Certificari ISO	Producatorul sa fie certificat ISO 9001
Conformitate cu standarde europeene	EN60950-1:2006 2nd Ed., EN 55022:2010 Class A, EN 61000-3-2:2006 + A2:2009(Harmonics),ETSI EN 300 386 v1.6.1, 2012-09 (EMC Telecommunications)

3.3.1.13. UPS – spital – 36 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Tehnologie	On line dubla conversie
Putere iesire	8KVA/8KW
Tensiunea nominala iesire	230V
Tensiunea nominala intrare	230V, 400V trifazat
Frecventa tensiunii de intrare	40 - 70 Hz (detectare automată)
Tip intrare	Borne pt legare fire pe direct monofazat sau trifazat (1 faza + nul + impamantare) si (3 faze + nul + impamantare)
Randament la incarcare maxima	minim 95% la 70% sarcina
Forma de unda	Perfect sinusoidala
Distorsiune tensiune de ieşire	< 3%
Tip conector iesire	6 x IEC 320 C13 + 4 x IEC 320 C19 + borne pt legare fire pe direct (1 faza + nul + impamantare). Grupuri de prize controlate ce permit setarea secventelor de inchidere/deschidere, rebutare, inchidere programata
Bypass	Bypass intern (automat şi manual)
Tehnologie baterie	Baterie cu plăci de plumb şi acid, etanşată, care nu necesită întreţinere

Management inteligent baterie	Creste performanţa, durata de viaţă şi fiabilitatea bateriei prin încărcare inteligentă, reglând tensiunea de încărcare conform temperaturii bateriei
Timp de functionare la 75% sarcina	Minim 20 min (8KW)
Card de retea inclus	Da, pentru management in retea si cu sensor de temperatura
Panou comanda cu LCD	Da, cu afisare contor de energie si posibilitate setare /afisare IP card de retea direct de pe panoul de comanda
Dimensiuni H x W x D (mm)	432.00 mm x 263.00 mm x 715.00 mm, rackabil
Greutate	Maxim 120 Kg
Pierdere termică online	Maxim 1497.00 BTU/hr
Zgomot	Maxim 55.00 dBA
Management virtualizare	Trebuie sa permita oprirea masinilor virtuale in caz de oprire alimentare energie electrica (Gracefull Shutdown)
Garantie	Minim 36 de luni partea electronica si 24 de luni acumulatorii. Produsele defecte in perioada de garantie, se schimba de catre producator direct la beneficiarul final al echipamentului, fara costuri suplimentare pentru beneficiar.

3.3.1.14. Rack – spital – 18 bucati

Rack	Oferta va include si un rack de 47U inaltime, respectand standardul industrial de 19”, 800mm latime 1200mm adancime Rack-ul va fi echipat cu minim doua unitati de tip PDU verticale 32A cu 24 conectori C13 si 4 conectori C19. Rack-ul trebuie sa fie compatibil cu standardul EIA 310D. Alte solicitari: ● Usi din tabla perforata fata-spate ● Usa spate divizata vertical ● Organizatoare cabluri In rack se vor livra si 4 fiole pentru stingerea automata a incendiilor.Rack-ul va fi prevazut cu sitem de detectie si stingere incendiu.

Rack-ul va fi montat în camera serverelor din cadrul fiecărui spital din proiect. În cazul în care nu există deja o cameră a serverelor în cadrul spitalului sau nu este loc pentru montarea acestui rack în camera deja existentă, spitalul participant în proiect va pune la dispoziția proiectului un spațiu adecvat unei camere server din cadrul spitalului.

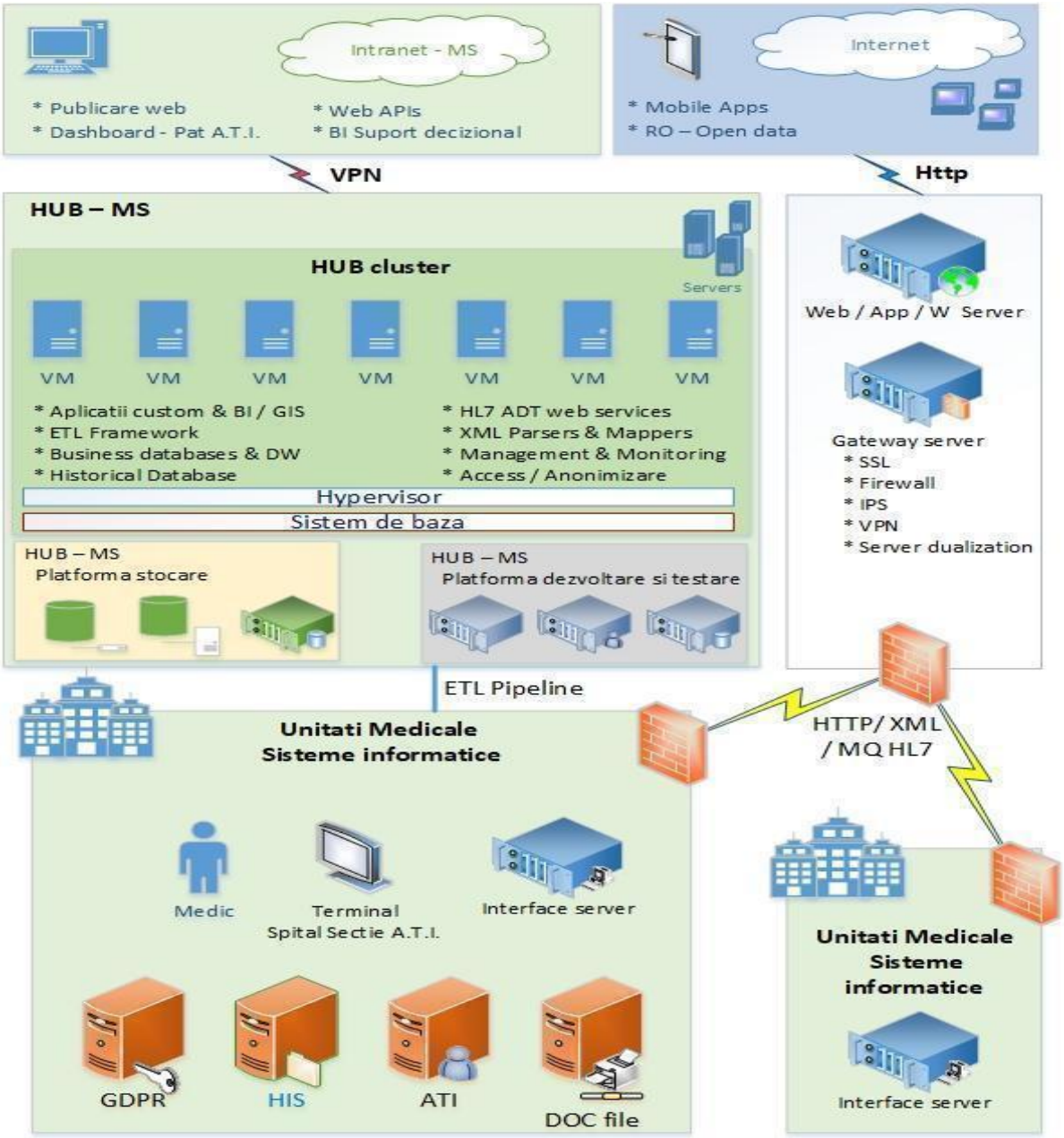
3.3.1.15. Climatizare – aer conditionat – 36 de bucati

In fiecare cameră a serverelor se va asigura climatizarea necesară – 2 echipamente pe locație de min. 45000 BTU, fiecare cu unitate interna standard duct 100Pa, FDUM, Qr/Qi=14.0/16.0kW,inverter, R410A si unitate externa Micro Inverter VSA, Qr/Qi=14.0/16.0kW, trifazata,R410A, filtru, comanda cu fir de perete, cu touch screen pentru fiecare pereche de echipamente din locație.
Aparatele se vor livra cu toată tubulatura necesară, tevi, sloturi refulare/aspiratie, țevi izolate, panou sandwich pentru canale de aer tip PIR, materiale conexe (tije filetate, sisteme de prindere și ancorare, cabluri electrice de alimentare și de automatizare etc.).Climatizarea va include unitatile interioare si exterioare precum si toate automatizarile necesare functionarii in bune conditii a echipamentelor IT.
Furnizorul va include cheltuielile de transport în locații, montajul in costul echipamentelor.

3.3.1.16. Cheltuieli de amenajare:

Ministerul Sanatatii are obligatia, impreuna cu spitalele partenere, sa puna la dispozitia Furnizorului un spatiu amenajat si igienizat, cu o instalatie electrica corespunzatoare consumului echipamentelor ce urmeaza a fi instalate (putere, amperaj, volum, suprafata, etc).

III.3.2. Echipamente hardware la nivel central HUB-MS



Fiug. 15. - hardware la nivel central HUB MS

Echipament monitorizare spitale centrul HUB MS – 5 bucati

CPU	minim 2.80GHz, minim 9MB cache, minim 6 nuclee si 6 fire de executie; set instrucţiuni pe 64 biţi, minim 11000 puncte conform testelor de benchmark publicate la adresa http://www.cpubenchmark.net
Memorie	minim 8GB RAM
Stocare	SSD min. 256GB NVMe, rata de citire min. 3200MB/s; rata de scriere min. 1300MB/s, MTBF min. 1.6 milioane ore

Carcasa	format mATX, format compact („Small Form Factor”) cu volum maxim 18 litri, pozitionare Tower si Desktop, 1x 5.25” bay extern, 2x 3.5” bay intern, sursa de alimentare minim 350W cu eficienta 80+ Bronze;
Porturi	1xLAN, 1x HDMI, 1x DVI, 1 x VGA, 10x USB (din care 4 x USB 3.0), 3x Audio Jack, 2 x PS/2 Sloturi: 2 x PCI-E, KB & MS,
Securitate	TPM, senzor de instruziune, incuietoare integrata pentru securizarea accesului in interiorul PC -ului (nu se acepta improvizatii de tip lacat)
Certificari oficiale	listare Windows 10 WHQL, Energy Star 6.1
Conformitati	CE, RoHS, CS, EMI, WEEE
Monitor	Minim 65”, rezolutie minima 1920x1080, minim conectori: DisplayPort 1.2, DVI-D, VGA, 2x HDMI, Component (BNC), Composite (BNC), RS232, RJ45, USB, Audio In – 3.5 mm jack, 2x RCA, Audio Out – 2x RCA, conector boxe externe
Boxe integrate	2 x 10W RMS
Consum	in stand by maxim 0.5W, MTBF min. 50.000 ore
Certificari	EPEAT, CE, UL/cUL, CB, GOST, C-Tick, RoHS, FCC, Class B sau echivalent
Garantie	minim 3 ani
Sistem de operare	pentru PC-uri, in ultima versiune lansată de producator, varianta Professional, care să permită conectarea la un domeniu de tip Active Directory si să includă drept de downgrade la versiuni anterioare (minim 1 versiune anterioară). Produsul va fi livrat licentiat in regim OEM sau echivalent, preinstalat si preactivat pe echipament
Program licentiat	Pentru restaurarea configuratiei de functionare optima software, respectiv utilitar (altul decat utilitarul System Restore inclus in sistemul de operare) de restaurare a sistemului de operare cu urmatoarele functionalitati minimale: • permite refacerea sistemului de operare de catre utilizator, prin intermediul unei interfete simple si intuitive • permite salvarea datelor utilizatorului inainte de procesul de restaurare (in functie de optiunea utilizatorului), prin crearea unei copii de siguranta. • permite creearea de catre utilizator, al unui set de medii optice de back-up (DVD sau CD), acesta permitand restaurarea S.O.-ului instalat initial pe sistem daca HDD-ul se defecteaza • este accesibil si in cazul deteriorarii sistemului de operare.

Platforma interconectare infrastructura convergenta – centru HUB MS – 1 bucata

Platforma infrastructura convergenta
● Solutia propusa trebuie sa fie un sistem integrat care sa contina unitati de procesare de tip server, componenta de retea si sistem de stocare. ● Soluţia oferită trebuie să fie oferită şi livrată cu servicii de instalare si montare intr-un rack standard de 42U livrat odata cu echipamentele (cu toate cablurile incluse între componente pentru server, echipamente stocare, switch-uri). ● Soluţia propusă trebuie să suporte conectivitatea de tip NFS si iSCSI la sisteme externe de stocare. ● Solutia propusa trebuie sa contina minim urmatoarele componente: ● Servere (noduri) de management; ● Servere (noduri) pentru procesare; ● Echipament de stocare; ● Echipamente de networking; ● Solutie de virtualizare ● Software de monitorizare si administrare.

- Sistemul propus trebuie să poată provizionat intr-un mod facil componentele de hardware si software
- Solutia propusa trebuie sa suporte scalabilitate de pana la minim 25 de noduri de procesare intr-un rack de 42U;
- Solutia propusa trebuie sa ofere suport pentru minim urmatoarele sisteme de operare: Linux, Microsoft Windows.

Servere/noduri de management:

- Solutia va include minim doua servere de management;
- Fiecare dintre cele doua servere de management va fi echipat cu minim doua procesoare cu minim 18 core-uri fiecare avand o frecventa de minim 2.3 GHz;
- Fiecare dintre cele doua servere de management va include minim 256GB RAM DDR4 (cu posibilitatea de upgrade la 1.5TB) si minim doua discuri de 1.2 TB 10000 rpm SAS-3.
- Fiecare server de management va dispune minim de urmatoarele porturi:
    - Minim patru porturi 10 Gigabit Ethernet
    - Minim doua porturi de mare viteza, minim 32 Gb/sec
    - 1GbE management port
- Fiecare server trebuie sa dispune de surse de alimentare redundante.
- Fiecare server de management trebuie sa ocupe un spatiu de maxim 1U in rack.
- Serverele de management trebuie sa fie preinstalate cu aplicatiile necesare si precablate in solutia ofertata.

Servere/noduri de procesare tip 1

Aceste noduri vor fi folosite pentru instalarea următoarelor componente de infrastructură software şi aplicații: baza de date relațională, integrare ETL, soluție de raportare.

- Solutia propusa trebuie sa includa minim doua servere de procesare
- Solutia propusa trebuie sa fie scalabila pana la minim 25 servere intr-un rack de 42U.
- Fiecare server trebuie sa fie echipat cu minim doua procesoare, fiecare avand minim 24 core-uri si o frecventa de minim 2,1 GHz
- Fiecare server va fi echipat cu minim 384 GB RAM DDR4 (cu posibilitate de upgrade la minim 1.5TB) si minim doua discuri SAS-3, 10000 rpm, cu o capacitate de minim 1.2 TB fiecare.
- Fiecare server va include un controller RAID SAS3 12Gb cu minim 2GB cache.
- Fiecare server de de procesare va dispune minim de urmatoarele porturi:
    - Minim doua porturi 10 GbE si minim doua porturi 25 GbE cu interfata SFP28
    - Minim doua porturi de mare viteza, minim 32 Gb/sec
    - 1GbE management port.
- Fiecare server va include surse de alimentare si ventilatoare redundante de tip hot-swapp.
- Fiecare server de procesare trebuie sa ocupe maxim 1U in rack.
- Serverele vor folosi mecanismul de virtualizare recomandat de producătorul bazei de date relaționale ofertate.
- Serverele de procesare trebuie sa fie preinstalate si precablate in solutia ofertata.

Unitatea de stocare aferenta nodurilor de procesare tip 1

- Sistemul de stocare inclus trebuie sa dispuna de controller-e redundante
- Fiecare controller al sistemului de stocare trebuie sa includa minim 384GB cache
- Fiecare unitate de tip controller va dispune de minim doua SSD-uri avand o capacitate minima de 3TB fiecare pentru accelerarea operatiunilor de citire
- Fiecare unitate de tip controller va dispune de minim doua porturi de mare viteza de minim 32 Gb/s.
- Sistemul de stocare trebuie sa includa o capacitate de:
    - minim 24TB, realizata cu discuri de minim 10K rpm
    - minim 800GB realizata cu discuri de tip SSD dedicata pentru accelerarea operatiunilor de scriere.
- Sistemul trebuie să permita acces de tip fișier la informațiile stocate prin intermediul protocoalelor NFS, CIFS/SMB, HTTP, WebDAV, FTP/SFTP/FTPS
- Sistemul trebuie să permita acces de tip bloc la informațiile stocate prin intermediul protocoalelor iSCSI, FC, IP over InfiniBand sau echivalaent
- Sistemul de stocare ofertat trebuie sa include posibilitatea de replicare locala, in interiorul aceluias sistem

- Sistemul de stocare ofertat trebuie sa suporte minim urmatoarele niveluri RAID: 0, 1, 5, 6 sau echivalent (striping, mirroring, triple-mirroring, single-parity RAID, double-parity RAID)
- Sistemul de stocare ofertat trebuie sa suporte minim urmatoarele protocoale de management: HTTPS, SSH, SNMP v1/v2c, IPMI
- Solutia de stocare trebuie sa suporte checksum data si metadata
- Solutia de stocare ofertata trebuie sa fie preinstalata si precablata in solutia ofertata.

Solutia de networking ofertata trebuie sa fie redundanta si compusa din minum urmatoarele echipamente (fiecare dintre ele va fi ofertat in configuratie redundanta)

- Switch-uri de mare viteza pentru intreconectarea echipamentelor
- Switch-uri pentru management
- Fabric interconnect-uri

Switch-uri de mare viteza pentru intreconectarea echipamentelor de tip 1 si 2:

- Solutia ofertata va include doua switch-uri de mare viteza, intr-o arhitectura de tip "non-blocking"
- Fiecare dintre aceste switch-uri va fi echipat cu minim 36 porturi de minim 32 Gb/sec
- 4 x port 10Gb/40 Gb QSFP+
- 4 x porturi 10Gb/25Gb/40Gb
- Fiecare dintre aceste switch-uri va fi echipat cu ventilatoare redundante
- Fiecare dintre aceste switch-uri trebuie sa suporte un throughput de minim de 2.3Tb/sec bidirectional
- Latenta port-to-port sa fie de maxim 100ns
- MTU: 4,094 bytes
- Switch-urile trebuie sa suporte crearea de "clustere virtuale" izolate
- Switch-urile trebuie sa suporte izolarea traficului si QoS
- Switch-urile trebuie sa dispuna de functionalitati de monitorizare a functiilor critice
- Switch-urile trebuie sa suporte minim urmatoarele protocoale de management: IPMI v1.5/v2.0, SNMP v1/v2c/v3, SSH, HTTP/HTTPS, syslog
- Fiecare switch trebuie sa dispuna de port dedicat pentru management
- Switch-urile trebuie sa suporte mecanisme de detectare automata a problemelor de conectivitate (automated connectivity check)
- Fiecare switch trebuie sa dispuna de surse de alimentare redundante si hot swappable

Switch-uri pentru management:

- Solutia propusa trebuie sa includa switch-uri de management redundante
- Fiecare dintre switch-uri trebuie sa includa minimum 20 porturi de 1Gb cu conector RJ45
- Fiecare port trebuie sa suporte viteze de 1Gbps si 100Mbps
- Fiecare dintre switch-uri trebuie sa includa minimum patru porturi 10GbE SFP+ (porturile trebuie sa suporte si viteze de 1GbE)
- Fiecare dintre switch-uri trebuie sa includa surse de alimentare redundante si ventilatoare de tip hot-swapp

Fabric interconnect-uri:

- Solutia propusa trebuie sa includa minim 2 echipamente de tip "*fabric interconnect*" redundante pentru conectarea unificata la retea locala (LAN) si/sau la un echipament de stocare extern (FC)
- Fiecare echipament de tip "fabric interconnect" va dispune de min 20 de porturi de mare viteza de minim 32 Gb/sec pentru conectarea la echipamentele de tip server (procesare si management) si la echipamentul de stocare.
- Echipamentele de tip "fabric interconnect" ofertata trebuie sa fie preinstalate si precablate in solutia ofertata
- Fiecare echipament de tip "fabric interconnect" trebuie sa dispuna de module Ethernet totalizand un numar de minim 16 porturi 10GbE SFP+
- solutia ofertata trebuie sa include un numar de minim 8 transceiver-e SFP+
- Fiecare echipament de tip fabric interconnect trebuie sa suporte module de accces la retea SAN (fibre channel) totalizand un numar de minim patru porturi FC
- Fiecare echipament de tip fabric interconnect trebuie sa suporte management prin port Ethernet dedicat, RS232 sau USB.

- Fiecare echipament de tip fabric interconnect trebuie sa dispuna de surse de alimentare si ventilatoare redundantede tip hot-swapp.

Servere/noduri de procesare tip 2

Aceste noduri vor fi folosite pentru instalarea următoarelor componente de infrastructură software şi aplicaţii: soluţie antivirus, management echipamente de comunicatii securizare (firewall si AP), soluţie dashboard HUB MS.

- Solutia propusa trebuie sa includa minim doua servere de procesare virtualizare
- Fiecare nod sa contina minim 2 procesoare cu urmatoarele caracteristici minime 10-core cu frecventa nativa 2.2GHz, 20 MB cache, HT, VT;
- Fiecare nod va fi echipat cu minim 96GB DDR4 REG ECC; suport arhitectura six-channel, sparing, mirroring, chipkill, minim 24 sloturi DIMM cu suport pentru minim 3TB in configuratie maximala (upgrade-uri ulterioare); suport memorie persistenta tip optane (sau echivalent, module de minim 512GB);
- Fiecare nod de procesare va dispune minim de urmatoarele porturi: 2 x 10Gbps RJ45, 4 x 10Gbps SFP+
- Fiecare nod de procesare va avea surse de alimentare redundantă hot-plug minim 1000W, eficienta 80Plus Platinum si racire cu ventilatoare redundante de tip hot-swapp
- Fiecare nod de procesare trebuie sa ocupe maxim 1U in rack si sa aiba incluse sinele de rack
- Fiecare nod de procesare trebuie sa fie dotat cu minim 8 x bay-uri hot-plug 2.5”; SD slot intern, suport NVMe
- Fiecare nod de procesare trebuie sa includa minim: 2 x SSD 480GB SATA tip Enterprise cu circuit PLI sau echivalent si sa fie dotat cu controller hardware minim RAID 0,1
- Fiecare nod de procesare trebuie sa fie dotat cu minim 2 Interfete I/O PCI-E X16 Gen 3.0 si 3 x USB 3.0, 1 x serial, VGA
- Fiecare nod de procesare sa fie dotat cu un controler video integrat cu minim 16MB memorie dedicata
- Nodurile de procesare de virtualizare trebuie sa aiba minimal asigurate minim facilitatile enumerate mai jos:
    - management acustic si termic
    - modul Management IPMI cu port dedicat 1Gbps, suport KVM-over-IP.
    - Aplicatie pentru monitorizarea granulara a componentelor nodurilor de procesare virtualizare, sa faca: analiza predictiva la defectare cel putin pentru procesor, memorie, unitati de disc/ssd, alertare proactiva erori (inclusiv alertare prin email), obtinere date de performanta, configurare remote a serverului si generare rapoarte pentru componentele incluse.
    - aplicatia sa furnizeze informatii despre senzorii integrati (temperaturi si turatii ventilatoare), log sistem/ audit securitate, unitati disc, procesor, memorie, configurare BMC. Suport SNMP, SSL.
    - sa permita colectarea in timp real a informatiilor legate de temperatura si consum de putere al nodurilor din sistem (indiferent de producatorul acestora) cu functionalitati incluse de power-capping. Solutia permite vizibilitate completa a serverelor din retea inclusiv la nivel de rack si permite reducerea consumului de putere si optimizarea alocarii resurselor neutilizate de procesare.
- Nodurile de procesare virtualizare trebuie sa fie compatibile cu solutia de virtualizare descrisa la capitolul software si sa fie certificate de catre producatorul acesteia

- Nodurile de procesare virtualizare trebuie sa fie licenţiate perpetuu pentru minim Windows Server 2016 Standard
- Minim certificate CE, ISO9001, si conformitate electrosecuritate si electrocompatibilitate sau echivalent

Unitatea de stocare aferenta nodurilor de procesare tip 2

Nodurilor de procesare tip 2 se vor conecta la un modul de stocare dedicat cu urmatoarele caracteristici minimale:

- minim doua controller-e cu minim 2 procesoare fiecare, procesoarele avand minim 4-core si o frecventa de minim 2.2Ghz. cu minim 20MB cache
- interfete de interconectare: minim 4 porturi 10 Gb Ethernet SFP+ per controller, minim 2 porturi 10 Gb Ethernet RJ45 per controller, minim 2 porturi 1 Gb Ethernet RJ45 per controller, 1 port remote management (KVM-over-IP)
- sa ocupe maxim 6U, cu sine de montaj incluse
- memorie cache minim 96GB de tip RAM instalata pe fiecare controller
- 2x400GB SSD SAS 12Gbps cache citire 3DWPD
- 2x400GB SSD SAS 12Gbps cache scriere 10DWPD
- minim 2 sloturi PCI-e per controller pentru posibilitatea de suplimentare a porturilor de conectare
- capacitate de stocare bruta instalata: minim 24 x 6 TB HDD SAS hot-swap
- modulul de stocare virtualizare trebuie sa aiba suport pentru cel putin 1PB
- modulul de stocare virtualizare trebuie sa dispuna de redundanta la nivelul componentelor si facilitati hot-plug la nivel de: ventilatoare, surse, unitati de disc/SSD, module I/O;
- modulul de stocare virtualizare trebuie sa dispuna minimal de urmatoarele facilitati de fiabilitate, disponibilitate, mentenanta:
    - metode de autodiagnosticare si izolare a defectelor
    - sa functioneze in configurate de cluster activ-activ sau activ-pasiv cu minim o pereche de noduri. In cazul in care un controller din perechile de noduri este scos din productie (din cauza unor defectiuni sau operatiuni de mentenanta), celalalt nod/pereche trebuie sa preia sarcinile si resursele asignate anterior nodului inactiv;
    - diagnosticare si rezolvare in cel mai scurt timp a problemelor aparute (de exemplu, administratorul trebuie sa aiba vizibilitate si posibilitati de analiza in timp real asupra intregului Sistem de stocare de tip NAS/transport a datelor);
    - la operatiuni de upgrade a sistemului de operare sa nu fie afectata disponibilitatea modulului de stocare virtualizare; Inlocuirea discurilor defecte trebuie sa se poata realiza cu modulul de stocare in functiune, fara intreruperea accesului la date.
- modulul de stocare virtualizare trebuie sa dispuna minimal de urmatoarele caracteristici software si facilitati aditionale:
    - sa suporte mecanisme de optimizare a procesului de stocare si protectie a datelor: compresie LZ4, deduplicare, thin provisioning;
    - sa suporte acces de tip fisier la informatiile stocate prin intermediul protocoalelor NFS, SMB si acces de tip bloc la informatiile stocate prin intermediul protocoalelor iSCSI, FC;
    - sa suporte in mod standard caching/ tiering si functii de clonare si replicare; sa includa in mod standard un numar nelimitat de clone si snapshot-uri.
    - sa includa in mod standard urmatoarele functionalitati de redundata si integritate a datelor: Data & metadata checksumming, self-healing, paritate tripla si suporta functionalitati de recovery tip on-site si off-site.
    - sa suporte functionalitati pentru backup si disaster recovery.
- Modulul de stocare virtualizare trebuie sa fie certificat pentru solutia de virtualizare descrisa la capitolul software
- Modulul de stocare virtualizare trebuie sa fie compatibil cu urmatoarele: VMware, Microsoft Windows, Microsoft Hyper-V, Microsoft Active Directory, Citrix, Linux, RHEL, MacOS, XEN, OpenStack
- modulul de stocare virtualizare trebuie sa dispuna minimal de urmatoarele caracteristici pentru monitorizare si alertare:
    - sa permita monitorizarea in timp real si sa alerteze automat, inclusiv prin e-mail, administratorul de sistem.
    - configurarea si administrarea modulul trebuie sa se poata realiza prin interfata web/ CLI.
    - sistemul de management trebuie sa includa functionalitatea de roll-back la o stare anterioara.
    - sa includa suport pentru: SNMP, REST API
    - sistemul de management trebuie sa ruleze integral pe controllerele unitatii de stocare

Serviciile de instalare ale echipamentului vor fi asigurate de personal autorizat din partea producatorului echipamentului.

Se va prevedea o librarie de benzi cu urmatoarele caracteristici:

- Libraria de benzi va ocupa maxim 3U, va include kit de montare în rack 19", şi va avea următoarele caracteristici minimale:
- Va fi dotată cu braţ robotic intr-o arhitectura modulară care ofera posibilitatea de extindere pe masura creşterii în volum a necesarului de date ce trebuie salvate-restaurate.
- Va fi echipata cu minim de 30 de slot-uri licentiate si activate cu posibilitate de extensie pana la minim 400.
- Va fi echipata cu cel puţin 2 unitati de citire/scriere (drive-uri) LTO-8 cu interfata SAS cu posibilitate de extensie pana la 30 drive-uri.
- Libraria trebuie sa poata fi administrată şi monitorizată prin intermediul unui browser web sau a unui software dedicat echivalent, detectând şi eliminând erorile apărute în funcţionarea normala a librăriei;
- Va fi prevazută cu un panou de control cu ecran LCD ce va oferi operatorului o metodă simplificată de instalare, configurare, control si diagnosticare;
- Va fi dotată cu unităţi de citire/scriere si surse de alimentare care să nu necesite oprirea librariei pentru a fi inlocuite (hot swap);
- Libraria va fi certificata pentru cel putin 2 milioane de cicluri load/unload ale bratului robotic de schimbare a casetelor.
- Trebuie să includă cel puţin 20 de casete LTO-8 si 5 de curatare a capetelor de citire/scriere.

Server aplicatie backup – centru HUB MS – 1 bucata

Caracteristica tehnica	Cerinte tehnice minimale
Carcasa	- Rackmount 1U; Echipamentul trebuie să poata fi instalat în rack-uri de 19"
CPU	- Server-ul trebuie să fie echipat cu minim 2 cpu de ultimă generaţie procesoare cu urmatoarele specificatii minimale: 12-core cu frecventa nativa 2.2GHz, 20 MB cache, HT, VT;
Memorie RAM	- Modelul ofertat trebuie sa aiba minim - 24 slot-uri pentru memorie RAM; - Configuratia ofertata trebuie sa fie includa minim 128 GB memorie RAM.
Stocare	- Modelul ofertat trebuie sa suporte minim 8 unitati interne de stocare de tip SAS: HDD, SSD - configuratia ofertata trebuie sa contina minim 2 x 600GB SAS 10krpm
Porturi si Sloturi I/O	- serverul ofertat trebuie sa dispuna de minim 3 sloturi PCIe x8 - server-ul trebuie sa fie echipat cu minim: o 2 porturi 1/10GB RJ45; o doua porturi SAS 12Gbps; o un port 1000Base-T dedicat pentru management o un port serial RJ-45;
Sistem de operare şi software adiţional	- Sistemul ofertat trebuie să fie echipat cu un sistem de operare licenţiat de tip Windows sau Linux. Configuratia ofertata trebuie să includă licenţe pentru sistemul de operare pentru toate core-urile instalate.
Sursa de alimentare	- minim 2 surse de alimentare redundante de tip hot-swap
Ventilatie	- sa dispuna de ventilatoare redundante de tip hot-swap
Garantie	- 3 ani

Firewall – centru HUB MS – 2 bucati

Cerinte tehnice minimale	
Descriere generala	Echipament integrat de protectie in retea cu capabilitati de rutare Layer 3, precum si capabilitati avansate de securitate precum scanare antivirus, scanare antispam, control la nivel de aplicatie, prevenirea intruziunilor, filtrare WEB, destinat folosirii ca o solutie de securitate unificata. Se va folosi un cluster de 2 echipamente configurate in regim de inalta disponibilitate. Functionalitatile de baza trebuiesc accelerate folosind ASIC-uri specializate, iar echipamentul trebuie sa suporte configurarea atat in modul Transparent, cat si in modul NAT. Datorita necesitatii protectiei investitiei si a suportului, este impedios necesar ca toate modulele de filtrare si tehnologiile aplicate (incluzand sistemul de operare) sa provina de la acelasi producator. Sistemul nu trebuie licentiat per numar de utilizatori (nu exista numar limitat de utilizatori).
Specificatii hardware	Pentru a asigura acuratete si performanta, toate modulele de protectie ce alcatuiesc modulele de securitate trebuie sa functioneze avand la baza un sistem de operare dedicat, dezvoltat de catre producatorul echipamentului. Nu este permisa folosirea unui sistem de operare comercial, pentru uz general. - Montabil in rack, maximum 2U rack unit - 2 x interfete dedicate pentru management/HA GE RJ-45 - 16 x interfete GE RJ45 - 16 x interfete GE SFP - 2 x interfete 10 GE SFP+ - 2 x USB - 1 x port consola RJ-45 - Suport pentru aduagarea unei surse interne redundata de putere

	- 1 modul de stocare intern instalat de minim 250 GB GB
Performanta sistemului	- Firewall Throughput IPv4/IPv6 (packete UDP de 1518 bytes): 52 Gbps - Firewall Throughput IPv4/IPv6 (packete UDP de 512 bytes): 52 Gbps - Firewall Throughput IPv4/IPv6 (packete UDP de 64/86 bytes): 33 Gbps - Firewall Throughput (pachete pe secunda) : 49 Mpps - IPSec VPN Throughput (512 bytes): 25 Gbps - SSL-VPN Throughput: 3.6 Gbps - NGFW Throughput: 5 Gbps - Tunele IPSec VPN concurente: 20.000 - Concurrent sessions (TCP): 10.500.000 - New Session/Sec: 280.000 - Politici de firewall : 100.000 - Suport definire pana la 10 firewall-uri virtuale (tabele separate de rutare) fara licenta aditionala - Configuratii redundante posibile: Activ/Activ, Activ/Pasiv - Licentiat pentru un numar nelimitat de utilizatori
Parametrii echipament	- Alimentare alternativa 100-240V, 50-60Hz, - Consum mediu de putere: 160 W
Protocoale si standarde	Rutare/Retea: - Suport WAN multiplu - Suport PPPoE - Client/Server DHCP - Policy-based routing - Rutare dinamica IPv4/IPv6- RIP, OSPF ,BGP, IS-IS, Multicast(IPv4) - Suport multi-zone - Rutare intre zone - VLAN Tagging(802.1q) - Link aggregation (802.3ad) - Rutare intre VLAN-uri - Multi-link aggregation(802.3ad) - Suport IPv6 (Firewall, AntiVirus, Web-Filtering, IPS, DNS, Transparent Mode, SIP, rutare dinamica, Admin access, Management) - Suport pentru redirectarea traficului utilizand ICAP si WCCP Traffic shaping : - Policy-based - Suport DiffServ - Banda Garantata/Maxima/Prioritara - Shaping per- IP, per-Policy, per application Domenii virtuale: - Domenii Firewall/Rutare separate - Posibilitatea de folosire mixta a domeniilor virtuale in modul Transparent/NAT - Interfete VLAN separate High Availability: - Activ/Activ, Activ/Pasiv, virtual clustering - Statefull Failover - Link status monitor - Link failover - Server Load balancing Firewall : - NAT, PAT, Transparent - Rutare dinamica-RIP, OSPF, BGP, Multicast, Policy-based NAT - Domenii Virtuale (NAT/Transparent) - VLAN Tagging (802.1q) - SIP/H.323/SCCP NAT Traversal

	- Suport session helpers (DCE-RPC, DNS, FTP, H.245, H.323, MGCP, ONC-RPC, PPTP, RSH, RTSP, SIP, TFTP, TNS) - Profile granulare de protectie per-policy - Suport proxy explicit - Suport pentru autentificarea userilor la nivel de politici firewall : ▪ baza locala ▪ Windows AD ▪ External RADIUS/LDAP/TACACS+ ▪ XAUTH over RADIUS (IPSEC) ▪ RSA Secure ID ▪ 2-factor authentication cu tokenuri hardware/software dedicate VPN: - PPTP, IPSec, SSL - Suport criptare DES, 3DES, AES - Autentificare SHA-l *I* MD5 - PPTP, L2TP, VPN Client pass through - Suport VPN "Hub and Spoke" - Autentificare IKE cu Certificate (x.509 v1 si v2) - IPSec NAT Traversal - Producatorul trebuie sa aiba in portofoliu client de VPN propriu, atat pentru PC-uri cat si pentru device-uri mobile Prevenirea intruziunilor : - Suport pentru detectarea anomaliilor de protocol - Protecţie bazată pe semnături predefinite (minim 7.000 de semnaturi) dar şi suport pentru semnături custom. - Suport Ipv6 - Update-uri automate pentru semnături. - Protecţie împotriva DDoS. Antivirus : - Suport Antispyware - Worm Prevention - HTTP/HTTPS;POP/POP3S;SMTP/SMTPS;IMAP/IMAPS;FTP/FTPS;IM - Blocarea fisierelor in functie de tip sau dimensiune - Suport Ipv6 - Suport pentru integrarea cu o solutie externa de tipul „sandbox”, care poate fi atat on-premise, cat si in cloud Antispam : - Inspectie SMTP/SMTPS;IMAP/IMAPS;POP/POPS - Suport IP address check, URL check, email checksum - Suport Helo DNS lookup, return email DNS check, black/white list Application control : - Identificarea si controlul la nivel de aplicatie cu minim 3.000 de semnaturi (control Layer 7 indiferent de port/protocol) - Traffic shaping (per aplicatie) - Diff Serv per aplicatie - Suport inspectie trafic SSL Suport Data Loss Prevention - Identificarea si controlul datelor sensitive - Suport actiuni configurabile (block/log/archive) - Suport document fingerprinting Filtrare WEB - Blocarea accesului utilizatorilor la site-uri de tip malitios sau cu continut nepotrivit folosind o baza de date globala cu certificare recunoscuta. - Posibilitatea definirii de liste statice cu URL-uri permise/blocate

	- Posibilitatea de customizare a categoriilor globale prin suprascriere Wireless controlller : - Posibilitatea de a functiona ca si controler wireless - Suport pentru management centralizat pentru minim 1.000 de access access point-uri fizice Identificarea device-urilor: - Colectarea informatiilor device-urilor conectate la retea precum adresa MAC, adresa IP, sistem de operare, hostname, username. Antimalware/ATP : - Capabilitati Anti-botnet prin utilizarea unei baze de date de tipul IP reputation si respective URL reputation, cu capabilitati de terminare a conexiunilor de comunicatie catre serverele de tip Command & Control - Posibilitatea de a utiliza un framework de semnaturi ATP pentru protectia utilizatorilor cu device-uri mobile cum ar fi Android, pentru detectia si prevenirea atacurilor. - Posibilitatea de a primi update-uri dinamice (checksum-uri ale fisierelor malitioase si URL-urilor) folosind baza de date a solutiei de sandbox (atat on-premise cat si cloud based) pentru a suplimenta baza de date de malware deja existent pe echipament
Management	Administrare: - Consola, Telnet, SSH, HTTP/HTTPS, CLI - Utilizatori/ Administratori cu drepturi configurabile - Syslog, SNMP, log-uri interne, grafice, notificari email - System software rollback - Posibilitatea de management centralizat prin intermediul unui echipament dedicat Autentificare : - Baza de date locala - Integrare Active Directory - Integrare LDAP/RADIUS/Tacacs+ - IP/MAC address binding - Suport 2-factor authentication
Software	- Licente pentru activarea actualizarilor serviciilor Antivirus, Antispam, Prevenirea Intruziunilor, Web Filtering
Certificate	Acuratetea filtrarii componentelor trebuie sa fie demonstrata de urmatoarele certificate: - ICSA: Firewall, VPN - SSL/TLS, IPS, Antivirus - FCC Class A Part 15 - ISO 9001 pentru producator
Service si garantie	Garanţia echipamentului este de 3 ani de la receptia in locatia de instalare. In perioada de garantie, dacă echipamentul defect nu este remediat în maxim 30 de zile, produsul va fi schimbat cu unul nou. Se vor livra din partea producatorului update-uri de firmware pentru o perioada de 3 ani si servicii securitate, actualizari semnaturi conform licentelor.

Switch agregare model 1 –centru HUB MS– 2 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Porturi	48 x porturi 10/100/1000 BASE-T (RJ-45)
	4 x porturi 1GBASE-X SFP combo ports
	4 x porturi SFP+ (din care 2 pot fi folosite pentru stacking)
	2 x porturi 10GBASE-T copper combo ports

	Compatibil cu 10GBASE-SR SFP+, 10GBASE-LR SFP+, 10GBASE-ER SFP+, 1000BASE-SX SFP, 1000BASE-LX SFP, 1000BASE-ZX SFP, 1000BASE-LX SFP
	Port de management Out Of Band dedicat 10/100/1000 BASE-T
	1 port de consola seriala implementat ca si conector RJ-45
	Stack number indicator LED
	Sasiu rackabil maxim 1U
	1 port USB 2.0
Performanta	Capacitate Switch Bandwidth minim 174 Gbps
	Frame Forwarding Rate minim 130 Mpps
	Layer 2 MAC Addreses : 16.000
	Procesor 64 biti MIPS, minim 1 Ghz
	1 GB ECC DDR3 DRAM
	4 GB eMMC Flash
	Sistem de operare modular, care permite repornirea unui modul fara intreruperea proceselor
	suport stackare prin porturile SFP+ (minim 8 unitati per stack)
	SYN attack protection
	CPU DoS Protection with traffic rate-limiting to management CPU
	Suport pentru 2 versiuni diferite de firmware in locatii diferite ale memoriei flash, una primara si una pentru backup
	sa poata stoca mai multe fisiere de configurare
	suport IEEE 802.az Energy Efficient Ethernet (EEE)
	suport JSON-RPC pentru "machine-to-machine" configuration
	suport pentru rularea de script-uri Python, script-uri TCL, posibilitatea de a rula script-uri bazate pe reguli de tip ACL
	suport link flaping detection cu posibilitatea de a loga si de a dezactiva portul respectiv si de a rula un script
	protocol de detectie a buclelor layer 2 (fara a fi bazat pe Spanning Tree)
	sub 4 micro seconds latency (64-byte packet)
	9216 octeti marimea unui pachet (Jumbo Frame)
Surse	minim 1 sursa de putere interna (maxim 64 W consum de putere)
	1 sursă externă redundantă de putere de minim 90 de W
QOS	1024 ingress bandwidth meters
	8 QoS egress queues/port
	Rate Limiting Granularity : 8 Kbps
	Layer 2 Trusted Mode (IEEE 802.1p tagging)
	RFC 2598 DiffServ Expedited Forwarding (EF)
	RFC 2597 DiffServ Assured Forwarding (AF)
	RFC 2474 DiffServ Precedence
	RFC 2475 DiffServ Core and Edge Router Functions
Agregare	Suport pentru LACP IEEE 802.3ad si Multi-switch Link Aggregation Groups (M-LAG)
	Link Aggregation cu suport pentru cel putin 8 porturi pe fiecare link de agregare, 128 load sharing trunks

VLAN-uri	Minim 4000 VLAN-uri simultane (port, protocol, IEEE 802.1q)
Protocoale rutare Layer 3	Static Unicast Routes
	Static Multicast Routes
	Routing Information Protocol (RIP) v1/v2
	Classless Inter-Domain Routing (CIDR)
	Internet Control Message Protocol (ICMP)
	ICMP Router Discover Protocol (IRDP)
	Address Resolution Protocol (ARP)
	Internet Group Management Protocol (IGMP) v1/v2/v3
	DHCP – Helper/Relay and Server
Performanta rutare Layer 3	25000 IPv4 Routes
	minim 1000 IPv4 ARP entries in hardware
	Graceful protocol restart
Management	Kerberos snooping
	sFlow v5
	Unicast Reverse Path Forwarding prin intermediul ACL-urilor
	RFC 854 – Telnet
	Suport RADIUS (Authentication & Accounting) si TACACS+
	Suport pentru profilurile de securitate: - Alocare dinamică de ACL-uri pe baza răspunsului la autentificare - Alocare dinamică de QoS bazată pe răspunsul la autentificare - Asignare dinamică a Vlan-ului bazată pe răspunsul la autentificare - Executarea unui script dinamic pe baza răspunsului la autentificare cum ar fi setările duplex, setările de auto-negociere, setările LLDP, etc.
	RFC 1155 – SMI v1
	RFC 1157 – SNMPv1
	RFC 1212 – Concise MIB Definitions, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & TRAPs
	RFC 1901 – 1908 SNMPv2c, SMIv2 and Revised MIB-II
	RFC 2068 – HTTP web server
	SSL/TLS transport suport
	RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
	RFC 2576 – Coexistence between SNMP v1, v2 and v3
	RFC 2578 - RFC 2580 SMIv2
	RFC 3410 – 3415 SNMPv3, user based security, encryption and authentication
	RFC 1866 HTML – for Web-basedLogin and WebBased management
	Secure Shell (SSH-2), Secure Copy (SCP-2) client & server, and SFTP client/server with encryption/authentication
	IEEE 802.3ab – 1000 Base-T
	IEEE 802.3z 1000BASE-X
	IEEE 802.1Q VLAN Tagging

	IEEE 802.3ad – Link Aggregation si Multi-switch Link Aggregation Groups (M-LAG)
	IEEE 802.3ae – 10 GigE
	IEEE 802.1D – Spanning Tree
	IEEE 802.1S – Multiple Spanning Tree
	IEEE 802.1W – Rapid Spanning Tree
	IEEE 802.1Q – Virtual LANs with Port-based VLANs
	IEEE 802.1v – VLAN classification by Protocol and Port
	IEEE 802.1p – Ethernet Priority with User Provisioning and Mapping
	IEEE 802.1X – Port-based Authentication, Web and MAC-based mechanisms
	ITU-T G.8032 Ethernet Ring Protection Switching
	RFC 768 – UDP
	RFC 783 – TFTP
	RFC 791 – IP
	RFC 792 – ICMP
	RFC 793 – TCP
	RFC 826 – ARP
	RFC 951, 1542 – BootP
	RFC 2030 – Simple Network Time Protocol (SNTP) Version 4 for IPv4
	RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification
	RFC 2131 – BOOTP/DHCP relay agent and DHCP server
	RFC 2865 RADIUS Authentication
	RFC 2866 RADIUS Accounting
	RFC 3579 RADIUS EAP support for 802.1x
	RFC 3164 – The BSD Syslog Protocol
	IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
	IEEE 802.1AB – LLDP
	ANSI/TIA-1057 – LLDP-MED
Rutare	RFC 826 – Ethernet ARP
	RFC 894 – Transmission of IP Datagrams over Ethernet Networks
	RFC 1027 – Using ARP to implement Transparent Subnet Gateways (Proxy ARP)
	RFC 1256 – ICMP Router Discovery Messages
	RFC 1519 – CIDR
	RFC 1812 – Requirements for IP Version 4 Routers
	RFC 2131 – BOOTP/DHCP relay agent and DHCP server
	RFC 2453 – RIP v2
	RFC 3046 – DHCP Option 82 with port and VLAN ID
	RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
	RFC 2475 – DiffServ Core and Edge Router Functions
	RFC 2597 – DiffServ Assured Forwarding (AF)
	802.1p Packet Priority
	RFC 1112 – Host Extensions for IP Multicasting (IGMPv1)

	RFC 2236 – IGMPv2
	RFC 2710 – MLDv1
	RFC 3376 – Internet Group Management Protocol, Version 3 (IGMPv3)
	Data Center Bridging eXchange (DCBX) (IEEE P802.1Qaz)
Rutare iPv6	RFC 1981 – Path MTU for IPv6
	RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
	RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
	RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
	RFC 2462 – Stateless Autoconfiguration
	RFC 2464 – IPv6 over Ethernet
	RFC 3513 – Addressing Architecture for IPv6
	RFC 3587 – IPv6 Global Unicast Address Format
	RFC 2462, IPv6 Stateless Address Auto Configuration – Host Requirements
	RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
Accesorii	include sinele si toate accesoriile necesare montarii in rack
	cablurile de stackare (2 pentru fiecare switch)
Garantie	Minim 3 ani garantie
Certificari ISO	Producatorul sa fie certificat ISO 9001
Conformitate cu standarde europene	EN60950-1:2007, EN 55022:2006+ A1:2007 Class A, EN 61000-3-2,8-2006 (Harmonics),ETSI EN 300 386 v1.4.1, 2008-04 (EMC Telecommunications)sau echivalent

UPS – centru HUB MS – 2 bucati

Caracteristica tehnica	**Cerinta tehnica minimala**
Tehnologie	On line dubla conversie
Putere iesire	10KVA/10KW
Tensiunea nominala iesire	230V
Tensiunea nominala intrare	230V, 400V trifzat
Frecventa tensiunii de intrare	40 - 70 Hz (detectare automată)
Tip intrare	Borne pt legare fire pe direct monofazat sau trifazat (1 faza + nul + impamantare) si (3 faze + nul + impamantare)
Factor creasta	3:1
Forma de unda	Perfect sinusoidala
Distorsiune tensiune de ieşire	< 2%
Tip conector iesire	6 x IEC 320 C13 + 4 x IEC 320 C19 + borne pt legare fire pe direct (1 faza + nul + impamantare) . Grupuri de prize controlate ce permit setarea secventelor de inchidere/deschidere, rebutare, inchidere programata
Bypass	Bypass intern (automat şi manual)
Tehnologie baterie	Baterie cu plăci de plumb şi acid, etanşată, care nu necesită întreţinere

Management inteligent baterie	Creste performanţa, durata de viaţă şi fiabilitatea bateriei prin încărcare inteligentă, reglând tensiunea de încărcare conform temperaturii bateriei
Timp de functionare la 100% sarcina	Minim 10 min (10KW)
Card de retea inclus	Da, pentru management in retea si cu sensor de temperatura
Panou comanda cu LCD	Da, cu afisare contor de energie si posibilitate setare /afisare IP card de retea direct de pe panoul de comanda
Dimensiuni H x W x D (mm)	432.00 mm x 263.00 mm x 715.00 mm, rackabil
Greutate	Maxim 130 Kg
Pierdere termică online	Maxim 2000.00 BTU/hr
Zgomot	Maxim 55.00 dBA
Management virtualizare	Trebuie sa permita oprirea masinilor virtuale in caz de oprire alimentare energie electrica (Gracefull Shutdown)
Garantie	Minim 36 de luni partea electronica si 24 de luni acumulatorii. Produsele defecte in perioada de garantie, se schimba de catre producator direct la beneficiarul final al echipamentului , fara costuri suplimentare pentru beneficiar.

Rack – centru HUB MS – 1 bucata

Rack	Oferta va include si un rack de 47U inaltime, respectand standardul industrial de 19”, 800mm latime 1200mm adancime Rack-ul va fi echipat cu minim doua unitati de tip PDU verticale 32A cu 24 conectori C13 si 4 conectori C19. Rack-ul trebuie sa fie compatibil cu standardul EIA 310D sau echivalent. Alte solicitari: ● Usi din tabla perforata fata-spate ● Usa spate divizata vertical ● Organizatoare cabluri In rack se vor livra si 4 fiole pentru stingerea automata a incendiilor.

Climatizare – centru HUB MS – 2 bucati

Echipamentele vor fi de min. 45000 BTU, fiecare cu unitate interna standard duct 100Pa, FDUM, Qr/Qi=14.0/16.0kW,inverter, R410A si unitate externa Micro Inverter VSA, Qr/Qi=14.0/16.0kW, trifazata,R410A, filtru, comanda cu fir de perete, cu touch screen.
Aparatele se vor livra cu toată tubulatura necesară, tevi, sloturi refulare/aspiratie, țevi izolate, panou sandwich pentru canale de aer tip PIR, materiale conexe (tije filetate, sisteme de prindere și ancorare, cabluri electrice de alimentare și de automatizare etc.).
Furnizorul va include cheltuielile de transport în locații, montajul in costul echipamentelor.

Laptop-uri experti echipa de implementare – 15 bucati

Componenta	Cerinta tehnica minimala
Placa de baza	Fabricata sub aceeasi marca cu sistemul de calcul
Procesor	Numar nuclee: 4
	Numar fire de executie: 8
	Frecventa de baza: 1.80 GHz cu posibilitate crestere pana la ce putin 4.50 GHz
	Memorie cache: 8 MB
	Suport tehnologie 64bit

Memorie RAM 16 GB DDR4 2400 MHz cu suport Dual Channel si posibilitate de extindere pana la cel putin 32GB
Slot sau sloturi libere pentru a permite dublarea memoriei
Unitate de stocare interna SSD SATA III 450 GB
Placa video 2 GB memorie
Frecventa de lucru: min. 300 MHz
Suporta DirectX 12, OpenGL 4.4
Suport triple display
Audio Placa audio integrata High-definition
Boxe stereo integrate
microfoane integrate
Comunicatii integrate Retea 10/100/1000 Gigabit Ethernet
Modul WLAN 802.11 ac
Bluetooth 5.0
Porturi integrate 2 x USB 3.0 (din care unul permite alimentarea dispozitivelor USB chiar si cand portabilul este inchis);
(nu se accepta adaptoare) 1 x USB Type-C;
1 x Audio-Out, Audio-In;
1 x DisplayPort / HDMI;
1 x LAN (RJ-45)
Sloturi integrate Slot Memory Card Reader cu suport pentru cel putin SD/SDHC/SDXC

(nu se accepta adaptoare)
Slot SmartCard
Ecran Tip: LED
Diagonala 15.6”
Rezolutie 1920 x 1080 pixeli
Format 16:9

Camera web integrata HD
Tastatura US-Layout cu bloc numeric dedicat si iluminare led
Touchpad integrat
Prevazuta cu protectie impotriva varsarii accidentale de lichide
Carcasa
Baterie Baterie Li-Polymer min. 3 celule,
Mouse Optical wheel mouse 1000 dpi, interfata USB
Geanta Geanta de transport de dimensiunea laptop-ului prevazuta cu manere, bretea de transport reglabila si compartimente multiple pentru laptop, accesoriile acestuia, documente si ustensile de scris.

Sistem de operare Microsoft Windows 10 Professional preinstalat si licentiat perpetuu cu cheie de activare rezidenta in BIOS
Aplicatie software de birou Microsoft Office 2019 Home & Business (minim) preinstalat si licentiat perpetuu cu cheie unica de activare
Caracteristici de securitate Slot de securitate de tip Kensington.
Posibilitatea de a seta parole diferite pentru boot, BIOS si Hard-disk

Solutie hardware dedicata rezidenta in BIOS (diferita de formatarea sau simpla stergere a datelor) care sa stearga informatiile critice de pe unitatea de stocare folosind algoritmi de stergere diferiti in functie de importanta datelor (de la un ciclu de stergere pana la 35 de cicluri de stergere - algoritmul Guttmann) si care sa poata fi accesata de la distanta.
Cititor de amprenta integrat, inclusiv aplicaţie software dedicată Chip/modul de securitate integrat pe placa de baza tip TPM 2.0 care ofera posibilitatea criptarii datelor atat hardware cat si software

Management, back-up si restaurare de date Aplicatie de monitorizare si management local si de la distanta, cu cel putin urmatoarele functionalitati :

- Rapoarte detaliate despre componentele sistemului
- BIOS Management
- Alerte (via ASF)
- WoL (Wake on LAN)
- Gestionarea statii de lucru pe baza de serie
- Management energetic
- Diagnosticare de la distanta
- Managementul driverelor si patch-urilor

Solutie de recovery pentru sistemul de operare ofertat dezvoltata de catre producatorul sistemului licentiata si livrabila pe suport optic de tip CD/DVD

Drivere software pentru sistemul de operare Microsoft Windows 10 Professional disponibile pe site-ul producatorului

Conformitate cu standarde europene si internationale, 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
- Mediu inconjurator: WEEE, Energy Star 6.1

Compatibilitate cu sistemele de operare Certificare Microsoft Windows 10 Professional (HCL) pentru echipamentul ofertat

Garantie: Echipamentul trebuie sa includă garanţie cu suport tehnic de la producator pentru 3 ani de tip 24x7, next business day, la sediul beneficiarului.

3.3.2.11 Multifunctional A3 color, print, copy, scan, fax

Caracteristica	Cerinta tehnica minimala
Multifunctional A3 color, print, copy, scan, fax	
Viteza copiere/imprimare A4	minim 25 A4/minut color si alb-negru
Viteza copiere/imprimare A3	minim 15 A3/minut color si alb-negru
Timp de incalzire	maxim 20 secunde
Printare prima copie color	maxim 7.5 secunde
Printare prima copie alb-negru	maxim 6.1 secunde
Rezolutie copiator	600 x 600 dpi
Greutate hartie	minim 52 - 300 g/mp
Caseta 1	500 coli la 80g/mp, A5–A3, 52–256 g/mp
Caseta 2	500 coli la 80g/mp, A5–SRA3, 52–256 g/mp
Duplex automat	inclus
Alimentator automat de originale	100 coli la 80g/mp, 35 - 128 g/mp
Stand	inclus, cu rotile si spatiu de stocare
Display echipament	9 inch / Capacitiv, multi-touch, Webbrowser standard
Capacitate de alimentare	Standard: 150 coli la 80gmp tava manuala + 2x500 coli Maxim: 6.650 coli
Imprimanta	
Viteza copiere/imprimare A4	minim 25 A4/minut color si alb-negru
Viteza copiere/imprimare A3	minim 15 A3/minut color si alb-negru
Memorie	2 GB Standard 4 GB Maxim

HDD	minim 250 GB, optional HDD mirroring
Rezolutie Printare	1,800 x 600 dpi; 1.200 x 1.200 dpi
Conectivitate	10BaseT/100BaseTX/1000 BaseT USB 1.1/2.0
Protocoale de printare suportate	PCL6, PCL5e/c, PostScript 3, XPS Ver. 1
Format maxim	SRA3 (320 x 450 mm)
printare hartie banner	297 x 1.200 mm
Mobile Printing	AirPrint, Mopria, Google Cloud Print (optional), WiFi Direct (optional), NFC Authentication and Pairing
Scanare	
Rezolutie scanare	600 x 600 dpi
Viteza scanare	standard minim 80 ipm la 300 dpi, optional minim 160 ipm la 300dpi
Format scanare	JPEG; TIFF; PDF; PDF Compact; PDF encriptat;XPS; XPS Compact;
Functii scanare	Scanare catre E-Mail, Scanare catre FTP, Scanare catre Box (HDD), Scanare catre PC (SMB), Network Twain, Scanare catre WebDAV, Scanare catre Me, Scanare catre Home, Scanare catre USB, Scanare catre Scan Server, Scanare catre Web Service (WSD-Scan), Device Profile for Web Services (DPWS)
Consumabile incluse	
Tonere C,Y,M	26,000 pagini/culoare - 3 seturi.
Toner Black	28,000 pagini - 3 buc.
Unitatati de Imagine C,Y,M	90,000 pagini/culoare
Unitate de Imagine Black	120,000 pagini
Unitate developare K,C,Y,M	600,000 pagini/culoare

3.4. Componenta de securitate a sistemului

Nota: FHIR nu este un protocol de securitate și nici nu definește funcționalitati de securitate. Cu toate acestea, FHIR definește protocoale de schimb și modele ale continutului datelor care trebuie utilizate cu diverse protocoale de securitate definite in continuare si grupate pe : securitatea schimbului de date, autorizare si acces, audit, semnatura digitala, atasamente, politici in data management, validari de input in sistem)

Solutia de securitate trebuie sa:
- să ofere un mecanism de protecție împotriva aplicațiilor periculoase;
- să includă un modul de monitorizare a stării autorităților de certificare (CA);
- să includă un serviciu care previne scurgerea de informații confidențiale prin intermediul fișierelor în interiorul instituției.
- Securitatea rețelei se va realiza în regim distribuit, prin echipamente firewall de tip next-generation în fiecare locație de implementare. Firewall-urile vor avea funcționalități de criptare a traficului, algoritmi și baze de semnături de recunoaștere a malware-ului și a atacurilor cibernetice sofisticate, inclusiv funcții de sandboxing. La nivelul serverelor fizice și virtuale se va utiliza o soluție antivirus.
- Protecția datelor va începe din momentul introducerii informațiilor în sistem și va fi asigurată prin definirea și documentarea nivelurilor de protecție și luarea deciziilor de control al accesului.
- Sistemul trebuie să asigure protecția datelor pe tot parcursul ciclului de viață al acestora: creare, modificare, stocare, transport și distrugere.

Componenta de securitate trebuie să asigure următoarele servicii de:
- Identificare și autentificare asigurate pe baza implementării unui mecanism de autentificare

- serviciul de managementul identității va fi integrat cu sisteme de tip LDAP) pentru fiecare locatie.
- Autorizarea și controlul accesului asigurate pe baza criteriilor: grupuri, roluri și permisiuni (RBAC), prin mecanisme care să permită suspendarea conturilor inactive după o perioadă determinată prin politicile interne de securitate și care să permită limitarea numărului de încercări de conectare nereușite.
- Integritate ce vor fi asigurate prin utilizarea algoritmilor de criptare
- Confidențialitate asigurate pe baza criptării datelor stocate cât și criptarea datelor aflate în tranzit (VPN).
- Securizarea retelelor va fi asigurata pe baza unor soluții de firewall care să asigure protecție împotriva atacurilor cibernetice și protecție anti-malware.
- Responsabilitate (non-repudiation) asigurate pe baza creării de log-uri privind evenimentele și acțiunile utilizatorilor în sistem.

3.4.1. Securitatea sistemului la nivel de spitale (sectii ATI si SO)

Sistemul trebuie să includă mecanisme care permit accesul la date şi informaţii pentru personalul autorizat din mai multe secţii pe 3 nivele:
- secţie-secţie
- medic-secţie
- permisiune pacient

după cum urmează:
- secţie-secţie: pacientul transferat de la o secţie la alta. Personalul din secţia primitoare poate vedea parţial sau integral dosarul electronic cu datele pacientului (exemplu personalul ATI cardiologie poate vedea datele colectate pe durata cât pacientul a fost operat);
- medic-secţie: medicii pot vedea dosarul unui pacient transferat succesiv la mai multe secţii ale spitalului. Dacă de exemplu un pacient tratat la ATI este trimis la operaţie (altă secţie) medicul poate vedea dosarul de la Sala Operație (SO) chiar dacă nu există acces secţie-secţie;
- permisiune pacient: pacientul poate cere limitarea accesului la datele sale, nivelul de prioritate în acest caz fiind deasupra celor 2 anterioare (chiar dacă există acces secţie-secţie, dreptul pacientului prevalează). Key-userii pot stabili ce personal are acces la dosar şi niciun alt user nu îl poate accesa, indiferent de drepturile sale generale de acces.

Pentru diverse situații specifice, este necesară existența unui modul/aplicație de personalizare, accesibilă numai key-userilor, prin intermediul interfeței fiind posibilă personalizarea aplicației ATI și Săli Operație (SO).
Aplicația ATI și Săli Operație (SO) trebuie să aibă funcționalități de monitorizare a utilizării sistemului: să permită monitorizarea intrărilor în sistem şi acţiunilor efectuate), ce user a accesat datele cărui pacient, când, pentru cât timp, care sunt userii care au vizualizat datele pacientului x, datele căror pacienţi au fost accesate de user y, etc.).

3.4.2. Solutie de securizare de tip antivirus pentru servere

Produsul este o platforma integrata pentru managementul securitatii, gandita ca o solutie modulara. Produsul contine o consola de management care asigura functionalitati de administrare. Protectie servere fizice si servere virtuale. Soluția de securizare trebuie să poată fi extinsă ulterior printr-un modul de securizare a echipamentelor de tip stații, dispozitive mobile.
Consola de management trebuie să îndeplinească minim următoarele cerințe:

1. Instalare si configurare:
    1. Pachetul de instalare va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template se va putea importa in:
        a. VMware vSphere

b. Citrix XenServer
c. Microsoft Hyper-V
d. Red Hat Enterprise Virtualization
e. KVM
f. Oracle VM.

2. Consola de management se livreaza cu o baza de date inclusa care este de tip non-relationala, pentru o functionare cat mai rapida, fara a fi nevoie de licente aditionale.
3. Solutia va fi scalabila, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe masini virtuale sau pe aceeasi masina virtuala.
4. Masinile de scanare pentru mediile virtuale VMware si Citrix se insteaza la distanta prin task din consola de management, iar pentru alte platforme se descarca separat din interfata web a produsului.
5. Rolurile principale trebuie sa fie cel putin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web.
6. Solutia va include aditional si un modul de balansare (load balancer) pentru cazurile in care mai multe masini virtuale ale componentei de management sunt instalate cu acelasi rol (pentru Load Balancing si performanta/redundanta).
7. Solutia va include un mecanism de configurare a disponibilitatii pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe masini virtuale.

2. Cerinte generale:

1. Interfata consolei de management va fi in limba romana.
2. Interfata clientului de securitate, care se instaleaza pe statii si servere, va fi in limba romana.
3. Manualul de instalare a produsului va fi in limba romana.
4. Manualul de administrare a produsului va fi in limba romana.
5. Produsul suporta licentierea per procesor fizic (socket). In felul acesta numarul masinilor virtuale poate varia oricand, ele fiind protejate.
6. Solutia va include un modul de update server prin care se asigura actualizarea de produs si a semnaturilor.
7. Solutia va pemite activarea/dezactivarea actualizarilor de produs/semnaturi.
8. Solutia permite stabilirea actualizarii automate a consolei de management prin stabilirea recurentei zilnice, saptamanale sau lunare, dar si prin stabilirea intervalului orar in care acesta se va actualiza. De asemenea, permite si trimiterea unei alerte de nefunctionalitate, cu 30 de minute inainte de actualizare.
9. Pentru o mai buna urmarire a actualizarilor consolei de management, solutia permite vizualizarea unui jurnal de modificari in care sunt precizate istoric:
    a. versiunea consolei de management
    b. data versiunii
    c. functii noi si imbunatatiri
    d. probleme rezolvate
    e. probleme cunoscute
10. Notificarile – prezente in interfata, notificarile necitite sunt evidentiate, trimise catre una sau mai multe adrese de email, alerteaza key-userii in cazul unor probleme majore: licentiere, detectie virusi, actualizari de produs disponibile).
11. Solutia va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware.
12. Solutia va permite instalarea serviciului de SMNP prin care se pot raporta statusul masinilor din cadrul componentei de management.
13. Solutia permite creare unei copii de siguranta a bazei de date a consolei de administrare, la cerere sau programata, putand fi stocata local, pe un server FTP sau in retea.

3. Panou de monitorizare si raportare (Dashboard):

1. Rapoartele din panoul de monitorizare vor putea fi configurate specificand numele raportului, tipul raportului, tinta raportului, optiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul dupa care o statie este considerata neactualizata).
2. Panoul central contine rapoarte pentru toate modulele suportate.
3. Rapoartele din panoul central de comanda permit: adaugarea altor rapoarte, stergerea lor si rearanjarea.

4. Inventarierea retelei – managementul securitatii:

1. Solutia se va integra cu domenii Active Directory multiple, VMware vCenter, Citrix Xen sau echivalente si importa inventarul acestor platforme.
2. Pentru integrarea cu Active Directory, se va putea defini si intervalul (in ore) de sincronizare si forta sincronizarea.
3. Se permite descoperirea masinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM.
4. Se permite descoperirea statiilor statii fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
5. Solutia va oferi optiuni de cautare, sortare si filtrare dupa numele sistemului, sistem de operare si adresa IP.
6. Solutia va permite instalarea la distanta sau manual a clientilor antimalware pe masini fizice/virtuale.
7. Solutia va permite selectarea modulelor componente atunci cand se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale.
8. Solutia va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
9. Solutia va oferi posibilitatea de repornire a masinilor fizice de la distanta.
10. Solutia va oferi informatii detaliate despre fiecare task si se fiseaza daca task-ul s-a finalizat sau nu cu succes.
11. Solutia va permite configurarea centralizata a clientilor antimalware prin intermediul politicilor
12. Se vor oferi in consola de management informatii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnaturi.
13. Solutia permite descoperirea tuturor aplicatiilor instalate pe toate statiile si serverele din reatea, prin rularea unui task din consola de administrare.

5. Politici:

1. Solutia va permite configurarea setarilor clientului antimalware prin intermediul unei singure politici ce contine setari pentru toate module
2. Politica va contine optiuni specifice de activare/dezactivare si configurarea functionalitatilor precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicatiilor, scanarea traficului web,controlul dispozitivelor, power user.
3. Solutia permite aplicarea politicilor pe masini client, grupuri de masini, pool-uri de resourse (VMware), domeniu, unitati organizationale sau useri de active directoy.
4. Politica sa poate fi schimbata automat in functie de:
   a. User-ul logat pe statie
   b. IP sau clasa de IP al statiei
   c. Gateway-ul alocat
   d. DNS serverul alocat
   e. Clientul este/nu este in acceasi retea cu infrastructura de management
   f. Tipul retelei (lan, wireless)

6. Rapoarte:

1. Solutia va contine rapoarte care prezinta statusul masinilor clienti din punct de vedere al actualizarilor, fisierelor malware detectate, aplicatiile blocate, site-urilor web blocate.

2. Rapoartele programate pot fi trimise catre un numar nelimitat de adrese de email (nu este nevoie sa aiba un cont in consola de management).
3. Solutia va permite vizualizarea rapoartelor curente programate de key-useri.
4. Solutia va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv.
5. Solutia include un generator de rapoarte care ofera posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, mentinand informatiile concise si ordonate corespunzator. Astfel, solutia include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange.
6. Interogarea legata de starea terminalului include informatii precum:
    a. tip masina
    b. infrastructura retelei careia ii apartine terminalul
    c. datele agentului de securitate
    d. starea modulelor de protectie
    e. rolurile terminalelor.
7. Interogarea legata de evenimente terminal include informatii precum:
    a. calculatorul tinta pe care a avut loc evenimentul
    b. tipul starea si configuratia agentului de securitate instalat
    c. starea modulelor si rolurilor de protectie instalate pe agentul de securitate
    d. denunmirea si alocarea politicii
    e. utilizatorul autentificat in timpul evenimentului
    f. evenimente (site-uri blocate, aplicatii blocate, detectiile etc)
8. Interogarea legata de evenimente Exchange include informatii precum:
    a. Directia traficului e-mail
    b. Evenimente de securitate (detectarea programelor de tip malware sau a fisierelor atasate)
    c. Masurile implementate in fiecare situatie (curatarea, stergerea, inlocuirea sau carantinarea fisierului, stergerea sau respingerea e-mail-ului)

7. Carantina:

1. Solutia va permite restaurarea fisierelor carantinate in locatia originala sau intr-o cale configurabila.
2. Carantina va fi locala, pe fiecare statia administrata si va fi administrata, fie local, fie din consola de magement
3. Permite descarcarea fisierelor carantinate doar pentru masinile virtuale protejate prin modulul mediilor virtuale integrat cu VMware vShield.

8. Utilizatori:

1. Administrarea se va putea face pe baza de roluri.
2. Roluri multiple predefinite: Key-user, Administrator companie, Administrator retea, Reporter sau rol personalizat.
    a. Administrator companie: administreaza arhitectura consolei de management;
    b. Administrator retea: administreaza serviciile de securitate;
    c. Reporter: monitorizeaza si genereaza rapoarte.
3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati in consola de management.
4. Se va permite configurarea detaliata a drepturilor administrative, permitand selectarea serviciilor si obiectelor pentru care un utilizator poate face modificari.
5. Se va permite deconectarea automata a oricarui tip de utilizator dupa un anumit timp pentru o protectie sporita a datelor afisate in consola de administrare. Acest interval se poate personaliza de key-useri..

9. Log-uri:

1. Inregistrarea actiunilor utilizatorilor.
2. Se vor oferi informatii detaliate pentru fiecare actiune a unui utilizator.
3. Se va permite filtrarea actiunilor utilizator dupa numele utilizatorului, actiune.

10. Actualizare:

1. Se permite definirea de locatii de actualizare multiple.
2. Se permite activarea/dezactivarea actualizarilor de produs si semnaturi.
3. Se permite actualizarea produsului intr-o retea fara acces la Internet.
4. Orice client antivirus sa poata fi configurat sa livreze update-urile catre alt client antivirus
5. Solutia dispune un server de actualizare (update) care face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fara interventia administratorului. Astfel, administratorul va putea descarca pachetele pentru protectia statiilor si serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata in mediile de virtualizare VMware, Hyper-V sau Citrix.
6. In cadrul serverului de actualizare, pentru o mai buna urmarire a actualizarilor pachetele pentru protectia statiilor si serverelor sau a pachetelor pentru modul de scanare centralizata, se va putea vizualiza un jurnal de modificari in care sunt precizate istoric:
    a. versiunea pachetului
    b. data versiunii
    c. functii noi si imbunatatiri
    d. probleme rezolvate
    e. probleme cunoscute
7. Solutia permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, inainte de a fi instalate pe toate statiile si serverele din retea, evitand posibile probleme ce pot afecta serverele sau statiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizari de produs:
    a. Ciclu rapid, gandit pentru un mediu de test in cadrul retelei
    b. Ciclu lent, gandit pentru restul retelei (productie, servere critice etc)
8. Solutia permite stabilirea zonelor de test si critice din cadrul retelei prin intermediul politicilor din consola de management.

11. Certificate:

1. Accesul la consola de management sa se faca doar prin HTTPS.
2. Serverul web, din consola centrala de management trebuie sa permita importarea de certificate digitale eliberate de o autoritate de certificare autorizata sau proprie organizatiei.
3. Solutia permite afisarea in consola de management informatii despre certificate: nume, autoritatea emitenta, data eliberarii si data expirarii certificatelor eliberate.

Protectie servere fizice și virtuale:

1. Caracteristici generale minimale:

1. Pentru reducerea la minim a consumului de resurse, solutia antimalware trebuie sa permita instalarea personalizata a modulelor detinute (de exemplu, sa permita instalarea solutiei antimalware fara modulul de control al accesului web, modul de control al dispozitivilelor sau modulul firewall).
2. Pentru o mai buna protectie a statiilor si serverelor, solutia include un vaccin anti-ransomware. Acest vaccin asigura protectia impotriva tuturor amenintarilor cunoscute de tip ransomware, prin imunizarea statiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
3. Vaccinul anti-ransomware primeste actualizari de la producator, odata cu actualizarea semnaturilor produsului Antimalware.
4. Pentru o mai buna protectie a statiilor si serverelor, solutia include protectie impotriva atacurilor zero-day de tip exploit (atacuri directionate).

2. Cerinte de sistem:

- Sisteme de operare pentru servere: Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows

Server 2008 R2, Windows Server 2008, Windows Small Business Server (SBS) 2003, Windows Server 2003 R2, Windows Server 2003 with Service Pack 1, Windows Home Server

- Sisteme de operare Linux: Red Hat Enterprise Linux / CentOS 5.6 sau mai recent, Ubuntu 10.04 LTS sau mai recent, SUSE Linux Enterprise Server 11 sau mai recent, OpenSUSE 11 sau mai recent, Fedora 15 sau mai actual and Debian 5.0 sau mai recent.

3. Administrare si instalare remote:

1. Inainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
2. Instalarea se va putea face in mai multe moduri:
    a. prin descarcarea directa a pachetului pe statia pe care se va face instalarea;
    b. prin instalarea la distanta, direct din consola de management
3. Instalarea clientilor la distanta in alte locatii decat cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locatiile respective pentru a minimiza traficul in WAN.
4. In consola vor fi disponibile informatii despre fiecare statie: numele statiei, IP, sistem de operare, module instalate, politica aplicata, informatii despre actualizari etc.
5. Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe statii/servere.
6. Consola va include o sectiune, „Audit”, unde se vor mentiona toate actiunile intreprinse fie de administratori fie de reporteri, cu informatii detaliate: logare, editare, creare, delogare, mutare etc.
7. Posibilitatea creari unui singur pachet de instalare, utilizabil atat pentru sistemele de operare pe 32 de biti cat si pentru cele pe 64 de biti.
8. Posibilitatea creari unui singur pachet de instalare, utilizabil pentru statii (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.
9. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
10. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta statiile/serverele din retea pentru cele care nu sunt integrate domeniu.
11. Permite selectarea clientului care va realiza descoperirea statiilor din retea, altele decat cele integrate in domeniu.

4. Caracteristici si functionalitati principale ale modulului antimalware:

1. *Solutia permite administratorului sa stabileasca actiunea luata de produsul Antimalware la detectarea unei amenintari noi. Astfel administratorul va putea alege intre urmatoarele actiuni:*

a. *Actiune implicită pentru fisiere infectate:*
- *interzice accesul*
- *dezinfecteaza*
- *stergere*
- *muta fisierele in carantina*
- *nicio actiune*

b. *Actiune alternativa pentru fisierele infectate:*
- *interzice accesul*
- *dezinfecteaza*
- *stergere*
- *muta fisierele in carantina*

c. *Actiune implicită pentru fisierele suspecte:*
- *interzice accesul*
- *stergere*
- *muta fisierele in carantina*
- *nicio actiune*

d. *Actiune alternativa pentru fisierele suspecte:*
- *interzice accesul*
- *stergere*

- *muta fisierele in carantina*

2. *Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fisiere mai mari de « x » MB, marimea fisierelor putand fi definita de administratorul solutiei,*
3. *Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.*
4. *Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul caruia sunt rulate aplicatii cu potential periculos protejand sistemul de virusii necunoscuti prin detectarea codurilor periculoase a caror semnatura nu a fost lansata inca.*
5. *Scanarea oricarui suport de stocare a informatiei (CD-uri, harduri externe, unitati partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unitati care au informatii stocate mai mult de « x » MB.*
6. *Scanarea automata a emailurilor la nivelul statiei de lucru pentru POP3/SMTP.*
7. *Configurarea cailor ce urmeaza a fi scanate la cerere.*
8. *Clientii antimalware pentru workstation sa permita definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fisiere, extensii sau procese.*
9. *Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware.*
10. *Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa*
11. *Produsul antimalware poate fi configurat sa foloseasca scanarea in cloud, si partial scanarea locala. Pentru statiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalata in retea.*
12. *Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:*
    - *Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.*
    - *Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.*
    - *Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate.*
    - *Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full)*
    - *Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light)*
13. Pentru o protectie sporita, solutia antimalware trebuie sa aiba 3 tipuri de detectie: bazata pe semnaturi, bazata de comportamentul fisierelor si bazata pe monitorizarea proceselor.
14. Pentru o protectie sporita, solutia antimalware trebuie sa poata scana paginile HTTP.
15. Pentru o mai buna gestionare a antimalware instalat pe statii, produsul va include optiunea de setare a unei parole pentru protectia la dezinstalare.
16. Pentru siguranta utilizatorului, clientul va include un modul de antiphishing.
17. Solutia ofera protectie in timp real pe masinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalata.
18. Pe masinile virtuale parte a unui pool instalarea clientului antimalware se face doar pe masina de tip template, dupa care se recompune pool-ul de masini virtuale.

5. Firewall:

1. *Posibilitatea de a configura reguli de firewall pentru aplicatii sau conectivitate.*
2. *Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.*
3. *Posibilitatea de a defini retele de incredere pentru masina destinatie.*

6. Carantina:

1. *Produsul antimalware sa permita trimiterea automata a fisierelor din carantina catre laboratoarele antimalware ale producatorului.*
2. *Trimiterea continutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.*
3. *Produsul antimalware sa permita stergerea automata a fisierelor carantinate mai vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare.*
4. *Posibilitatea de a restaura un fisier din carantina in locatia lui originala.*
5. *Modulul de carantina va permite rescanarea obiectelor dupa fiecare actualizare de semnaturi.*

7. Protectia datelor:

1. *Produsul permite blocarea datelor confidentiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.*

8. Controlul continutului:

1. Consola va avea integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati:
   a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de masini.
   b. Permite blocarea accesului la Internet pe intervale orare.
   c. Permite blocarea paginilor de internet care contin anumite cuvinte cheie.
   d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator;
   e. Permite blocarea accesului la anumite aplicatii definite de administrator;
   f. Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii prestabilite (ex: online dating, violenta, pornografie etc).

9. Controlul aplicatiilor:

1. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate aplicatiile descoperite in retea, grupate dupa: nume, versiune, descoperit la, gasit pe.
2. Pentru o mai buna inventariere si administrare, solutia va include o sectiune in consola de administrare unde se vor regasi toate procesele negrupate descoperite in retea, grupate dupa: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, gasit pe.
3. Pentru prevenirea infectarii statiilor si serverelor dar si pentru a permite aplicatiilor descoperite in retea sa se poata actualiza, solutia permite definirea unor programe de actualizare (Updater) care vor fi lasate sa actualizeze diferite aplicatii instalate pe statii sau servere.
4. Solutia include optiunea de a permite sau a bloca rularea anumitor aplicatii sau procese definite de administrator (inclusiv subprocese) dupa:
   a. Cale fisier: local, CD-ROM, portabil sau retea
   b. Hash
   c. Certificat

10. Controlul dispozitivelor:

1. *Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.*
2. *Modulul va permite controlul urmatoarelor tipuri de dispozitive:*
   a. Bluetooth Devices
   b. CDROM Devices
   c. Floppy Disk Drives
   d. Security Policies 153
   e. IEEE 1284.4
   f. IEEE 1394
   g. Imaging Devices
   h. Modems
   i. Tape Drives

j. Windows Portable
k. COM/LPT Ports
l. SCSI Raid
m. Printers
n. Network Adapters
o. Wireless Network Adapters
p. Internal and External Storage

3. *Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la masina client.*
4. *Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.*

10. Power User:

1. *Modulul poate fi instalat/dezinstalat in functie de preferinta administratorului.*
2. *Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setarile clientului antimalware dintr-o consola dispobibila local pe masina client.*
3. *Administratorul va putea suprascrie din consola setarile aplicate de utilizatorii Power User.*

11. Actualizare:

4. Posibilitatea efectuarii actualizarii la nivel de statie in mod silentios (fara avertizare).
5. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
6. Actualizarea pentru locatiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.

Solutia antivirus pentru serverele fizice si virtuale va avea acces la baza actualizata de semnaturi a producatorului, pentru o perioada de 3 ani de zile. Solutia se va dimensiona pentru toate serverele utilizate in cadrul spitalelor si cele de la centrul HUB MS.

3.4.3. Securitatea sistemului la nivel central

Se va instala si configura un Certificat SSL/PKI pentru a securiza Serviciile Web. Serverul de Aplicatii al HUB-ului MS va rula un SSL Secured Service.

Se va prevedea cate un certificat pentru fiecare spital si unul pentru HUB-ul central cu reinnoire pe toata durata existentei proiectului (Furnizorul asigurand acest certificat in perioada de implementare, iar Beneficiarul in perioada de sustenabilitate).

3.4.4.Managementul utilizatorilor si accesul la sistem
Accesul se face cu user-name şi parolă alocate fiecărui utilizator în parte.

- În fiecare spital se va realiza un sistem director de management al utilizatorilor și grupurilor de utilizatori, cu aplicare de politici de securitate și de acces diferențiate funcție de rolul din cadrul spitalului și sistemului.

- La nivel central aplicatia va realiza un sistem de management (fara sistem director) al utilizatorilor și grupurilor de utilizatori, cu aplicare de politici de securitate și de acces diferențiate funcție de rolul fiecaruia.

Sistemul permite definirea unei perioade standard de inactivitate a unui user logat, după care face logout automat.

La nivel de spital in afară de parolă şi username, sistemul are 3 (trei) nivele de acces:

- acces total – orice dosar de pacient poate fi vizualizat şi editat;
- acces read-only- datele pacientului pot fi văzute, dar nu pot fi editate;
- no access: un pacient poate cere restricţionarea accesului unui anumit user la datele sale.

Key-userii pot limita accesul anumitor useri la datele unui pacient (pentru cazurile sensibile: persoane publice, somităţi etc.).

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

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

3.4.4. Componenta integrata de mascare, anonimizare si de-identificare a datelor – centru HUB MS

Sistemul propus trebuie să asigure 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.
Cerinţe pentru componenta integrata de mascare, anonimizare si de-identificare a datelor

- Soluția trebuie să fie capabilă să modifice date sensibile cu un conținut alternativ. Soluția trebuie să dispună de capacitatea 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 înțelege modelele de date, în scopul de a menține integritatea referențială într-o bază de date.
- Soluția trebuie să permită o mascare directă a datelor.
- Soluția trebuie să permită deidentificarea (pseudoanonimizare) datelor pacientilor prin ascunderea sau stergerea anunitor subseturi de date, in mod configurabil. Solutia trebuie sa permita reidentificarea totala sau partiala a datelor initiale.
- Soluția trebuie să permită o anonimizare completa a datelor, prin ascunderea sau stergerea metadatelor unui intreg subset de date, fara posibilitatea de a reconstitui datele initiale.
- Soluția trebuie să permită programarea rulării funcțiilor de mascare, deidentificare si anonimizare 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 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.

3.4.5. Solutie pentru monitorizarea centralizata a evenimentelor din retea si raspuns la incidentele de securitate – centru HUB MS

Pentru ca sistemul informatic existent să beneficieze de un nivel cât mai ridicat de vizibilitate, control și securitate, este necesară furnizarea unui sistem dedicat de Management al Evenimentelor și Securității Informațiilor (SIEM), care să asigure într-un mod unificat:

- Funcționalități de tip SIM (Managementul Securității Informației) prin stocarea log-urilor pentru perioade îndelungate de timp (atât online cât și offline prin arhivare), posibilitatea de analizare a acestora și generarea de rapoarte;
- Funcționalități de tip SEM (Managementul Evenimentelor de Securitate) prin monitorizarea constantă, corelarea evenimentelor și alertarea automată în cazul producerii unor incidente de securitate;

Având în vedere arhitectura rețelei dedicate creată în cadrul proiectului, soluția SIEM trebuie să fie una de tip software, care să permită utilizarea optimă a infrastructurii hardware după cum urmează:
Să poată fi instalată peste platforma de virtualizare Vmware sau Hyper-V;

- Să poată utiliza (pentru stocarea log-urilor/evenimentelor/configurațiilor): stocare locală, infrastructura elasticsearch, infrastructura NFS ce va fi configurată în locația centrală în cadrul proiectului;
- Să permită colectarea, parsarea și arhivarea log-urilor și transmiterea acestora în mod securizat, peste conexiunile VPN/WAN/Internet. Pentru preîntâmpinarea întreruperilor temporare ale comunicațiilor dintre locația centrală și unitățile spitalicești din teritoriu cuprinse în proiect, soluția trebuie să asigure mecanisme locale de colectare și stocare temporară a log-urilor și retransmiterea automată a acestora către sediul central (în momentul în care este restabilită comunicația);

Interfața de administrare/operare trebuie să fie de tip web-based și să permită:
- rularea de slideshow-uri pentru vizualizarea rapoartelor ce necesită monitorizare mai atentă/frecventă;
- vizualizarea topologiei logice a rețelei (cu posibilitatea de analizare detaliată a incidentelor la nivelul fiecărui echipament);
- vizualizarea și filtrarea incidentelor în funcție de atributele evenimentului, severitate, categorie (securitate/performanță/disponibilitate) sau interval orar;

Colectarea logurilor:
- Posibilitatea de a adăuga în sistem noi module/noduri care să asigure funcționalitățile de analiză/căutare, fără a cauza întreruperi la nivelul soluției SIEM;
- Colectarea evenimentelor de securitate aferente monitorizării integrității fișierelor, modificărilor de regiștrii sau instalării de noi aplicații software;
- Posibilitatea de a modifica/edita parsarea log-urilor fără întreruperea logării sau a funcționării sistemului;
- Posibilitatea de a crea/importa/exporta noi parsere utilizând interfața GUI/API;

Soluția SIEM trebuie să asigure un nivel cât mai ridicat de securitate, disponibilitate și performanță prin furnizarea următoarelor funcționalități de bază:
- Alertare automată în situația în care este afectată integritatea datelor prin modificări (realizate de către persoane neautorizate sau aplicații malware/ransomware) de fișiere/directoare, regiștrii windows, fișiere de sistem etc.
- Alertare automată în situația în care (datorită unor defecțiuni, erori umane sau atacuri cibernetice) anumite conexiuni, sisteme sau aplicații devin inaccesibile/nefuncționale;
- Alertare automată în situația în care se produc evenimente atipice/neuzuale (neconforme cu
- valorile statistice de referință);
- Posibilitatea de investigare cât mai rapidă a unor eventuale tentative de încălcare a securității datelor, atacuri cibernetice sau probleme de performanță/disponibilitate prin analizarea a log-urilor și evenimentelor colectate pentru anumite intervale specifice de timp, predefinite/personalizabile;
- Compatibilitate cu diverse tipuri de log-uri aferente diferitelor tipuri de echipamente de rețea/IT, cu posibilitatea de a defini noi parsere in timp real, fara intreruperea funcționării (restartarea) soluției SIEM;
- Ușurința în operare și administrare prin automatizarea procesului de descoperire (și adaugare în baza de date locală) a echipamentelor de rețea (routere, firewall-uri, switch-uri) sau echipamente IT (servere, stații de lucru, storage-uri) prin interogari recurente standard (SNMP/SSH/HTTPS/etc.) după definirea/specificarea credențialelor și a claselor/subclaselor de adresare IP;
- Key-userii trebuie să poată rula rapoarte predefinite (de analiză și raportare a evenimentelor), cu posibilitatea de modificare și personalizare a acestora în funcție de nevoi;
- Scalabilitate:
- Soluția trebuie să poată fi extinsă prin adăugarea de mașini virtuale în cadrul infrastructurii virtuale locale;
- Soluția furnizată trebuie să permită adăugarea de noi module/componente care să extindă performanțele sistemului în ceea ce privește funcționalitățile de căutare, interogare, analiză evenimente, generare rapoarte, rulare automata de reguli de alertare/notificare

- Soluția trebuie să permită colectarea, parsarea, normalizarea, indexarea și stocarea log-urilor de securitate la viteze cât mai mari;

Funcționalități de analiză în timp real:
- Update-area în timp real a informațiilor ce țin de starea operațională a echipamentelor de rețea/IT: modificări de configurații, instalări software/patch-uri, status servicii (active/inactive);
- Colectarea fișierelor de configurare a echipamentelor de rețea (switch-uri/routere) urmată de versionarea și stocarea locală a acestora;
- Analizarea în timp real a informațiilor legate de sistemele și aplicațiile IT, cu posibilitatea de a filtra aceste informații pe baza unor atribute (predefinite la nivelul aplicației SIEM sau definite de către key-useri) pentru a putea tria/identifica cât mai rapid problemele de securitate;
- Detectarea modificărilor neautorizate ale configurațiilor aplicațiilor și echipamentelor de rețea;
- Monitorizarea performanțelor:
- La nivel de sistem (CPU/RAM/Storage/network trafic) utilizând SNMP, WMI, PowerShell;
- La nivel de aplicație utilizând JMX, WMI, PowerShell;
- Pentru platforma de virtualizare utilizată – VMWare;
- Microsoft Active Directory și Exchange utilizând WMI și Powershell;
- La nivelul traficului de rețea: Cisco AVC, Netflow, Sflow;
- Posibilitatea de a genera rapoarte predefinte referitoare la performanța, disponibilitatea,
- conformitatea și securitatea infrastructurii IT (echipamente de rețea, servere, stații de lucru, aplicații, servicii etc.);
- Analiza disponibilității:
- La nivel de sistem:
    - prin interogari Ping, SNMP, WMI;
    - monitorizarea modificărilor la nivelul serviciilor, proceselor și interfețelor critice;
    - monitorizarea modificărilor status-ului protocoalelor de rutare dinamice (BGP/OSPF/EIGRP);
    - monitorizarea stării porturilor de stocare (stare activă/inactivă);
- La nivelul unui serviciu: prin interogări Ping, HTTP, HTTPS, DNS, LDAP, SSH, SMTP, IMAP, POP, FTP, JDBC, ICMP, trace route;

Managementul incidentelor:
- Posibilitatea de configurare a regulilor/politicilor ce definesc un incident;
- Posibilitatea de a rula în mod automat un script în cazul producerii unui anumit incident;
- Sistem integrat de ticketing, dar și posibilitatea de a integra (prin API-uri) sisteme externe de ticketing;
- Raportarea incidentelor trebuie să poată fi structurată astfel încât să evidențieze în mod prioritar aplicațiile și serviciile critice;
- Notificări în timp real în cazul identificării unor evenimente complexe;
- Integrarea cu sisteme externe de tip Threat Intelligence:
- Soluția SIEM oferită trebuie să asigure integrarea (de ex. prin API-uri) cu sisteme externe ce pun la dispozitie informații/liste/baze de date despre domenii malware, IP-uri, URL-uri sau noduri Tor (de ex. ThreatStream, CyberArk, SANS, Zeus, etc.);
- Soluția ofertată trebuie să poată gestiona volume foarte mari de update-uri, printr-un download incremental și update-area infrastructurii locale SIEM pentru a verifica în timp real maparea informațiilor furnizate de sistemele externe de Threat Intelligence cu datele aferente traficului local;

Analiza evenimentelor:
- Posibilitatea de a căuta/sorta evenimente în funcție de cuvinte cheie sau atribute asociate evenimentelor;
- Cautarea/identificarea evenimentelor aferente unor perioade de timp prin filtrarea rezultatelor utilizând atribute (ex. utilizator, IP sursa/destinatie, numele sau tipul de malware, nume sau tipul de atac, etc.), operatori logici (egal, diferit, mai mare, mai mic, mai mare sau egal, mai mic sau egal,

contine, nu contine, RegEXP, non RegEXP) si valori ce sunt mapate (prin intermediul operatorilor logici) cu atributele respective;
- Posibilitatea filtrării și analizării evenimentelor la nivelul întregii organizații sau la nivelul obiectelor existente în baza de date: dispozitive de rețea/IT/servicii/aplicații/utilizatori;
- Posibilitatea de a defini rapoarte și de a programa transmiterea acestora prin email pentru a fi analizate ulterior;

Suport API (Application Programming Interface);
- Conectare prin API cu surse externe de the threat intelligence;
- Conectare prin API cu sisteme externe de helpdesk/ticketing;
- Conectare prin API cu baze de date externe pentru importul/exportul obiectelor ce definesc dispozitive hardware, servicii, componente software etc.;
- API care să permită: creare credențiale, inițierea procedurii automate de scanare și descoperire a obiectelor ce definesc infrastructura IT, modificarea evenimentelor monitorizate;

Simplitate și flexibilitate în administrare:
- Administrare facilă utilizând o interfață web;
- Posibilitatea de a defini roluri de administrare prin restricționarea accesului la anumite componente din cadrul interfeței web;
- Comunicația între componentele centrale (analiză/raportare/management) și cele remote (colectare log-uri la nivel de sucursală) trebuie să se realizeze în mod securizat (criptat) prin intermediul unor protocoale ce funcționează optim peste infrastructuri WAN/Internet (ex. HTTPS);
- Posibilitatea de update-are cu noi parsere, reguli sau rapoarte predefinite puse la dispoziție de către producator;
- Posibilitatea de arhivare a log-urilor și de stocare a acestora offline. Soluția trebuie să permită definirea de politici care să stabilească pentru câte zile sunt stocate evenimentele online (înainte de a fi arhivate și stocate offline). Datele arhivate trebuie să fie semnate criptografic (ex. SHA256) și să asigure mecanisme de non-repudiere și verificare a integrității acestora;
- Soluția trebuie să permită generarea de rapoarte în format PDF referitoare la integritatea arhivelor (evenimentelor) stocate offline.
- Autentificarea utilizatorilor trebuie să se poată realiza local sau extern prin Microsoft AD, OpenLDAP, Cloud SSO/SAML ș.a.;
- Solutia trebuie sa includa functionalitati de rulare a unui serviciu de tip IOC (Indicator of Compromise) prin intermediul caruia sa poata fi realizata o analiza retrospectiva a log-urilor, in vederea alertarii si raportarii automate in situatiile in care exista indicii conform carora anumite dispozitive IP ar fi putut fi compromise ca urmare a accesarii unor domenii, IP-uri sau URL-uri cu reputatie proasta.

Solutia trebuie sa aiba suport pentru extinderi ulterioare posibile pentru monitorizarea platformelor Windows, cu urmatoarele functionalitati:
- Monitorizarea platformelor Windows prin utilizarea protocoalelor SSH, WMI, SNMP, Syslog ș.a. pentru obținerea informațiilor de sistem, aplicație, securitate și performanță;
- Furnizarea unor modalități (ex. prin instalarea de agenți Windows) care să asigure funcționalități avansate precum:
    - Verificarea integrității fișierelor, cu raportare automată în cazul în care integritatea acestora este alterată: rapoartele/alertele trebuie să conțină tipul operațiunii (ex. ștergere, redenumire, creare, modificare) precum și informații relevante despre incident: nume utilizator, data, ora, adresa IP a stației de lucru etc.;
    - Colectarea log-urilor aferente serviciilor DNS, DHCP, DFS și IIS;
    - Parsarea locală și normalizarea informațiilor legate de timp;
    - Detectarea softurilor/aplicațiilor instalate;
    - Monitorizarea și raportarea în cazul modificării regiștrilor;
    - Customer Log File Monitoring;
    - WMI Command Output Monitoring;

- PowerShell Command Output Monitoring;

Performante:
- Solutia ofertata trebuie sa asigure gestionarea unui numar total de cel putin 10 EPS-uri (Evenimente pe Secunda) pentru firewall, servere fizice, echipamentele de stocare, masinile de aplicatii si serverele de fisiere
- Solutia ofertata trebuie sa asigure gestionarea unui numar total de cel putin 2 EPS-uri (Evenimente pe Secunda) pentru fiecare statie, access-point, echipament de retea
- colectarea, stocarea si analiza log-urilor pentru cel putin toate dispozitivele IT&C:
  - 150 device-uri de retea: firewall, switch-uri
  - 750 end-points

Licentele ofertate trebuie sa fie perpetue. Se va asigura suport de la producator pentru 3 ani de zile in regim 24x7.

3.5. Cerințele non-funcționale ale sistemului informatic

3.5.1. Cerințele de performanță specifice pentru sistemul informatic

- Timpul mediu de răspuns al serverului nu va depăși 3 secunde la încărcarea unei pagini web.
- Sistemul informatic de tip web HUB MS va permite activitatea a cel puțin 25 utilizatori interni concurenti
- Sistemul informatic de tip ATI si SO va permite activitatea simultana in rețeaua de spitale a cel puțin 550 utilizatori concurentiali
- Anterior livrării soluției informatice vor fi efectuate totalitatea testelor de performanță a sistemului
- Testarea performanței va include minim doua componente: testarea încărcarii sistemului (load testing) și testarea comportamentului sistemului la solicitări mari (stress testing).

3.5.2. Cerințe privind documentația sistemului informatic

Sistemul informatic va fi acompaniat de un set complet de documentație a sistemului informatic care cuprinde următoarele:
- Proiectul tehnic de detaliu al sistemului informatic implementat (care va include capitole referitoare la analiza, proiectare, dezvoltare, testare)
- Manualul utilizatorului în limba Română
- Manualul key-userului în limba Română.
- Ghidul de instalare si configurare a sistemului (care să includă cel puțin instrucțiuni privind instalarea aplicației, cerințe hardware și software, descrierea și configurarea platformei, configurarea aplicației, proceduri de backup).
- Documentația pentru integrare cu alte sisteme informatice.

3.6. Etapele de implementare a sistemului informatic

Activitățile de implementare sunt activitățile necesare pentru a face sistemul informatic gata de folosire de către utilizatori.
In cadrul proiectului se vor avea in vedere realizarea de catre furnizor a serviciilor de implementare: management de proiect, analiza, proiectare, configurare si customizare aplicatii, dezvoltare, integrare, testare, instruire, trecere in productie.

3.6.1. Management de Proiect

In relația cu Beneficiarul, prin intermediul Managerului de Proiect si a echipei de management si implementare din partea acestuia, Furnizorul va asigura si raporta

- Planificarea activitatilor astfel incat sa se incadreze in toate etapele planului de implementare
- Monitorizarea si raportarea implementării proiectului
- Elaborarea planului revizuit de activități ale Furnizorului și urmărirea respectării termenelor proiectului
- Elaborarea rapoartelor de progres lunare ce vor fi înaintate spre aprobare Beneficiarului

In relația cu Furnizorul si cu ceilalti parteneri si stakeholderi din proiect, activitatea se va desfasura in coordonarea Managerului de Proiect si a echipei de management si implementare din partea Beneficiarului asigurand si raportand
- Supravegherea îndepliniriia de către furnizor a obligațiilor asumate în conformitate cu contractul semnat
- Coordonarea activităților de informare și instruire aferente fiecărei etape a proiectului
- Asigurarea accesului tuturor membrilor echipelor de lucru la toată documentația/corespondentaaferenta fiecarui nivel de decizie/implementare
- Elaborarea planului revizuit de activități și urmărirea respectării termenelor proiectului
- Elaborarea rapoartelor de progres lunare ce vor fi înaintate spre aprobare catre finantator

3.6.2. Servicii de analiza si proiectare

Rolul principal al fazei de analiză este de a înțelege corect nevoile utilizatorilor înainte de proiectarea și implementarea unui sistem care să le îndeplinească.
În vederea implementării sistemului, Furnizorul va trebui să execute activități de analiză care să asigure premisele unei implementări eficiente.
Beneficiarul va acorda tot sprijinul necesar pentru înțelegerea cât mai bună și completă a contextului în care va fi implementat sistemul.
Serviciile de analiză vor acoperi cel puțin următoarele aspecte:
- Analiza contextului existent;
- Înțelegerea structurii organizatorice a Beneficiarului;
- Definirea cerințelor informaționale pentru noul sistem. Se va contura astfel, imaginea viitorului sistem informațional prin stabilirea proceselor operaționale.
- Stabilirea actorilor de business care vor interacționa în viitorul sistem;
- Identificarea utilizatorilor, a nivelurilor si drepturilor de acces, a modului de securizare a accesului la diversele module/componente ale sistemului;
- Se vor analiza sistemele operationale existente (inclusiv structurile de date, aspecte legate de consistenta si coerenta datelor) pentru identificarea posibilitatilor si a modului in care se va face preluarea datelor din solutiile existente.

Rolul principal al fazei de proiectare este de a descrie sistemul care urmează a fi implementat.
În vederea implementării sistemului, Furnizorul va trebui să execute activități de proiectare care să asigure premisele unei implementări eficiente.
Proiectarea sistemului dorit, care va conține detalierea la nivel tehnic a cerințelor și specificațiilor rezultate din activitatea de analiză pentru toate nivelurile și componentele sistemului care va fi realizat:
- Arhitectura de sistem – va prezenta cel puțin următoarele niveluri: hardware, comunicații, componente software instalate (sisteme de operare, produse COTS), arhitectura logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate și caracteristicile funcționale și non-funcționale ale acestora;
- Modelul de securitate – la nivel logic (organizarea pe roluri, grupuri, drepturi, poziția în structura organizatorică etc.) și la nivel fizic (servere, comunicații, aplicații etc.);
- Integrările la nivel de componentă software – pentru fiecare interacțiune se va specifica sistemul sursă/destinație, modalitatea de implementare, canal de comunicare, setul și structura de date transferate, reguli specifice de validare etc;

În urma activităților de analiză și proiectare, pentru a se obține un sistem final operațional se vor desfășura activități de configurare, testare și implementare (deployment).
Pe perioada desfășurării activității de analiză și proiectare și distinct de această activitate, se vor derula în paralel activitati legate de achizitionarea si livrarea echipamentelor hardware si a licentelor necesare pentru dezvoltarea si implementarea solutiei informatice.

Pentru componentele din fiecare spital:
- Identificarea amplasamentului fiecarei componente a sistemului;
- Optimizarea traseelor de cabluri;
- Identificarea echipamentelor medicale proprii locațiilor (ATI + SO);
- Identificarea posibilitatii si a modalitatii de comunicare cu sistemul de comunicare a echipamentelor medicale existent in fiecare locatie;
- Identificarea posibilitatii si a modalitatii de comunicare cu HIS (Hospital Information Sistem) existent in fiecare locatie;

Pentru HUB-MS - Dashboard:
- Analiza proceselor existente
- Remodelarea proceselor de business viitoare, definirea actorilor (modelare BPMN)
- Modelarea conceptuala, logica (modelare UML) si fizica (modelare XSD) a seturilor de date, cel putin a celor expuse prin API/web-service/HL7 (intrari, iesiri)
- Elaborarea specificatiilor de integrare pentru spitale (altele decat cele partenere, pentru integrări viitoare, în afara scopului acestui proiect)
- Elaborarea specificatiilor de integrare pentru colectare date de pozitionare (GIS)

Pentru HUB-MS - BI:
- Analiza rapoartelor și a indicatorilor de performanță
- Modelarea conceptuala a rapoartelor (parametri, date de raportare, tipuri diagrame, grupare pe dashboarduri, etc)

3.6.3. Servicii de configurare si customizare

In cadrul fiecarui spital se va configura aplicatia in functie de numarul de paturi, tipuri de echipamente, raportul de paturi pe sectii, procedurile medicale folosite in cadrul spitalului, medicatie, tipurile de medicatii utilizate in spital si protocoalele specifice, rapoartele uzitate.

3.6.4. Servicii de integrare

In cadrul implementarii aplicația ATI se vor integra:
- Componenta software aplicativ pentru sectiile ATI cu paturi si Sali de Operatii cu sistemele HIS din fiecare spital prin intermediul mesageriei HL7
- Componenta software aplicativ pentru sectiile ATI cu paturi si Sali de Operatii cu echipamente medicale specifice ATI. Comunicarea se va efectua prin intermediul unui gateway
- Componenta software aplicativ pentru sectiile ATI cu paturi si Sali de Operatii cu Componenta Dashboard Disponibilitate paturi ATI prin intermediul mesageriei HL7

3.6.5. Servicii de dezvoltare

Se vor derula activitati de parametrizare, configurare, customizare si dezvoltare a componentelor solutiei informatice.
La finalul fazei de dezvoltare va rezulta o solutie informatica completa, in conformitate cu cerintele mentionate in Caietul de Sarcini, si detaliate in cadrul fazei de analiza.

Se vor dezvolta urmatoarele:

- Dezvoltare rapoarte statistice si indicatori de sanatate publica
- Dezvoltare procese ETL (non-SOA FHIR implementations) pentru integrare HIS/sistem ATI cu solutia BI din HUB MS (sau integrare prin RESTful sau SOAP Web Services/Interfaces, SOA in FHIR environment)
- Dezvoltare Componenta BI Self-Service Dashboard Disponibilitate paturi ATI (aplicatie BI)

Servicii de testare

Furnizorul va pune la dispoziția beneficiarului pe toată durata contractului un mediul de dezvoltare/integrare continuă și un mediu de test/accepnață. Cele două medii vor facilita/automatiza procesele de dezvoltare, testare, acceptanță și mentenanță corectivă pentru componentele de software aplicativ de la nivelul centru HUB MS. Mediul de testare/acceptanță, va respecta arhitectura software a mediului de producție si va fi dimensionat corespunzător in funcție de soluția propusa.

În fiecare locație de implementare se vor testa configurarile, customizările, dezvoltarile si intregrarile realizate, în baza unor scenarii de test elaborate de catre furnizor.

Supunerea aplicaţiei la operaţiuni critice de test, verificarea tuturor funcţionalităţilor, testarea meniurilor şi altor elemente de interfaţă, testarea securităţii pe rolurile definite in aplicatii.

3.6.6. Testarea și asigurarea calității

Beneficiarul (cu asistența Furnizorului) va rula toate scenariile pentru testele de acceptanță ale întregului sistem sau componentă livrată. Testele de acceptanță se vor derula în conformitate cu Planul de Teste realizat de Prestator și agreat de Beneficiar.

Planul de testare pentru acceptanță va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerințelor din prezentul proiect tehnic. Astfel, se va avea în vedere faptul că sistemul funcționează corect din punct de vedere al respectării cerințelor.

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. 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).

3.6.7. Servicii de instruire utilizatori

Se vor realiza sesiuni de instruire cu utilizatorii sistemului, key-userii de aplicație ATI+SO, administratorii de sistem/rețea din cadrul celor 18 spitale de implementare, precum și instruirea utilizatorilor și key-userilor componentelor software (componente web, componente aplicative si componente solutia BI) și hardware din locația centrală.
Toți utilizatorii și key-userii vor fi instruiți de furnizor, la sediul fiecărei unități medicale, în utilizarea sistemului informatic integrat, în conformitate cu atribuțiile pe care le au prin fișa postului. Furnizorul va asigura, prin instruirea utilizatorilor, realizarea cel puțin a următoarelor obiective:

- cunoașterea sistemului integrat în ansamblul său;
- învățarea modului de operare în sistem;
- învățarea modului de rezolvare a problemelor curente folosind sistemul informatic;
- înțelegerea implicațiilor sistemului și a avantajelor acestuia asupra modului de rezolvare a problemelor curente;
- cunoașterea modului de obținere a rapoartelor extrase din solutia de BI

Sesiunile de instruire vor fi realizate de către furnizorul soluției informatice, în conformitate cu prevederile contractuale.
De asemenea, furnizorul soluției informatice va elabora și pune la dispoziția beneficiarului manuale de utilizare și suport de curs în limba română pentru utilizarea funcționalităților sistemului.
Instruirea se va desfășura în limba română și va fi urmată de verificarea cunoștințelor și a abilitaților dobândite de către utilizatorii finali (evaluare).
Cursurile pentru utilizarea aplicatiei ATI si pentru administrarea echipamentelor din fiecare locatie se vor desfășura la sediul fiecărui Spital.
La terminarea instruirii, cursanții vor primi de la furnizor certificate de instruire individuale. Va exista câte un model de astfel de certificate de instruire pentru principalele categorii de utilizatori: utilizatori și key-useri ai sistemului informatic.

3.6.8. Servicii de trecere in productie

Reprezintă etapa prin care se finalizează fiecare implementare din cele 18 spitale din proiect, prin darea in folosinta a sistemului, astfel încât acesta să poată fi folosit efectiv pentru activitățile curente. Punerea în funcțiune în mediul real a aplicației, încărcarea cu date reale și informații necesare pornirii sistemului.

3.6.9. Graficul de implementare

Avand in vedere ca fiecare ofertant va propune propria metodologie de implementare, in cadrul etapei de ofertare acestia vor prezenta graficul Gantt propriu de implementare, pe etape, care va trebui sa respecte graficul de implementare al proiectului ce va fi comunicat in documentatia de atribuire.

Conform Gantt-ului de proiect, Activitatea „Livrari dotari hardware si software, licente aplicatie si servicii analiza, proiectare, configurare, testare, instruire, trecere in productie" este prevazuta a se derula intre lunile 11-35 de proiect.

Diagrama Gantt aferentă calendarului de activități previzionate a se realiza în vederea implementării proiectului „SIEC pentru ATI"

Activitate	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13	L14	L15	L16	L17	L18	L19	L20	L21	L22	L23	L24	L25	L26	L27	L28	L29	L30	L31	L32	L33	L34	L35	L36
Management de proiect																																				
Achizitie Management de proiect extern																																				
Derulare servicii PM																																				
Informare si publicitate																																				
Achizitie Servicii de informare si publicitate																																				
Derulare servicii de informare si publicitate																																				
Implementare SIEC																																				
Achizitie Sistem integrat																																				
Livrari dotari hardware si software, licente aplicatie si servicii analiza, proiectare, configurare, testare, instruire, trecere in productie																																				
Audit proiect																																				
Achizitie audit																																				
Derulare servicii audit																																				

4. RESURSE

4.1.PERSONAL ŞI INSTRUIRE

Personalul din unitățile spitalicești de implementare a proiectului ce vor folosi sistemul, vor fi instruite în cadrul unităților unde își desfășoară activitatea. Instruirea se va realiza în ture pentru a acomoda timpii diferiți de disponibilitate a personalului medical.

În cadrul fiecărei instituții medicale, vor fi instruite persoane din cadrul secțiilor ATI și bloc operator pentru a acumula cunoștințele necesare pentru utilizarea sistemului. Instruirea se va finaliza cu testarea cunoștințelor acumulate în cadrul sesiunilor de instruire și este de preferat ca 100% din numărul de cursanți să obțină certificarea de utilizare.

Suplimentar personalului care va utiliza aplicația ATI și Săli Operație (SO) vor fi instruiți în fiecare spital din proiect minim 2 administratori de aplicație (key-useri), care în urma testării vor obține certificare de administrare a aplicației.

Din cadrul fiecărui spital de implementare, se vor instrui minim 1 key-user de retea/sistem cu privire la administrarea infrastructurii hardware, de comunicații și de securitate din locație, minim 2 zile.

Pentru aplicațiile la nivel central, se vor instrui minim 2 key-useri, timp de minim 3 zile pentru administrarea aplicațiilor centrale, a infrastructurii hardware, de comunicații și de securitate.

În cadrul sesiunilor de instruire se vor folosi suporturi de curs și exemplificări pentru o însușire rapidă din partea cursanților a noțiunilor/informațiilor prezentate.

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.

De asemenea, se va asigura un modul de curs care să vizeze conștientizarea utilizatorilor privind securitatea sistemului, vizând:
- Prezentare principalele tipuri de atacuri cibernetice
- Elemente referitoare la motivațiile atacatorilor
- Tactici de inginerie socială
- Cum recunoaștem un incident de securitate?
- Exemple de incidentele care ar trebui raportate
- Aspecte juridice privind protecția și securitatea sistemelor informaționale
- Măsuri administrative pe linia securității informatice

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 vor primi de la furnizor certificate de instruire individuale. Certificarea se va face diferenţiat pentru cele două categorii.

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

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.

Prestatorul va asigura toate resursele necesare desfășurarii serviciilor de instruire, va elabora şi susţine cursurile și va tipări materiale de curs pentru toţi participanţii.
Toate cursurile în format electronic – însoțite de documente suport – vor fi publicate în soluția de knowledge management (KM) inclusiv pentru Operatorii de date.

De asemenea, se va asigura un modul de curs de securitate, vizând următoarele:
- Politici, standarde, norme și proceduri de securitate
- Prioritizarea resurselor pentru îmbunătățirea securității
- Securitatea aplicațiilor
- Securitatea infrastructurii
- Securitatea autentificării și a gestionării sesiunilor
- Etapele unui plan de răspuns la incidente de securitate
- Identificarea și izolarea incidentelor de securitate

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, LMCSI, document).

Ghidul de operare va cuprinde cel puţin:
- procedurile de administrare şi operare a sistemului: administrarea utilizatorilor, salvarea şi restaurarea datelor, optimizarea timpului de răspuns şi a perioadelor de maximă încărcare a cererilor de la utilizatori
- opţiunile şi procedurile de configurare a sistemului propus
- descrierea completă a arhitecturii cuprinzând:
  - componentele hardware, caracteristicile şi configuraţia principala a acestora
  - componentele software, versiunile, configuraţiile şi maparea componentelor software pe componente hardware
  - configurarea securităţii şi descrierea arhitecturii de securitate a soluţiei

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

4.2. RESURSE MATERIALE

Structura proiectului este:

Nr	Spitale	Nr.Paturi ATI	Nr.Paturi Bloc Operator
0	**C.O.S.U. – Centrul Operaţional de Situaţii de Urgenţă**		
1	Spitalul de Urgenta "Bagdasar Arseni" **Bucureşti**	44	16
2	Spitalul de Urgenta "Sf. Ioan" **Bucureşti**	26	11
3	Spitalul de Urgenta "Sf. Pantelimon" **Bucureşti**	25	14
4	Spitalul Clinic de Urgenta **Bucureşti**	68	28
5	Spitalul Universitar de Urgenta **Bucureşti**	52	30
6	Spitalul de Chirurgie Plastică Reparatorie şi Arsuri **Bucureşti**	5	4
7	Spitalul de Urgente Pediatrice "M.S. Curie" **Bucureşti**	24	11
8	Spitalul de Urgenta pentru Copii "G. Alecsandrescu" **Bucureşti**	28	12
9	Institutul Inimii de Urgenţă pentru Boli Cardiovasculare "Nicolae Stăncioiu" **Cluj-Napoca**	18	5
10	Institutul Oncologic "Prof. Dr. I. Chiricuţa" **Cluj-Napoca**	20	10
11	Institutul Regional de Hepatologie si Gastroenterologie " O. Fodor" **Cluj-Napoca**	30	7
12	Spitalul Clinic Judeţean de Urgenta **Cluj-Napoca**	82	29
13	Institutul Regional de Oncologie **Iaşi**	28	10
14	Spitalul Judeţean de Urgenta "Sf. Spiridon" **Iaşi**	55	25
15	Institutul de Urgenţă pentru Boli Cardiovasculare şi Transplant **Târgu Mureş**	23	5
16	Spitalul Judeţean de Urgentă **Târgu Mureş**	51	21
17	Institutul de Boli Cardiovasculare **Timişoara**	15	2
18	Spitalul Clinic Judeţean de Urgenta **Timişoara**	55	35
	Total Paturi	**649**	**275**
	Total Paturi ATI + SO POSTURI	**924**	

Pentru asigurarea compatibilității maxime între tehnologiile folosite în cadrul implementării proiectului, dotările TIC hardware și software vor fi achiziționate ca un tot unitar în cadrul unei singure achiziții.

Dotările vor fi achiziționate de către Beneficiarul proiectului/Autoritatea Contractantă – Ministerul Sănătății. Echipamentele TIC și licențele software aferente, care vor deveni proprietatea Ministerului Sănătății, vor fi date spre folosința unităților spitalicești din teritoriu în baza unui borderou, Ministerul Sănătății rezervându-și dreptul de a încheia contracte de comodat cu fiecare spital participant în proiect.

Echipamentele TIC si licentele ce vor fi alocate pentru fiecare instituție în parte sunt:

Nr.	Locaţie	Echipamente hardware si licente software	Cantitate
0	HUB MS	Platforma interconectare Server backup	1 bucata 1 bucata

		Firewall	2 bucati
		Switch agregare model 1	2 bucati
		UPS	2 bucati
		Rack	1 bucata
		Aer conditionat	2 bucati
		Echipament monitorizare spitale centrul HUB MS	5 bucati
		Licenta platforma virtualizare	1 bucata
		Pachet licente backup	1 bucata
		Pachet licente solutie management centralizat echipamente comunicatii	1 bucata
		Pachet licente solutie pentru monitorizarea centralizata a evenimentelor din retea si raspuns la incidentele de securitate	1 bucata
		Pachet licente solutie de gestiune Data warehouse	1 bucata
		Pachet licente solutie de raportare	1 bucata
		Pachet licente solutie de securizare de tip antivirus pentru servere fizice si virtuale	1 bucata
		Modulul de transfer de date între aplicaţii	1 bucata
		Aplicaţie centrală Dashboard HUB MS	1 bucata
		Aplicaţie raportare pentru Ministerul Sănătăţii	1 bucata
1	Spitalul de Urgenta “Bagdasar Arseni” **Bucureşti**	Servere pentru BD	2 bucati
		Servere de virtualizare	3 bucati
		Storage	1 bucata
		Server backup	1 bucata
		Firewall	2 bucati
		Switch agregare model 1	Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO
		Switch model 2	2 bucati
		UPS	2 bucati
		Rack	1 bucata
		Aer conditionat	2 bucati
		PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată	Conform nr paturi din centralizatorul de mai sus
		Data Terminal Server	Conform nr paturi
		Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă	2 bucati
		Acces point	Conform centralizatorului de mai sus
		Licente software pentru baze de date relationale	
		Licenta platforma virtualizare	1 bucata
		Pachet licente solutie director	1 bucata
		Licenta aplicatie ATI + Sala operatie	1 bucata

			Conform nr paturi din centralizatorul de mai sus
2	Spitalul de Urgenta "Sf. Ioan" **București**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
3	Spitalul de Urgenta "Sf. Pantelimon" **București**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati

		Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
4	Spitalul Clinic de Urgenta **Bucureşti**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
5	Spitalul Universitar de Urgenta **Bucureşti**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus

		operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
6	Spitalul de Chirurgie Plastică Reparatorie şi Arsuri **Bucureşti**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
7	Spitalul de Urgente Pediatrice “M.S. Curie” **Bucureşti**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata

		Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
8	Spitalul de Urgenta pentru Copii "G. Alecsandrescu" **Bucureşti**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
9	Institutul Inimii de Urgenţă pentru Boli Cardiovasculare "Nicolae Stăncioiu" **Cluj-Napoca**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei

		Switch model 2	spitalului si numarul de posturi ATI+SO
		UPS	2 bucati
		Rack	2 bucati
		Aer conditionat	1 bucata
		PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată	2 bucati Conform nr paturi din centralizatorul de mai sus
		Data Terminal Server	
		Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă	Conform nr paturi
		Acces point	2 bucati
		Licente software pentru baze de date relationale	Conform centralizatorului de mai sus
		Licenta platforma virtualizare	
		Pachet licente solutie director	1 bucata
			1 bucata
		Licenta aplicatie ATI + Sala operatie	1 bucata
			Conform nr paturi din centralizatorul de mai sus
10	Institutul Oncologic "Prof. Dr. I. Chiricuţa" **Cluj-Napoca**	Servere pentru BD	2 bucati
		Servere de virtualizare	3 bucati
		Storage	1 bucata
		Server backup	1 bucata
		Firewall	2 bucati
		Switch agregare model 1	Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO
		Switch model 2	2 bucati
		UPS	2 bucati
		Rack	1 bucata
		Aer conditionat	2 bucati
		PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată	Conform nr paturi din centralizatorul de mai sus
		Data Terminal Server	Conform nr paturi
		Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă	2 bucati
		Acces point	
		Licente software pentru baze de date relationale	Conform centralizatorului de mai sus
		Licenta platforma virtualizare	1 bucata
		Pachet licente solutie director	
			1 bucata
		Licenta aplicatie ATI + Sala operatie	1 bucata
			Conform nr paturi din centralizatorul de mai sus
11	Institutul Regional de Hepatologie si Gastroenterologie " O. Fodor" **Cluj-Napoca**	Servere pentru BD	2 bucati
		Servere de virtualizare	3 bucati
		Storage	1 bucata
		Server backup	1 bucata

		Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
12	Spitalul Clinic Judeţean de Urgenta **Cluj-Napoca**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus

13	Institutul Regional de Oncologie **Iaşi**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
14	Spitalul Judeţean de Urgenta “Sf. Spiridon” **Iaşi**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata

		Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
15	Institutul de Urgenţă pentru Boli Cardiovasculare şi Transplant **Târgu Mureş**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus
16	Spitalul Judeţean de Urgentă **Târgu Mureş**	Servere pentru BD Servere de virtualizare Storage Server backup Firewall Switch agregare model 1 Switch model 2 UPS Rack Aer conditionat PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point	2 bucati 3 bucati 1 bucata 1 bucata 2 bucati Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO 2 bucati 2 bucati 1 bucata 2 bucati Conform nr paturi din centralizatorul de mai sus Conform nr paturi 2 bucati

		Licente software pentru baze de date relationale	Conform centralizatorului de mai sus
		Licenta platforma virtualizare	1 bucata
		Pachet licente solutie director	1 bucata
		Licenta aplicatie ATI + Sala operatie	1 bucata Conform nr paturi din centralizatorul de mai sus
17	Institutul de Boli Cardiovasculare **Timişoara**	Servere pentru BD	2 bucati
		Servere de virtualizare	3 bucati
		Storage	1 bucata
		Server backup	1 bucata
		Firewall	2 bucati
		Switch agregare model 1	Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO
		Switch model 2	2 bucati
		UPS	2 bucati
		Rack	1 bucata
		Aer conditionat	2 bucati
		PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată	Conform nr paturi din centralizatorul de mai sus
		Data Terminal Server	Conform nr paturi
		Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă	2 bucati
		Acces point	Conform centralizatorului de mai sus
		Licente software pentru baze de date relationale	1 bucata
		Licenta platforma virtualizare	1 bucata
		Pachet licente solutie director	1 bucata
		Licenta aplicatie ATI + Sala operatie	Conform nr paturi din centralizatorul de mai sus
18	Spitalul Clinic Judeţean de Urgenta **Timişoara**	Servere pentru BD	2 bucati
		Servere de virtualizare	3 bucati
		Storage	1 bucata
		Server backup	1 bucata
		Firewall	2 bucati
		Switch agregare model 1	Alocarea se va determina in etapa de proiectare functie de dimensiunea retelei spitalului si numarul de posturi ATI+SO
		Switch model 2	2 bucati
		UPS	2 bucati
		Rack	1 bucata
		Aer conditionat	2 bucati
		PC certificat IP65 (protecţie contra apei) şi antibacteriană pentru sala de operaţii şi terapie intensivă cu masă dedicată	Conform nr paturi din centralizatorul de mai sus

		Data Terminal Server Echipamentele mobile de vizualizare soluţie mobilă terapie intensivă Acces point Licente software pentru baze de date relationale Licenta platforma virtualizare Pachet licente solutie director Licenta aplicatie ATI + Sala operatie	Conform nr paturi 2 bucati Conform centralizatorului de mai sus 1 bucata 1 bucata 1 bucata Conform nr paturi din centralizatorul de mai sus

4.3. RESURSE UMANE

Managementul de proiect reprezintă procesul de organizare, alocare și gestionare a activităților interdependente și a resurselor, pentru a asigura atingerea obiectivelor stabilite la standardele de calitate dorite, în condițiile existenței unor constrângeri referitoare la timp, resurse și costuri.

4.3.1. Resurse umane necesare în echipa Beneficiarului

Ministerul Sanatatii

Echipa de management:

- Manager de proiect (practician metodologia Comisiei Europeana PM² sau PMP/PMI)
- Manager tehnic
- Responsabil achizitii publice
- Responsabil financiar
- Responsabil contabilitate

Echipa de implementare, contractuali in afara organigramei:

- experți IT (1 **Team leader** cu experienta in Agile methodology, 1 **expert hardware** cu experienta in ATI/ICU Digital Infrastructure, point-of-care medical devices, experienta pe conectivitatea hardware dintre unitatile ATI si Sursele de date, 1 **expert software** cu experienta pe interoperabilitatea semantica HL7 si standardul eHealth Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR), experienta pe "smart " BI systems pe ATI/ICU medical devices clinical data)
- 1 expert în management de proiect (practician metodologia Comisiei Europeana PM² sau PMP/PMI, experienta in Agile SCRUM)
- 6 experți activități profesionale (medici)

Autoritatea pentru Digitalizarea Romaniei

Echipa de management:

- Coordonator activități partener
- Responsabil financiar

Echipa de implementare, contractuali in afara organigramei:

- Expert management de proiect (practician metodologia Comisiei Europeana PM² sau PMP/PMI)
- Expert monitorizare si raportare (experienta pe raportarile PM² /PMP/PMI artefacts (Issue, Risk, Change, Quality Review, Acceptanta, alte checklist-uri si log-urile cerute de metodologia aplicata)
- Expert financiar
- Expert 1 IT
- Expert 2 IT
- Expert 3 IT

-

4.3.2. Resurse umane necesare în echipa Furnizorului

Furnizorul va îndeplini următoarele condiții minime pentru echipa de proiect:

1.Manager de proiect - 1 persoană

Managerul de proiect din partea Furnizorului raportează direct Responsabilului de proiect al Beneficiarului și va asigura conducerea unică a echipei de proiect.

Cerințe minime:
- Studii superioare în domeniul IT de lungă durată, finalizate și cu diplomă de licență;
- Diploma/certificare prin care se dovedește deținerea de competențe/cunoștințe în domeniul managementului de proiect;
- Experiența profesională generală în management de proiect de minim 5 ani;
- Participarea în cel puțin un proiect similar cu desfășurare națională în poziția de manager, coordonator sau director de proiect.

Responsabilități:
- Punct unic de contact în relația cu BENEFICIARUL
- Monitorizarea implementării proiectului;
- Elaborarea planului revizuit de activități și urmărirea respectării termenelor proiectului;
- Elaborarea rapoartelor de progres lunare ce vor fi înaintate spre aprobare BENEFICIARUL
- Supraveghează îndeplinirea de către prestator a obligațiilor asumate în conformitate cu contractul semnat.
- Coordonarea activităților de informare și instruire aferente fiecărei etape a proiectului;
- Asigurarea accesului ușor la toată documentația proiectului.

2.Manager de proiect tehnic - 1 persoană

Cerințe minime:
- Studii superioare în domeniul IT de lungă durată, finalizate și cu diplomă de licență;
- Certificat privind metodologia Scrum Agile Waterfall (sau echivalent) de dezvoltare produse software pentru rolul și responsabilitățile de Scrum Master;
- Experiența profesională specifica de minim 5 ani;
- Participarea în cel puțin un proiect/contract la nivelul căruia să fi desfășurat activități similare contractului;

Responsabilități:
- Gestionarea implementării sistemului (componente software și de securitate);
- Coordonarea întregii echipe tehnice, cu alocarea sarcinilor pe fiecare membru al
- echipei;
- Asigură o adresă de e-mail funcțională a echipei de proiect în scopul facilitării comunicării dintre echipa de proiect și BENEFICIARUL
- Asigură resurse pentru executarea serviciilor de implementare cuprinse în specificațiile tehnice;
- Menține și aplică managementul riscurilor și procedurile de asigurare a calității;
- Întocmește toate rapoartele tehnice necesare conform cerințelor proiectului și/sau alte rapoarte cerute de către managerul de proiect.

3.Arhitect de soluție - 1 persoană

Cerințe minime:
- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licență;
- Diploma/certificare prin care se dovedește deținerea de competențe/cunoștințe in domeniul arhitecturilor complexe, de tip Enterprise (exemplu TOGAF);

- Experiența profesională generală de minim 5 ani;
- Participarea în cel puțin un proiect similar cu desfășurare națională în poziția de arhitect.

Responsabilități:
- Coordonează activitatea de proiectare și definire a arhitecturii sistemului;
- Participă la definirea modelelor de date
- Participă la definirea arhitecturii de integrare
- Raportează stadiul proiectării soluției către managerul de proiect și către Responsabilul de proiect din partea Beneficiarului.

4.Analist business - 1 persoană

Calificări și experiență:
- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licență;
- Diploma/certificare prin care se dovedește deținerea de competențe / cunoștințe privind analiza de business în contextul sistemelor informatice, conform unei metodologii standardizate (exemplu CBAP, CCBA);
- Experiența profesională generală similar de minim 5 ani;
- Participarea în cel puțin un proiect similar (modelarea proceselor de business conform BPMN 2.0) cu desfășurare națională în poziție similară.

Responsabilități:
- Analiza a cerințelor funcționale și nefuncționale;
- Realizarea documentelor de analiza și a specificațiilor;
- Coordonează activitățile de analiză de business;
- Analizează, definește procesele de business și elaborează specificațiile detaliate ale proceselor;
- Coordonează analiza cerințelor pentru schimb de date cu organizațiile implicate și elaborează un raport în acest sens;
- Participă la definirea scenariilor de testare;
- Participă la structurarea procesului de instruire.

5. Arhitect infrastructură hardware - 1 persoană

Cerințe minime:
- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licența;
- Certificare recunoscuta national/international în soluții de virtualizare (design, instalare, configurare, management);
- Certificare recunoscuta national/international pentru soluțiile de server si storage propuse
- Experiență profesională generala de minim 5 ani în infrastructură software, hardware și de comunicații;
- Participarea în cel puțin un proiect similar cu desfășurare națională în poziție similară.

Responsabilități:
- Evaluarea configurării infrastructurii hardware și de comunicații, precum și configurarea părții de infrastructură software din proiect;
- Documentarea instalării și configurării infrastructurii;
- Raportarea stadiului privind implementarea soluției către managerul de proiect și către Responsabilul de proiect din partea beneficiarului

6.Arhitect infrastructură hardware si comunicatii - 1 persoană

Cerințe minime:
- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licența;
- Certificare recunoscuta national/international pentru soluțiile de tip firewall propuse
- Certificare recunoscuta national/international pentru soluțiile de server si storage propuse

- Experiență profesională generala de minim 5 ani în infrastructură software, hardware și de comunicații;
- Participarea în cel puțin un proiect similar cu desfășurare națională în poziție similară.

Responsabilități:

- Evaluarea configurării infrastructurii hardware și de comunicații, precum și configurarea părții de infrastructură software din proiect;
- Documentarea instalării și configurării infrastructurii;
- Raportarea stadiului privind implementarea soluției către managerul de proiect și către Responsabilul de proiect din partea beneficiarului

7.Coordonator tehnic proces- 1 persoană

Cerințe minime:

- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licență;
- Certificare în domeniul bazelor de date, recunoscută de producătorul soluției, inclusiv pe specializarea de clustering de baze de date;
- Certificare tehnică în platforma de interconectare, recunoscută de producătorul soluției;
- Experiență profesională în cel putin un proiect de consolidare aplicații ce utilizează baze de date într-un rol similar.

Responsabilități:

- Evaluarea bazelor de date existente ale beneficiarului;
- Coordonarea activităților de proiectare si configurare a bazelor de date;
- Instruirea key-userilor beneficiarului;
- Coordonarea activităților de suport post-implementare.

8.Manager asigurarea calității, documentare tehnică și instruire - 1 persoană

Cerințe minime:

- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licență;
- Certificare de auditor în domeniul calității;
- Experiența profesională generală de minim 5 ani;
- Calificare/Certificare de formator;
- Participarea în cel puțin un proiect/contract la nivelul căruia să fi desfășurat activități similare contractului;

Responsabilități:

- Urmărește asigurarea calității în procesul de analiză /proiectare/ customizare /instalare/ testare/ validarea a sistemului;
- Pregătește întreaga documentație suport aferentă implementării și transferului de cunoștințe către Beneficiar;
- Urmărește implementarea metodologiilor;
- Întocmește planul de instruire;
- Coordonează instruirea conform planului de instruire;

9.Consultanți software aplicativ – 4 persoane

Cerințe minime:

- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licență;
- Experiență relevantă în proiecte similare în tehnologiile ofertate;
- Certificare recunoscuta national/international pentru solutia aplicativa de tip ATI +SO propusa
- Experiență în minim un proiect similar pe soluția propusă
- Experiența profesională generală de minim 5 ani;

Responsabilități:

- Analiza, configurare si customizare aplicatie ATI + SO

- Intocmire suport curs instruire utilizatori si key-useri
- Participarea la testarea aplicațiilor

10.Expert GDPR

Cerințe minime:
- Studii superioare în domeniul IT de lungă durată, finalizate și cu diplomă de licență;
- Certificare recunoscută internațional în domeniul protecției datelor cu caracter personal;
- Experiență de minimum 5 ani in domeniul IT;
- Participarea în cel puțin un proiect național la nivelul căruia să fi desfășurat activități conform rolului propus, protecția datelor cu caracter personal;

Responsabilități:
- Contribuie la analiza cerințelor care derivă din GDPR;
- Verifică/Testează funcțional și tehnic produsul rezultat împotriva cerințelor care derivă din GDPR.

11.Expert Business Intelligence – 1 persoană

Cerințe minime:
- Studii superioare de lungă durată în domeniul IT, finalizate și cu diplomă de licența;
- Certificari recunoscute la nivel național/internațional pe soluții de business intelligence si baze de date.
- Experiență profesională generala de minim 5 ani în IT;
- Participarea în cel puțin un proiect similar în poziție similară.

Responsabilități:
- Analiza cerințelor funcționale;
- Realizarea documentelor de analiza și proiectare a soluției de raportare;
- Configurarea și customizarea soluției de raportare;
- Participă la definirea scenariilor de testare
- Participă la structurarea procesului de instruire.

4.3.3. Experţii non-cheie

Prestatorul poate include in echipa de proiect si alți experți, daca este cazul, pentru îndeplinirea la timp a cerințelor din cadrul caietului de sarcini.
Pentru fiecare expert se vor prezenta următoarele documente justificative:
- Declarație privind disponibilitatea;
- CV - format Europass;
- diplome, certificate, atestate privind specializarea personalului (studiile, pregătirea profesionala, calificarea fiecărui expert propus in cadrul echipei de proiect);
- Recomandări emise de beneficiari si/sau orice alte documente relevante prin care se face dovada îndeplinirii experienței.

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.

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.

Serviciul de suport tehnic va avea scopul de a oferi utilizatorilor finali un Punct Unic de Contact pentru toate solicitările de intervenţii asupra componentelor software, pentru suport operativ şi pentru semnalările unor funcţionari defectuoase a soluţiei furnizate.
Remedierea defecţiunilor pe perioada garanţiei se va face la sediul beneficiarului proiectului sau prin intervenţie de la distanţă (*remote maintenance*), iar în cazul unor defecte mai grave, echipamentele se vor transporta la sediul furnizorului de către acesta.
Fiecare intervenţie în perioada de garanţie va fi documentată cu ajutorul unei fişe de intervenţie care va conţine următoarele detalii: data intervenţiei, descrierea intervenţiei, modalitatea de rezolvare a intervenţiei (reparaţie/înlocuire), durata de intervenţie şi confirmarea recepţiei prin semnăturile furnizorului şi beneficiarului.

Controlul intervenţiilor
Pentru înregistrarea tuturor tipurilor de intervenţii (preventive, corective, actualizări etc) si pentru asigurarea bunei funcţionări a produselor ofertate, se va propune daca este cazul, un model de registru pentru controlul intervenţiilor, care va fi validat de comun acord in urma workshop-urilor comune avute cu beneficiarul. Beneficiarul va actualiza acest registru cu toate informaţiile care descriu intervenţiile respective.

Prin garanţie se va asigura faptul că produsele sunt conforme cu specificaţiile tehnice, fără costuri suplimentare, pe toată durata garanției.
Ofertantul va da o declaraţie scrisă din care să rezulte garantarea produselor furnizate în conformitate cu cerinţa stabilită.

Ofertantul va da o declaraţie scrisă prin care să ateste că piesele de schimb, inclusiv bateriile reîncărcabile, dacă este cazul, vor fi puse la dispoziţia autorităţii/entităţii contractante de catre el sau printr-un prestator de servicii și că acestea (piesele de schimb) sunt conforme cu standardele europene.

6. MODALITATEA DE ELABORARE A OFERTELOR

În cadrul ofertei tehnice, Ofertantul va prezenta:

9.1.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

M.S. va indeplini rolul de Autoritate contractanta in prezenta procedura de achizitie publica si va fi responsabil cu organizarea acestei proceduri. Totodata, **M.S.** 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 **M.S.** (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 **M.S.**:
- 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 PRESATOR

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, M.S. (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 de prestare a serviciilor va fi elaborate conform standardelor internaționale în domeniu (ex: PM2, Prince2, PMBOK, ITIL, etc).

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)	Preţ unitar fără TVA (lei)	Valoare totală fără TVA (lei)	Valoare TVA (lei)	Valoare totală maximă cu TVA (lei)
1	……				
2	……				
…	……				
n	……				
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 **……. (……..) plati** 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 pentru fiecare livrabil din oferta financiara.

Platile se vor efectua pentru realizarea și finalizarea sub-activităților (conform Gantt al proiectului, livrabile si propunerea financiară) și se vor încadra în următoarele categorii:

- Analiza necesităților și proiectarea soluției informatice;
- Proiectarea, dezvoltarea aplicației 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 activitaţilor 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 - achiziţie soluţie 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 activitaţi
4	Fluctuaţii 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 influenţeaza 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	-selecţia atentă a furnizorilor de bunuri şi servicii, inclusiv pe baza performanţelor dovedite anterior -întocmirea unor documentaţii 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	-flexibilităţii 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 şi coordonare între membrii echipei de proiect	-stabilirea şi 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 influenţeze realizarea investiţiei.

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.