CAIET DE SARCINI

Achiziţia infrastructurii hardware şi software necesare pentru realizarea proiectului, precum și a serviciilor pentru managementul proiectului, a serviciilor de dezvoltare şi implementare a platformei de Cloud Computing (analiza cerințelor, proiectare, implementare, testare platforma, inclusiv portal web, precum și instruirea personalului care va administra Centrul de Date și platforma de Cloud Computing)

în cadrul proiectului

„INFRASTRUCTURĂ DE TIP CLOUD PENTRU INSTITUȚIILE PUBLICE DIN ROMÂNIA” - ICIPRO

Notă privind "Marca de produs"

În conformitate cu OUG 34/2006 privind achiziţiile publice, art.38, facem următoarele precizări:

- *Oriunde în caietul de sarcini se întâlnesc nume, mărci, denumiri pentru anumite produse se va considera implicit adăugată menţiunea „sau echivalent".*
- *Ofertele care vor stipula "echivalent" vor fi evaluate numai în baza informaţiilor furnizate de ofertanţi. Comisia de evaluare nu este responsabilă pentru obţinerea oricăror alte informaţii ajutătoare care nu sunt conţinute în ofertă.*

Notă privind dreptul de proprietate asupra acestui document

Notă privind cerinţele tehnice conţinute în acest document

Toate cerinţele tehnice conţinute în acest document sunt minime și obligatorii.

Cuprins

1 INFORMAŢII GENERALE

1.1 Detalii de contact ale Beneficiarului, loc de implementare

Beneficiar: Institutul Naţional de Cercetare-Dezvoltare în Informatică (ICI)

Adresa: B-dul Mareşal Al. Averescu 8-10, sector 1, 011455 București

1.2 Denumirea proiectului

Acest Caiet de Sarcini a fost pregătit pentru achiziţionarea soluţiei informatice (produse şi a servicii) necesară pentru realizarea proiectului „INFRASTRUCTURĂ DE TIP CLOUD PENTRU INSTITUȚIILE PUBLICE DIN ROMÂNIA” – ICIPRO.

1.3 **Contextul derulării proiectului**

Sfârșitul primului deceniu al secolului 21 a fost descris ca fiind atât un "punct de cotitură istorică" în dezvoltarea serviciilor de e-guvernare și "trecerea spre maturitate". [1] Aceste declarații, cuprinse în Documentul de lucru de e-Guvernare 2009 a sub-grupului Comisiei Europene, sunt confirmate și de creșterea măsurilor de politică în acest domeniu și schimbările în disponibilitatea și utilizarea informațiilor și comunicațiilor (TIC) pentru furnizarea de servicii publice. La lansarea Planului de acțiune privind guvernarea electronică 2011-2015 pentru Europa[2], vice-președintele Comisiei Europene și Responsabilă cu Agenda Digitală, Neelie Kroes a subliniat scopul de a *"ajuta autoritățile publice să utilizeze TIC pentru a oferi servicii mai bune la costuri mai mici, pentru a face viața mai ușoară și mai buna pentru cetățeni și mediul de afaceri"*. Cu toate acestea la 2 ani de la lansarea planului de acțiune, cetățenii UE sunt mai satisfăcuți de serviciile bancare online decât de serviciile publice online (6.5 nota de satisfacție pe o scara de la 0 la 10)[3], ceea ce arată că instituțiile publice trebuie să facă eforturi suplimentare în direcția e-Guvernare. Mai mult, România a rămas în urma majorităţii statelor membre UE în termeni legaţi de Tehnologia Informaţiei și Comunicațiilor (TIC), ocupând locul 67 din 142 în The Network Readiness Index (NRI) 2012. Indexul măsoară tendinţa ţărilor de a exploata oportunităţile oferite de TIC. Considerând acelaşi index, Bulgaria ocupă locul 70. România a căzut de pe locul 59 din 133 de ţări în NRI 2009. Tot în Planul de acțiune privind guvernarea electronică 2011-2015 pentru Europa se subliniază, de asemenea, că Mediul IT folosit în prezent în administrația publică, este caracterizat de fragmentarea accesului la resurse, sisteme duplicat, slabă utilizare a resurselor disponibile, proceduri de achiziţii complicate, în general un mediu greu de administrat și controlat, cu efect imediat asupra calităţii serviciilor prestate de către Administraţia publică către cetățeni. Un factor important în dezvoltarea serviciilor de e-Guvernare o reprezintă Cloud

1 Visions and priorities for eGovernment în Europe: Orientations for a post 2010 eGovernment Action Plan, European Commission eGovernment Sub-group, Working Paper (20 March 2009)

2 The European eGovernment Action Plan 2011-2015: Harnessing ICT to promote smart, sustainable & innovative Government, European Commission COM(2010)743 (15 December 2010)

3 Comunicat de presa Vicepreședintele Comisiei Europene, Neelie Kroes, Bruxelles , 28 mai 2013.

Computing-ul, cu potenţial de a juca un rol major în a adresa aceste ineficienţe și de a îmbunătății modul livrării serviciilor de către administrația publica. Modelul de Cloud Computing poate ajuta în mod semnificativ administrația publică prin servicii de înaltă disponibilitate, servicii inovative, accesibile imediat trecând peste bariera disponibilității resurselor specifice unui mediu IT tradițional. În sectorul privat, furnizorii și-au extins oferta de servicii de tip Cloud Computing, acum aceasta incluzând întreaga stivă de servicii specifică IT-ului tradițional: infrastructura software și hardware, platforma middleware, componente de aplicații și servicii, aplicații la cheie. Sectorul privat a identificat acest avantaj de a folosi și oferi servicii de tip Cloud Computing, pentru a îmbunătății modul de utilizare a resurselor, disponibilitate, accesul și inovativitatea. În mod similar pentru sectorul public (administrația publică), Cloud Computing deţine un potențial semnificativ pentru creșterea eficienței cu care sunt oferite serviciile publice către cetățeni, printr-o creștere a eficienței operaționale şi prin oferirea de resurse în mod optim.

Printre cele mai notabile inițiative de Cloud Computing la nivelul țărilor membre UE sunt: G-Cloud (Marea Britanie), Andromede (Franța) și Trusted Cloud (Germania). Toate aceste proiecte au demonstrat o eficiență energetică rezultată în urma optimizării folosirii centrelor de date. În Marea Britanie s-a înregistrat un consum energetic sub 10% pentru infrastructură față de soluțiile standard non-cloud. De asemenea, la nivel european exista un punct unic de acces la o gamă mare de date de la instituțiile și alte organisme ale Uniunii Europene „EUROPEAN UNION OPEN DATA[4]”. Acesta asigură un acces ușor și liber la date, cu scopul de a promova utilizarea inovatoare a acestora și creșterea potențialul economic. Se urmărește de asemenea stimularea transparentei și responsabilității instituțiilor și altor organisme ale UE. La nivel extra-european este notabilă inițiativa Open Government (cunoscută și sub numele Open Data) a Guvernului SUA, care are ca obiectiv creșterea transparenței actului guvernamental prin standardizarea, consolidarea și prezentarea unificată a datelor publice.

4 www.open-data.europa.eu

Conform unui studiu[5] efectuat la nivelul anului 2012 de către International Data Corporation, la nivelul Uniunii Europene, o investiție directă în servicii de tip Cloud Computing de 45 miliarde de euro, până în 2020, va avea un impact în produsul intern brut (GDP) de 957 Miliarde de euro.

Prezentul proiect se aliniază cu acțiunile întreprinse în aceasta direcție de Comisia Europeana și reprezintă totodată *o componentă a unei operațiuni mai complexe demarate de ICI București* în vederea sprijinirii instituțiilor publice prin implementarea unei soluții integrate de Cloud Computing la nivel național. Totodată, pentru a-și îndeplini rolul și responsabilitățile de furnizare de servicii de Data Center pentru beneficiarii din instituțiile publice, ICI București a demarat în 2011 lucrările de modernizare a „Clădirii corpului B, Secțiunea 2 din ansamblul ICI", cu destinație de Centru de Date și Cloud Computing. Prezentul proiect continuă inițiativele întreprinse de ICI București de a-și dezvolta capacitatea instituțională și operaționala în vederea asumării rolului de furnizor de servicii de Data Center pentru beneficiarii din administrația publică centrală și locala prin dotarea Centrului de Date și dezvoltarea și implementarea soluției de Cloud Computing la nivel central, incluzând integrarea soluțiilor proprii dezvoltate pentru Instituțiile publice din România.

Având în vedere contextul european și românesc, dar și:

- activitatea Institutului Naţional de Cercetare - dezvoltare în Informatică – ICI București în informatizarea administraţiei publice, a sectoarelor economiei naţionale şi a societăţii în ansamblu.

5 "Quantitative Estimates of the Demand for Cloud Computing în Europe and the Likely Barriers to Take-up", ICI

- portofoliul de proiecte relevante pentru sectorul de e-guvernare, printre care administrarea **ROTLD** (top level domain) ".ro", **Biblioteca naţionale de programe (BNP[6])**, **SPOCS[7].**
- atribuția de furnizare de servicii TIC la cerere, inclusiv servicii de data Center pentru beneficiarii din administrația publică centrală și locală și din alte instituții publice.

ICI București va asigura dezvoltarea și implementarea unei soluții integrate de Cloud Computing la nivel național, incluzând integrarea soluțiilor moderne dezvoltate pentru Instituțiile publice din România.

1.4 Sursa de finanţare

Proiectul a cărui implementare face obiectul acestui caiet de sarcini beneficiază de finanţare din Fondurile Structurale ale UE în cadrul Programului Operațional Sectorial Creșterea Competitivității Economice, Axa III „Tehnologia Informaţiei și Comunicaţiilor pentru sectoarele privat şi public”, Domeniul Major de Intervenţie 2 „Dezvoltarea și creşterea eficienţei serviciilor publice electronice”, Operaţiunea 1 „Susţinerea implementării de soluţii de e-guvernare și asigurarea conexiunii la broadband, acolo unde este necesar”, Apelul 5. Contractul de finanţare aferent acestui proiect este înregistrat la Ministerul Societății Informaționale cu numărul 194/321/6.12.2013, cod SMIS 48594.

1.5 Obiectivele şi rezultatele proiectului

Obiectivul General al proiectului îl constituie modernizarea, dezvoltarea și eficientizarea serviciilor publice oferite către cetățeni prin intermediul unei infrastructuri de tip Cloud

6 **Biblioteca naţională de programe şi e Servicii** implementată de către ICI București în vederea creșterii interoperabilității sistemelor informatice din administrația publică, prin utilizarea produselor software deja existente pe piața IT și colectarea și administrației informațiilor despre produsele program potențial utilizabile în instituțiile administrației publice și în mediul de afaceri din România.

7 Comisia s-a angajat să sprijine dezvoltarea și utilizarea unor servicii publice online care să funcționeze dincolo de frontiere. În special, Comisia a contribuit la finanțarea unor Proiecte-pilot la scară largă care creează legături între diferite sisteme online naționale și pun temelia serviciilor publice transfrontaliere europene. În prezent sunt în curs de pregătire proiectele eID (STORK 2.0), e-sănătate (epSOS) și eJustiție (eCODEX). Proiectele-pilot anterioare e-Afaceri **(SPOCS)** și e-achiziții publice (PEPPOL, în prezent Open PEPPOL ASBL) s-au încheiat cu succes.

Computing care să eficientizeze achiziția și utilizarea TIC (Tehnologia Informației și Comunicațiilor) la nivelul instituțiilor publice, să sporească transparența activității instituțiilor publice și să faciliteze interoperabilitatea între serviciile electronice publice.

Obiective specifice:

1. Creșterea capacitații operaționale la nivelul Institutului Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti, în conformitate cu standardele și normele naționale şi europene, în vederea asigurării unui cadru organizațional și funcţional eficient pentru amenajarea, utilarea și dotarea unui Centru de Date dedicat în principal susținerii informatizării instituțiilor publice din Romania.

2. Eficientizarea sistemului de achiziții publice pentru echipamente și servicii IT&C în cadrul instituțiilor publice locale și centrale prin proiectarea şi implementarea unei platforme de Cloud Computing la nivel central dedicată instituțiilor publice din România;

3. Dezvoltarea capacității profesionale a angajaților Institutului Naţional de Cercetare - Dezvoltare în Informatică - ICI Bucureşti în vederea creşterii abilităţilor de utilizare a tehnologiilor Cloud, utilizând cunoştinţe specifice dobândite în urma activităţilor de instruire, precum și diseminarea acestora către alte structuri TIC din instituțiile publice din România.

Proiectul se încadrează în prevederile obiectivului general al Programului Operaţional Sectorial „Creşterea Competitivităţii Economice”, privind îmbunătăţirea productivităţii în toate sectoarele de activitate și reducerea decalajului acestui indicator faţă de nivelul mediu al productivităţii în UE, astfel ca până în 2015, România să atingă 55% din productivitatea medie a UE. Implementarea proiectului va contribui la creşterea eficienţei serviciilor publice oferite către populaţie/mediul de afaceri/administraţie, îndeplinind astfel obiectivele Axei Prioritare 3 – „Tehnologia Informaţiei și Comunicaţiilor pentru sectoarele privat şi public” de sprijinire a competitivităţii economice și promovarea interacţiunii între sectorul public şi întreprinderi/cetăţeni prin valorificarea potenţialului TIC.

Proiectul se află în concordanţă cu obiectivul specific al Domeniului Major de Intervenţie 2 („Dezvoltarea şi creşterea eficienţei serviciilor publice electronice”) întrucât are ca scop oferirea de facilitați instituțiilor publice în vederea eficientizării activității de furnizare de servicii publice cetăţenilor/mediului de afaceri/administraţiei.

Totodată proiectul este realizat în spiritul promovării Guvernării electronice prin utilizarea de instrumente și sisteme disponibile graţie tehnologiilor informaţiilor şi comunicațiilor (TIC), pentru a asigura premisele de oferire de servicii publice mai bune pentru cetăţeni și întreprinderi. Guvernul României, consideră Cloud Computing ca având importanță strategică pentru dezvoltarea sectorului public și a industriei TIC locale. Serviciile de Cloud Computing vor deveni prima opțiune pentru instituţiile publice, asigurând astfel o utilizare mai eficientă a resurselor TIC, o reducere semnificativa a costurilor și o creștere semnificativa a serviciilor oferite către cetățeni. Beneficiile pentru utilizatori pot fi exprimate succint printr-un acces facil, indiferent de locaţie şi timp, la informaţiile de care au nevoie într-un mod eficient şi transparent prin intermediul portalului web care va fi creat în cadrul proiectului, reducerea reală a costurilor, îmbunătăţirea managementului operaţional printr-o mai bună alocare a resurselor necesare rezolvării problemelor și necesităților instituțiilor publice beneficiare.

Soluţia tehnică ce va fi implementată va permite găzduirea de sisteme informatice ce sprijină desfășurarea activităților instituțiilor publice, în calitate de beneficiari finali, obiectivul fiind oferirea de servicii de eGuvernare către cetățeni la nivele ridicate de calitate.

Prin implementarea proiectului, ICI va oferi instituțiilor publice din Romania, prin intermediul rețelei Internet, putere de calcul „brută” sau specializată și acces la o serie de servicii și facilități partajate. Esenţa acestui model îl reprezintă virtualizarea: beneficiarul îşi poate configura prin software un întreg sistem informatic, în care poate integra o gamă largă de „echipamente virtuale” (servere, router-e, etc.), softuri generice (servere web, baze de date) şi, peste toate acestea, propriile aplicaţii. Implementarea unei soluții integrate de Cloud Computing național, la rândul său, implică urmărirea următoarelor direcții:

a. **Consolidare Centre de Date***:* Asigură resurse IT, de procesare și stocare și comunicații performante ce vor permite ministerelor, agențiilor și oricăror alte instituții locale sau centrale să migreze tehnica de calcul regăsită sub formă de centre de date locale, sau calculatoare individuale, pe o platformă unică centrală, disponibilă într-un regim înalt de disponibilitate conform tuturor bunelor practici în domeniu, reducând astfel costurile locale cu administrarea propriei infrastructuri IT, specifice fiecărei instituții.

b. **Continuitatea serviciilor în urma unui dezastru** (Business Continuity):

    i. Construiește o platformă ce va permite salvarea datelor oricărei instituții publice locale sau centrale din România.

ii. Stochează imagini ale aplicațiilor și bazelor de date pe un spațiu de stocare central, permițând recuperarea rapidă în cazul unei erori apărute în sistemul productiv primar.

iii. Mecanismele de salvare (backup) și recuperarea după dezastre (Disaster Recovery) permit planificarea și execuția acestora prin rețea, permițând utilizatorilor să folosească în mod optim resursele de rețea.

c. **Platforma de Cloud Computing,** care va asigura**:**

i. Îmbunătățirea capacitaților centrului de date atât din punct de vedere al funcţionalităţii oferite de clădire, mecanisme mecanice și electrice puse la dispoziție pentru suportul operațional.

ii. Îmbunătățirea capacitaților de rețea pentru a putea oferi un suport eficient și centralizat sistemelor informatice.

d. **Servicii Cloud Computing,** ce vor defini bazele dezvoltării de servicii Cloud Computing:

i. Asigură servicii adecvate ce permit diferitelor instituții publice sa migreze pe platforma de Cloud Computing a serviciilor electronice, sau să dezvolte servicii electronice noi. Aceste servicii vor pune la dispoziție resurse IT (Procesoare, Spații de Stocare, capacitații de comunicații) dar și platforme de software specializate. Aceste servicii în ansamblul lor vor constitui servicii de tip:

- IaaS (Infrastructure as a Service),
- PaaS (Platform as a service);

ii. Asigură o platformă națională de interoperabilitate, punând la dispoziție servicii de integrare la nivel de date și servicii partajate.

iii. Dezvoltă capabilitățile de tip e-guvernare, prin implementarea de servicii electronice specifice.

e. **Instruire și dezvoltare,** prin asigurarea:

i. Instruirii personalului care va utiliza și administra soluția integrată de Cloud Computing.

ii. Asigură instruirea online întregii comunităţi IT&C din România, cu privire la serviciile de Cloud Computing ale Guvernului României.

iii. Dezvoltarea unei expertize în vederea implementării de servicii naționale electronice, prin punerea la dispoziție a tuturor informațiilor necesare și a unui cadru operațional de lucru ce face posibilă definirea, dezvoltarea și implementarea de astfel de servicii.

În vederea atingerii acestor obiective sunt luat în considerare următoarele activități:

I. Implementarea și operaționalizarea unei infrastructuri eficiente de tip Cloud Computing destinată consolidării centrelor de date ale Instituțiilor Publice din România, în măsură să ofere acestora Infrastructură TIC ca Serviciu (IaaS – Infrastructure as a Service) și Platformă TIC ca Serviciu (PaaS – Platforma as a Service). Această infrastructură de tip Cloud Computing va avea ca obiectiv eficientizarea achiziționării și operării de infrastructură TIC de către instituțiile publice din România.

II. Implementarea și operaționalizarea unei platforme destinate standardizării, unificării și prezentării integrate a datelor de interes public din România. În cadrul acestui obiectiv specific se disting următoarele componente:

   a. Implementarea unei platforme de preluare, standardizare și unificare a datelor de interes public

   b. Preluarea unui set de date relevante de la instituțiile partenere ale ICI

III. Implementarea și operaționalizarea unei platforme de interoperabilitate destinate serviciilor publice din România. În cadrul acestui obiectiv specific se disting următoarele componente:

   a. Implementarea unei platforme de interoperabilitate de tip SOA (Service Oriented Architecture), care să includă un registru al serviciilor electronice publice și o platformă dedicată schimbului de mesaje între serviciile publice

   b. Implementarea unor interfețe de interoperabilitate cu Serviciul Electronic de Achiziții Publice (SEAP)

IV. Implementarea unui portal web care să prezinte Datele standardizate și unificate și Registrele cu aplicații și servicii ale instituțiilor publice din România

V. Implementarea unui set de servicii electronice standardizate care să adauge valoare infrastructurii TIC de tip Cloud Computing rezultate: serviciul de management electronic al documentelor, serviciul de gestiune standardizată a cataloagelor și registrelor, aplicații standardizate de aprobare și de planificare a audiențelor

VI. Pregătirea și constituirea unei noi entități specializate pentru administrarea și operarea Infrastructurii de tip Cloud Computing destinate Instituțiilor Publice din România

VII. Definirea unui cadru de lucru care să acopere modul de furnizare și utilizare a Infrastructurii ca serviciu și a Platformei ca serviciu, guvernanța datelor și serviciilor găzduite în cadrul ICIPRO, precum și nivelul de servicii

VIII. Promovarea proiectului și a Infrastructurii de tip Cloud Computing rezultate

1.6 **Aria de acoperire a proiectului**

1.6.1 Aria de acoperire instituțională

ICI București beneficiază de rezultatele prezentului proiect întrucât, conform HG nr. 1621/2003 pentru organizarea şi funcţionarea Institutului Naţional de Cercetare-Dezvoltare în Informatică și a ordinului nr. 306/10.05.2013 de aprobare a noii structuri organizatorice ICI București, principalele activități și atribuții, sunt orientate în principal spre: (i**) furnizare de servicii de data Center pentru beneficiarii din administrația publica centrala și locala** (ii) Servicii de administrare, organizare şi gestionare a **Bibliotecii naţionale de programe și e Servicii** în vederea creșterii interoperabilității sistemelor informatice din administrația publica, prin utilizarea produselor software deja existente pe piața IT și colectarea și administrarea informațiilor despre produsele program potențial utilizabile în instituțiile administrației publice și în mediul de afaceri din Romania; (iii) Servicii de securitate a informaţiilor şi reţelelor; (iv) Servicii de cercetare în dezvoltarea unor infrastructuri pilot de comunicaţii pentru Grid, a unor organizaţii virtuale în tehnologie Grid pentru modelare, simulare și optimizare de înaltă performanţă, elaborarea de metodologii, instrumente software şi produse prototip pentru dezvoltarea aplicaţiilor pe infrastructura Grid; (v) informatizarea administraţiei publice, a sectoarelor economiei naţionale şi a societăţii în ansamblu etc.;

Astfel, **beneficiarii direcți** ai proiectului sunt reprezentați în primul rând de **ICI București** prin faptul ca își va asigura infrastructura necesară pentru a-și asuma în condiții de maximă eficiență și eficacitate atribuția de furnizor de servicii de data Center pentru beneficiarii din administrația publică centrală și locală și va crea mediu propice pentru promovarea și accesibilizarea soluțiilor și programelor proprii destinate instituțiilor publice, precum Biblioteca Națională de Programe și e-Servicii.

Autoritățile publice locale, centrale și alte instituții publice în calitate de furnizori de date și informații cu caracter public de asemenea sunt beneficiari direcți, deoarece aceștia vor beneficia de transpunerea informațiilor/ datelor

publice proprii prin platforma de Cloud Computing, asigurând astfel premisele creării unui „unic” loc în care cetățenii, mediul de afaceri și instituțiile publice găsesc informații publice utile pentru activitățile acestora.

De asemenea, beneficiari direcți sunt și **163** de **angajaţi ai ICI** din departamentul „Data Center Cloud Computing”, prin crearea unui mediu eficient și complex de muncă și care vor avea astfel acces la o imagine globală asupra activităţii proprii, putând să-şi adapteze rapid acţiunile în funcţie de nevoile beneficiarilor și cerinţele economice și legislative ale momentului, dar și cei **14 participanți la cursurile de instruire** ce vor fi organizate prin proiect: 10 administratori de servicii și 4 administratori de sistem instruiți în vederea dobândirii de competențe de utilizare a infrastructurii rezultate din proiect. Beneficiile proiectului pentru participanții la cursuri vor consta în creșterea competențelor profesionale și dobândirea de noi abilități ca urmare a utilizării tehnologiilor informaționale pentru accesul la informații.

În categoria **beneficiarilor direcți** intra și **administrația publică centrală și locală** și alte instituții publice din România, în calitate de consumatori de informații, date și servicii electronice publice. De asemenea, cetățenii și mediul de afaceri vor beneficia direct de serviciile implementate în cadrul acestui proiect, cu precădere de serviciul „Date deschise” care le va facilita accesul la informații de interes public într-un mod integrat, standardizat.

Indirect, cetățenii și mediul de afaceri din Romania vor beneficia de rezultatele prezentului proiect, prin prisma faptului ca se creează premisele pentru eficientizarea activității autorităților publice locale și centrale în vederea furnizării de servicii publice de înaltă calitate.

1.6.2 Aria de acoperire geografică

Sistemul informatic care va fi implementat va fi unul de tip centralizat. Nodul central de procesare va fi instalat în sediul ICI din București, în spaţiul tehnic existent la adresa B-dul Mareșal Averescu nr. 8-10, sector 1, București. Utilizarea sistemului informatic se va realiza la nivel național, în cadrul tuturor structurilor beneficiare ale proiectului (conform secțiunii Error: Reference source not found), prin intermediul Internetului.

1.6.3 Populația de utilizatori - Grup țintă

Beneficiari direcți ai proiectului sunt **163** de **angajaţi ai Autorității Contractante** prin crearea unui mediu eficient și complex de muncă și care vor avea astfel acces la o imagine globală asupra activităţii proprii, putând să-şi adapteze rapid acţiunile în funcţie de nevoile beneficiarilor și de cerinţele economice și legislative ale momentului, dar și cei **14 participanți la cursurile de instruire** ce vor fi organizate prin proiect: 10 administratori de servicii și 4 administratori de sistem instruiți în vederea dobândirii de competențe de utilizare a infrastructurii rezultate din proiect.

1.6.4 Legătura cu alte sisteme informatice și proiecte

TIP	DENUMIRE	MOD DE RELAŢIONARE
PROGRAM	Programul de guvernare 2013-2016	- direct, proiectul contribuind la implementarea direcției de acțiune „e-Guvernare, Interoperabilitate, Cloud Computing, Media Sociale” pentru instituțiile publice”. Implementarea tehnologiilor de tip Cloud „la nivelul instituțiilor publice prin crearea unei platforme centralizate, scalabile și dinamice care să ofere servicii IT de calitate cu costuri reduse, la un nivel de securitate la standarde europene.”[8]
Strategia	„Strategia naţională privind Agenda Digitală pentru România”	direct, proiectul contribuind la implementarea direcției de acțiune „Întărirea eforturilor și a eficienței”, acțiuni privind *„Asigurarea unui sprijin financiar suficient pentru infrastructurile comune de cercetare din domeniul TIC și pentru clusterele inovatoare, dezvoltarea de noi e-infrastructuri și elaborarea unei strategii UE privind „cloud computing”,îndeosebi pentru administrația publică și știință;”* deoarece prin proiect este propusa implementarea la nivel central a unei soluții integrate de Cloud Computing destinate instituțiilor publice din Romania;
PROGRAM	POSCCE -Programul Operaţional Sectorial - Creşterea Competitivităţii Economice	- direct, prezentul proiect fiind elaborat în vederea finanţării în cadrul POS - Creşterea Competitivităţii Economice întrucât prin prezentul proiect sunt create premizele de îmbunătățire a cadrului relaţional dintre administraţia publică și întreprinderi/cetăţeni.
PROGRAM	PODCA - Programul Operaţional - Dezvoltarea Capacităţii	- direct, relaţionare atât cu Axa Prioritară 1 - *Îmbunătăţiri de structură și proces ale managementului ciclului de politici publice*, cât şi cu Axa Prioritară 2 – *Îmbunătățirea calităţii și eficienţei*

8
ICI

	Administrative	*furnizării serviciilor publice cu accentul pus pe procesul de descentralizare.* Prezentul proiect constituie un instrument pentru atingerea unor obiective precum: îmbunătăţirea procesului de luare a deciziilor, îmbunătăţirea eficacităţii organizaţionale, îmbunătăţirea calităţii și eficienţei serviciilor furnizate.
STRATEGIE	Strategia Europa 2020	- direct, deoarece proiectul propus se încadrează în liniile directoare ale **Strategiei Europa 2020** întrucât creează premisele utilizării de către solicitant și beneficiar, la scară largă, a tehnologiilor informaţionale recunoscute la nivel, prin infrastructura și soluția integrata de Cloud Computing la nivel central.
ALT DOCUMENT RELEVANT LA NIVEL NAŢIONAL/REGIONAL	Planul Naţional de Dezvoltare (PND) 2007 - 2013	- direct, proiectul propus se află în concordanţă cu **Planul Naţional de Dezvoltare 2007-2013 (PND)** întrucât acţionează în direcţia reducerii cât mai rapide a decalajelor existente faţă de Uniunea Europeană prin extinderea utilizării tehnologiei informaţiei și comunicaţiilor. Proiectul sprijină atingerea obiectivelor PND respectiv creşterea competitivităţii economice, îmbunătăţirea capacităţii administraţiei publice de formulare şi implementare a politicilor publice, creşterea calităţii serviciilor publice (inclusiv prin reducerea birocraţiei și realizarea unei administraţii eficiente, moderne şi orientate către cetăţean).
ALT DOCUMENT RELEVANT LA NIVEL NAŢIONAL/REGIONAL	**Cadrului Naţional Strategic de Referinţă 2007-2013 (CNSR)**	Proiectul contribuie la realizarea obiectivelor **Cadrului Naţional Strategic de Referinţă 2007-2013 (CNSR)** deoarece facilitează propagarea inovaţiilor tehnologice prin implementarea unui sistem informatic modern care va îmbunătăţi procesele de lucru din cadrul ANPC.
ALT DOCUMENT RELEVANT LA	Planul Naţional de Reforme	- direct, proiectul contribuind la promovarea TIC în administraţie. De asemenea, proiectul, prin

NIVEL NAŢIONAL/REGIONAL		implementarea sa, continuă şi dinamizează procesul de simplificare a activității administrative a instituțiilor publice, unul din obiectivele majore ale reformei administraţiei publice, venind astfel indirect în sprijinul cetăţeanului și al administraţiei însăşi.

1.7 Plan de implementare/execuţie

Proiectul în cadrul căruia se desfășoară prezenta achiziție se derulează pe o perioadă de 18 luni, începând cu data de 09.12.2013. Durata contractul de furnizare care va fi adjudecat ca urmare a acestei proceduri de atribuire se va desfășura conform graficului orientativ de mai jos, mai precis pe o perioada de maximum 12 luni, începând cu luna a 7-a a contractului de finanțare și având termenul final în luna a 18-a a perioadei alocate.

Ofertanții pot propune devansarea unor activități (termene intermediare de start și de finalizare), dar depășirea termenelor maximale de start și de finalizare indicate nu este permisă, sub sancțiunea respingerii ofertei.

Activitate/ Subactivitate	**Anul 1**							
	Luna 1	**Luna 2**	**Luna 4**	**Luna 5**	**Luna 6**	**Luna 8**	**Luna 9**	**Luna 11**
Activitatea 1. Managementul de proiect (managementul contractului de finanțare)								
Activitatea 2. Activități de amenajare a centrului de date și a spațiilor adiacente								
Subactivitatea Realizare podea tehnologică și tavan fals								
Subactivitatea Cablare structurată de date și alimentare cu energie electrica								
Subactivitatea Implementarea sistemului de asigurare a climatului controlat								
Subactivitatea Asigurarea continuității alimentării cu energie electrică								

Activitate/ Subactivitate	Anul 1							
	Luna 1	Luna 2	Luna 4	Luna 5	Luna 6	Luna 8	Luna 9	Lun 11
Subactivitatea Implementarea sistemului de detectare, prevenire și stingere a incendiilor								
Subactivitatea Implementarea sistemului de securitate (control al accesului, monitorizare perimetrala)								
Activitatea 3. Proiectarea şi implementarea platformei de Cloud Computing								
Subactivitatea Analiza cerințelor platformei de Cloud Computing								
Subactivitatea Identificarea cerinţelor de interfaţare cu alte sisteme și produse existente								
Subactivitatea Proiectarea platformei de Cloud Computing								
Subactivitatea Livrarea, instalarea și configurarea infrastructurii hardware și software necesare pentru platforma de Cloud Computing								
Subactivitatea Testarea infrastructurii de Cloud Computing								
Subactivitatea Implementarea serviciilor bazate pe platforma de Cloud Computing								
Subactivitatea Implementarea serviciului „Date Deschise”								
Subactivitatea Implementarea serviciului „Biblioteca virtuală”								
Subactivitatea Implementarea platformei de interoperabilitate								
Subactivitatea Migrarea serviciilor ICI pe platforma de Cloud Computing								

Activitate/ Subactivitate	Anul 1							
	Luna 1	Luna 2	Luna 4	Luna 5	Luna 6	Luna 8	Luna 9	Lun 11
Subactivitatea Instruirea personalului care va administra Centru de Date și platforma de Cloud Computing								

2 DESCRIEREA CADRULUI LEGAL ŞI TEHNIC EXISTENT

2.1 Introducere

Institutul Naţional de Cercetare-Dezvoltare în Informatică reprezintă cel mai important institut de cercetare-dezvoltare şi inovare în domeniul Tehnologiilor Informaţiei și Comunicaţiilor din România. Prin asumarea priorităţilor ştiinţifice și tehnologice ale domeniului, misiunea ICI o constituie consolidarea poziţiei câştigate și dezvoltarea suportului ştiinţific şi tehnologic în domeniul tehnologiilor informaţiei și comunicaţiilor necesar realizării structurilor şi serviciilor specifice societăţii informaţionale bazate pe cunoaştere.

2.2 Cadrul organizatoric şi legislativ

Date generale

Începând cu anul 2001, ICI Bucureşti a obţinut, din partea companiei "SGS România S.A. - Servicii certificare internațională", certificarea ISO 9001 pentru activitatea de cercetare științifică și dezvoltare tehnologică care are ca rezultate produse, tehnologii, sisteme și servicii în domeniul tehnologiei informaţiei.

SCURT ISTORIC

1970 - Este înființat Institutul Central de Informatica (ICI) având menirea de principal centru pentru cercetare avansata în informatica. De-a lungul celor peste treizeci de ani de existenta, ICI a fost reorganizat sub diferite titulaturi.

1971 - Este înființat Institutul Central pentru Sisteme de Conducere cu Mijloace de Automatizare (ICSCMA); se conturează structura sa organizatorica.

1973 - ICSCMA devine Institutul Central pentru Conducere și Informatica (ICCI); se dezvolta atribuțiile institutului pe patru coordonate principale: organizarea activității de conducere,

introducerea sistemelor informatice, dotarea economiei cu tehnica de calcul, pregătirea cadrelor de specialiști și alte atribuții de coordonare.

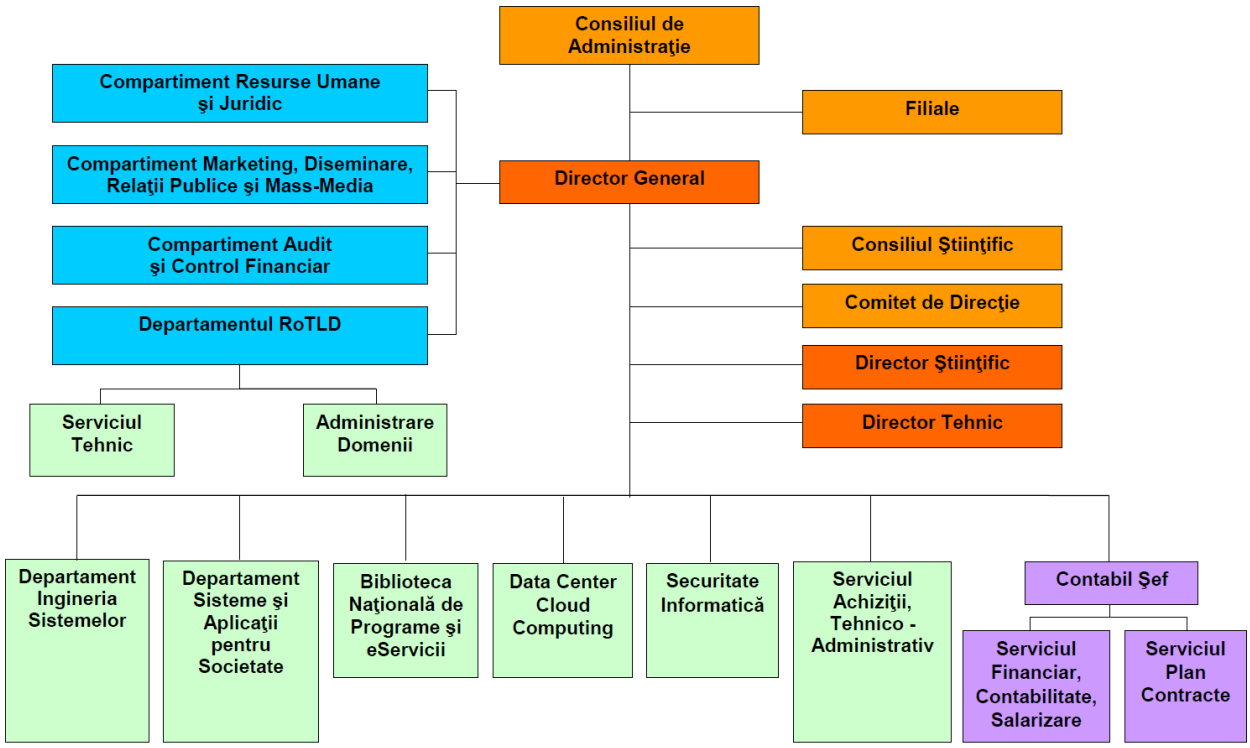
1985 - ICI devine direcția de "Informatica" în cadrul Institutului de Cercetare Științifică și Inginerie Tehnologica pentru Tehnica de Calcul și Informatica (ICSIT -TCI); în aceasta etapa, se pune un accent mai mare pe aspectele de dezvoltare și de valorificare a rezultatelor cercetării.

1990 - O noua denumire: Institutul de Cercetări în Informatica (ICI), reconstituirea ca institut de sine stătător și adaptarea la cerințele economiei de piață, cu intenția de a continua activitățile de cercetare științifică.

1998 - În temeiul **HG nr.936/23 decembrie 1998**, ia ființa Institutul National de Cercetare - Dezvoltare în Informatica - ICI București.

2001 - ICI trece în coordonarea Ministerului Comunicațiilor și Tehnologiei Informației.

ORGANIGRAMA



ICI

Arii de Competenţă

- reţele de comunicaţie şi tehnologii avansate pentru dezvoltarea de aplicaţii în medii distribuite;
- tehnologiile informaţiei și comunicaţiilor în domenii de interes public;
- conţinut digital, creativitate și dezvoltare personală;
- tehnologiile informaţiei și comunicaţiilor, suport pentru dezvoltarea afacerilor şi a industriei; noi modele şi tehnologii în ingineria sistemelor şi a produselor software;
- sisteme bazate pe cunoştinţe, învăţare şi sisteme cognitive;
- sisteme avansate de calcul şi control.

Activităţi

- cercetare-dezvoltare-inovare în cadrul programelor naţionale şi internaţionale;
- transfer tehnologic şi valorificarea rezultatelor cercetărilor din domeniul Tehnologiei Informaţiei și Comunicaţiilor;
- elaborare de produse şi sisteme informatice pentru diverse domenii de activitate;
- colaborare în domeniul de activitate cu academii de ştiinţă şi institute similare din alte ţări;
- dezvoltare, implementare şi furnizare de servicii informatice inclusiv în domeniul reţelelor de calculatoare;
- elaborare de studii de diagnoză și prognoză privind dezvoltarea domeniului Tehnologiei Informaţiei și Comunicaţiilor;
- realizare de proiecte în calitate de coordonator de proiecte complexe şi integrator de soluţii și componente hardware şi software;

- editare și tipărire de publicaţii în domeniul Tehnologiei Informaţiei și Comunicaţiilor;

2.3 Conformitatea cu obiectivele Strategiei "Agenda digitală pentru România

Proiectul se adresează Domeniului de acțiune 1, e-Guvernare, interoperabilitate, securitatea rețelelor și sistemelor informatice, cloud computing și media sociale, din cadrul Strategiei "Agenda digitală pentru România", răspunzând următoarelor obiective strategice ale acestui domeniu:

- Sporirea gradului de transparență a actelor administrației publice prin informatizarea serviciilor publice, întrucât proiectul propune servicii ce facilitează accesul cetățenilor la informații și documente de interes public și anume "Date deschise" (platformă de standardizare și unificare a datelor de interes public deținute/generate de instituțiile publice din România, care va facilita accesul unificat și standardizat al cetățenilor și mediului de afaceri la informații de interes public - de exemplu o hartă a zonelor de risc, o hartă cu ariile naturale protejate, indicatori și statistici cu privire la populația activă) și "Biblioteca virtuală" (serviciu destinat stocării și prezentării într-o formă standardizată a oricăror documente electronice ce nu pot fi stocate în mod eficient și în condiții de siguranță de către instituțiile publice din România, incluzând bibliotecile publice, muzeele, instituțiile de învățământ sau instituțiile administrației publice din România).

- Creșterea accesului la servicii publice digitalizate. Cetățenii și organizațiile, inclusiv mediul de afaceri, vor avea un acces sporit la servicii publice digitalizate prin creșterea numărului de servicii publice ce vor putea fi accesate online.

- Eficientizarea administrației publice și scăderea cheltuielilor administrației publice prin interoperabilitatea serviciilor de interes public și posibilitatea de a utiliza în mod gratuit infrastructura de tip cloud computing, ceea ce diminuează considerabil cheltuielile administrației publice cu infrastructura IT, precum și costurile operaționale și consumurile energetice.

- Îmbunătățirea mediului de afaceri - prin acest proiect mediul de afaceri va beneficia de un acces facil la documente și informații de interes atât pentru activitatea specifică de afaceri, cât și pentru relația cu autoritățile publice.

- Îmbunătățirea guvernanței asupra implementării serviciilor publice informatizate. În cadrul proiectului se are în vedere implementarea unei platforme de interoperabilitate

care să susțină principiile arhitecturilor de tip SOA (Service Oriented Architecture). Implementarea acestei platforme va facilita interoperabilitatea între serviciile găzduite în cadrul platformei Cloud computing. De asemenea, această platformă va asigura integrarea cu alte servicii publice electronice, cum ar fi SEAP (Serviciul Electronic de Achiziții Publice).

2.4 Conformitatea cu Strategia națională de securitate cibernetică

Obiectivele proiectului sunt aliniate scopului Strategiei naționale de securitate cibernetică.

Scopul Strategiei de securitate cibernetică a României este acela de a defini și de a menţine un mediu virtual sigur, cu un înalt grad de rezilienţă și de încredere, bazat pe infrastructurile cibernetice naţionale, care să constituie un important suport pentru securitatea naţională şi buna guvernare, pentru maximizarea beneficiilor cetăţenilor, mediului de afaceri și ale societăţii româneşti, în ansamblul ei. În acest context, acest proiect conține prevederi cu privire la securitatea serviciilor și a datelor ce vor fi disponibile pe platforma de cloud dedicată instituțiilor publice.

Prin obiectivele sale, proiectul propune măsuri de exploatare a oportunităților identificate în Strategia națională de securitate cibernetică, și anume:

- Susţinerea politicilor şi promovarea intereselor naţionale;
- Dezvoltarea şi susţinerea mediului de afaceri;
- Creşterea calităţii vieţii prin dezvoltarea serviciilor oferite de societatea informaţională;
- Îmbunătățirea cunoaşterii și susţinerea deciziilor strategice naţionale în era informaţională prin asigurarea capacităţilor şi instrumentelor cibernetice adecvate;
- Creşterea nivelului de cunoaştere și a capacităţii de predicţie în scopul avertizării timpurii privind riscurile și ameninţările la adresa securităţii naţionale;
- Creşterea capacităţilor tehnice și a competenţelor resursei umane pentru realizarea obiectivelor de securitate naţională

3 SARCINILE OFERTANTULUI

3.1 Activităţi

3.1.1 Activitatea 1 - Managementul de proiect

Activitatea de management de proiect acoperă atât managementul implementării tehnice a soluției ICIPRO, cât și asistență asigurată autorității contractante pentru derularea în bune condiții a relației cu finanțatorul proiectului. Activitățile de management de proiect și de monitorizare a derulării contractului de finanțare sunt descrise pe larg în cadrul secțiunii 6 a acestui caiet de sarcini.

3.1.2 Activitatea 3 - Activități de amenajare a centrului de date și a spațiilor adiacente

Subactivitate	***Descriere subactivitate***
Realizare podea tehnologică	Podeaua tehnologică va fi amenajată pe un cadru metalic solid, astfel încât să poată susține greutatea echipamentelor instalate.
Cablare structurată de date și alimentare cu energie electrica	Cablurile de date și cele pentru alimentare cu energie electrică vor fi așezate pe canale dedicate.
Implementarea sistemului de asigurare a climatului controlat	În cadrul centrului de date se va implementa un sistem de asigurare a climatului controlat, necesar asigurării unei temperaturi optime de funcționare a echipamentelor.
Asigurarea continuității alimentării cu energie electrică	Circuitul electric de alimentare a echipamentelor din centrul de date va fi configurat astfel încât, în cazul întreruperii alimentării cu energie electrică din rețeaua de distribuție, alimentarea echipamentelor să poată fi preluată temporar de Sistemul de tip UPS furnizat în cadrul proiectului.
Implementarea sistemului de detectare, prevenire și stingere a incendiilor	Sistemul de detectare, prevenire și stingere a incendiilor va fi compus din senzori de fum și dintr-o instalație automată de stingere a incendiilor specializată pentru centre de date.
Implementarea sistemului de securitate (control al accesului, sisteme supraveghere)	Sistemul de securitate va asigura controlul accesului fizic cu ajutorul unui sistem bazat pe carduri de proximitate. Sistemul de control al accesului va fi completat de un sistem de monitorizare bazat pe camere video.

3.1.3 Activitatea 4 - Proiectarea şi implementarea platformei de Cloud Computing

Subactivitate	***Descriere subactivitate***
Analiza cerințelor platformei de Cloud Computing	În cadrul acestei activităţi vor fi determinate cerinţele funcţionale ale platformei de Cloud Computing , atât din punctul de vedere al beneficiarilor, cât şi din punctul de vedere al infrastructurii tehnice şi de securitate necesară și a activităților specifice ICI
Identificarea cerinţelor de interfaţare cu alte sisteme și produse existente	Platforma de Cloud Computing va fi analizată în contextul infrastructurii hardware şi software necesare, urmând a fi identificate modalităţile de comunicare şi interfaţare cu toate sistemele și produsele destinate instituțiilor publice cu care se va realiza interconectarea.
Proiectarea platformei de Cloud Computing	Vor fi proiectate serviciile ce vor fi puse la dispoziție de platforma de Cloud Computing și va fi definită modalitatea de implementare a acestor servicii. De asemenea vor fi proiectate mecanismele de management (monitorizare, control) a acestor servicii.
Livrarea, instalarea și configurarea infrastructurii hardware și software necesare pentru platforma de Cloud Computing	Echipamentele contractate vor fi livrate/recepționate, instalate în spațiile special amenajate, configurate (conectarea la rețeaua de alimentare cu energie electrică, configurarea infrastructurii de comunicații, conectarea dintre server-e și echipamentele de stocare etc.). Va fi instalat software-ul contractat (infrastructura de virtualizare, sistemele de operare, platforma SOA, platforma pentru Biblioteca virtuală etc.)
Testarea infrastructurii de Cloud Computing	Platforma de Cloud Computing va fi testată din punct de vedere funcţional, rezultatele testării urmând a fi consemnate pe baza unui proces verbal de acceptanţă. Această activitate se va focaliza pe procesul de identificare a posibilelor erori de program, erori care ar putea avea un impact negativ asupra desfăşurării activităţilor viitoare.
Implementarea serviciilor bazate pe platforma de Cloud Computing	Va fi configurată soluția de management al infrastructurii virtualizate, vor fi configurate serviciile de platformă, vor fi configurate interfețele cu sistemele externe
Implementarea serviciului „Date Deschise”	Va fi implementat serviciul „Date deschise”, destinat implementării unei platforme integrate de consolidare, standardizare și unificare a

	datelor de interes public generate și/sau gestionate de instituțiile publice
Implementarea serviciului „Biblioteca virtuală”	Va fi implementat serviciul „Biblioteca virtuală”, compus din: o arhivă electronică pentru stocarea documentelor în format digital, un model de date, interfețe programatice pentru schimbul de documente electronice, interfața utilizator a serviciului
Implementarea platformei de interoperabilitate	Platforma de interoperabilitate va demonstra caracterul SOA (Service Oriented Architecture) al platformei de cloud computing, asigurând mecanisme standardizate pentru schimbul de date, mesaje și comenzi între serviciile găzduite în platformă.
Migrarea serviciilor ICI pe platforma de Cloud Computing	Vor fi preluate în platforma Cloud o serie de servicii ICI care la momentul demarării proiectului sunt implementate pe o infrastructură veche, uzată moral și fizic.
Instruirea personalului care va administra Centru de Date și platforma de Cloud Computing	În funcţie de tipul şi caracteristicile utilizatorilor platformei de Cloud Computing, se vor desfăşura următoarele categorii de cursuri: 1. instruire administratori de servicii: vor beneficia de instruire 10 administratori de servicii de valoare adăugata în vederea dobândirii de competențe de utilizare a infrastructurii rezultate din proiect; durata instruirii va fi de 4 zile x 4 ore/zi; instruirea se va realiza la sediul ICI; 2. instruire administratori de sistem: vor fi instruiți 4 administratori de sistem. Va fi organizată o sesiune de instruire cu o durată de 4 zile x 5 ore/zi. Instruirea se va realiza la sediul ICI; Instruirea administratorilor va viza: utilizarea generală a platformei; administrarea nomenclatoarelor generale şi a celor specifice activităților operative ale solicitantului; administrarea modulului de securitate şi a drepturilor utilizatorilor; configurarea; administrarea serverului de aplicaţie; administrarea instrumentelor de back-up/recovery; administrarea instrumentelor de arhivare/ restore; analiza performanţelor sistemului şi tunning-ul sistemului prin intermediul statisticilor serverului de baze de date şi de aplicaţie şi prin schimbarea diverşilor parametri ai sistemului. Instruirea se va face în limba română, urmând a fi emise de către furnizorul de instruire certificate de participare pentru toţi cursanţii. Furnizorul serviciilor de instruire va pune la dispoziţia utilizatorilor o

	documentaţie de instruire care va include: • Manuale/ghiduri de utilizare în limba română, atât în format fizic (hârtie), cât şi în format electronic, pe categorii de utilizatori; • Manuale/ghiduri de administrare/configurare pentru persoanele care vor administra şi opera sistemul. Manualele vor fi disponibile atât în format fizic, cât şi electronic. Toate materialele de instruire vor purta însemnele distinctive de vizibilitate prezentate în Manualul de Identitate Vizuală al POSCCE.

4 DESCRIEREA GENERALĂ A SOLUȚIEI TEHNICE SOLICITATE

Proiectul ICIPRO are în vedere implementarea unei platforme de cloud computing care să permită beneficiarului ICI oferirea de Infrastructură ca Serviciu (IaaS – Infrastructure as a Service) către instituțiile publice din România. Prin serviciile puse la dispoziție de ICIPRO, instituțiile publice din România vor beneficia de infrastructură IT de un nivel înalt de performanță, securitate și disponibilitate, ceea ce creează premizele pentru o calitate sporită a serviciilor publice electronice destinate cetățenilor și mediului de afaceri. În plus, proiectul ICIPRO își

propune implementarea directă a unor servicii electronice de interes public: o biblioteca virtuală și un serviciu de prezentare integrată a datelor publice.

Imaginea de mai jos sintetizează soluția ICIPRO, precum și modul în care aceasta se raportează la principalii actori implicați în operarea și utilizarea acesteia.

Figura 1 - Vedere de ansamblu asupra soluției ICIPRO

Din perspectivă tehnică, soluția acoperă amenajarea unui centru de date, echiparea acestuia cu server-e, echipamente de stocare a datelor (inclusiv soluție de backup al datelor), infrastructură de comunicații, infrastructura de virtualizare, sistem de management al resurselor hardware și al resurselor virtualizate, precum și componente de infrastructură pentru aplicații. De asemenea, proiectul acoperă și migrarea unor servicii existente în cadrul ICI pe noua platformă, precum și dezvoltarea unor servicii noi, în contextul inițiativelor larg răspândite la nivel guvernamental privind integrarea și publicarea datelor de interes public, date generate/publicate de instituții publice.

Din punct de vedere conceptual soluția tehnică ICIPRO este ilustrată mai jos:

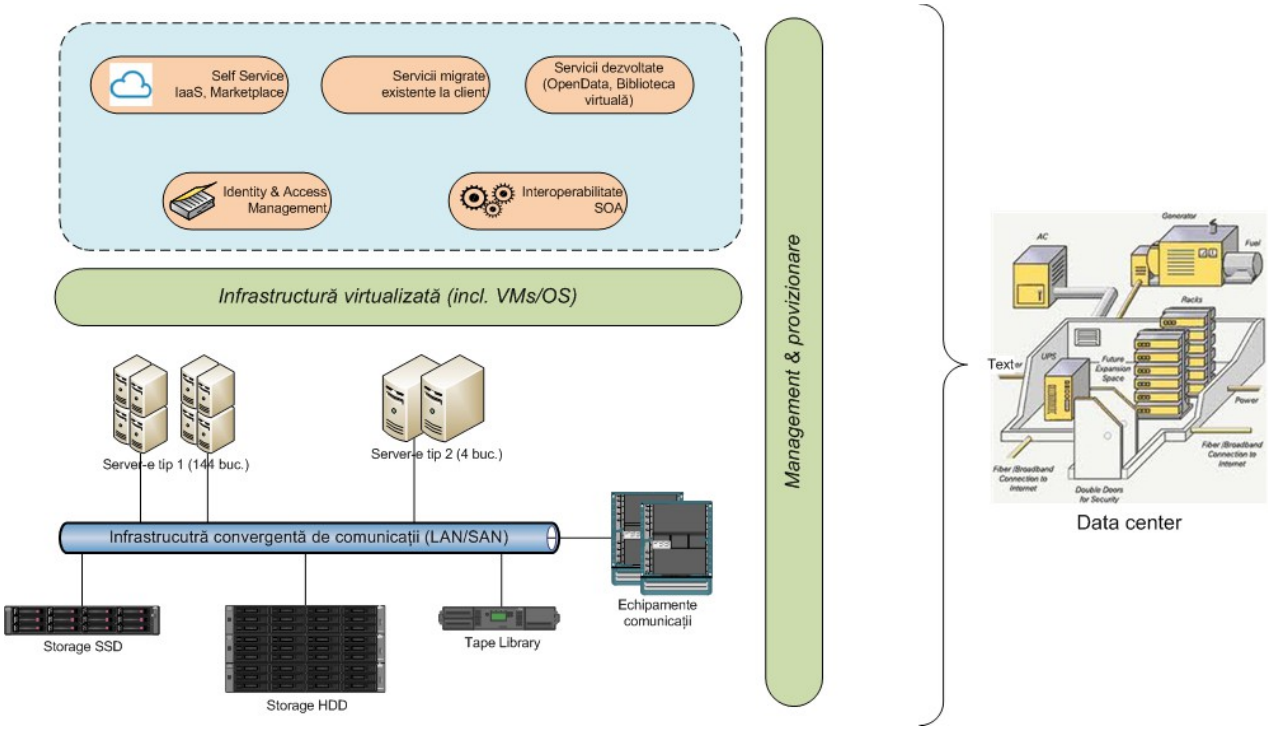


Figura 2 - Arhitectura generală a soluției

Infrastructura de tip cloud ce urmează a fi implementată trebuie să răspundă într-un mod optim necesităților de infrastructură de tip server ale instituțiilor publice din România. Platforma trebuie să ofere un grad mare de flexibilitate cu privire la resursele puse la dispoziție și la modalitatea prin care acestea sunt expuse beneficiarilor. Astfel, infrastructura trebuie să poată răspunde atât cerințelor reduse de putere de calcul (putere de procesare, memorie, spațiu de stocare date), cât și necesităților ridicate de resurse de calcul. Din acest motiv, luând în considerare limitările actuale ale tehnologiilor de virtualizare, soluția tehnică trebuie să asigure atât server-e modulare de capacitate relativ redusă, cât și server-e de mare capacitate. De asemenea, infrastructura trebuie să răspundă necesităților pentru spațiu de stocare cu performanțe ridicate (timp de răspuns, viteză de transfer), dar și necesităților de spațiu de stocare în cantități mari. Din acest motiv, soluția de stocare a datelor trebuie să asigure atât performanțe specifice discurilor de tip SSD, cât și capacitate specifică sistemelor bazate pe discuri clasice HDD.

Nu în ultimul rând, infrastructura de tip cloud ce va fi implementată în cadrul proiectului va trebui să ofere o interfață software de tip self-service pentru solicitarea/gestionarea resurselor

de calcul virtualizate. O astfel de interfață va permite beneficiarilor să solicite resurse virtualizate (de ex. mașini virtuale de tip server) și să gestioneze parametri ai acestor resurse.

Infrastructura de tip cloud implementată în cadrul proiectului trebuie să poată constitui o platformă solidă pentru servicii electronice guvernamentale, adresate atât instituțiilor publice cât și cetățenilor. Din acest motiv implementarea acestei infrastructuri reprezintă o foarte bună oportunitate pentru implementarea unei soluții de catalog al serviciilor electronice disponibile în regim SaaS (Software as a Service). Din acest motiv, soluția cerută prin acest caiet de sarcini trebuie să includă și o soluție de tip self-service pentru accesarea serviciilor electronice (aplicațiilor) în regim SaaS.

4.1 Descrierea componentelor sistemului

4.1.1 Infrastructura hardware

4.1.1.1 **Server-e și sisteme de stocare a datelor**

Platforma Cloud Computing necesită o infrastructură hardware dezvoltata pe principii de flexibilitate și eficienţă maximă. Aceste principii aplicate pentru platformă hardware înseamnă o nouă viziune asupra resurselor necesare, care nu mai sunt dedicate unui anumit proces în parte, ci sunt mai degrabă puse la dispoziţie în mod global. Îndeplinirea acestui deziderat se face prin împărţirea resurselor pe categorii, respectiv resurse de procesare, resurse de stocare și resurse de interconectare. Pentru implementarea fiecărei categorii se vor folosi tehnologii de ultima generaţie care să aibă următoarele caracteristici comune: platforma tehnologică deschisă, suport pentru virtualizare și management unitar.

Infrastructura hardware va fi găzduită în dulapuri metalice (rack-uri) standard cu lățimea de 19 țoli care oferă un spațiu de 42 unități standardizate de spațiu (42U). Vor fi instalate și configurate 4 rack-uri pentru server-e, în configurații identice.

4.1.1.1.1 Server-e de tip 1

Server-ele de tip 1 solicitate sunt destinate necesităților scăzute și moderate de putere de calcul. Server-ele de tip 1 vor fi optimizate pentru funcționarea în infrastructuri de tip cloud, cu o mare densitate a puterii de calcul. Este necesar ca aceste server-e să asigure o infrastructură modulară, cu un consum optimizat de energie și cu posibilitatea înlocuirii rapide și facile a oricărui server modular care suferă defecțiuni. În acest sens, aceste server-e vor fi găzduite în șasiuri metalice care vor dispune de surse redundante de alimentare cu energie cu un nivel ridicat de eficiență (vor respecta exigențele standardului 80 PLUS platinum), ce oferă posibilitatea înlocuirii fără întreruperea funcționării (hot-plug). Șasiurile metalice vor fi proiectate pentru a fi instalate în

dulapuri metalice (rack-uri), ocupând două unități de spațiu (2U), oferind posibilitatea de a găzdui până la 4 noduri de tip server.

4.1.1.1.2 Server-e de tip 2

Server-ele de tip 2 sunt destinate necesităților ridicate de putere de calcul, în soluții care necesită un nivel ridicat de încredere, disponibilitate și facilități avansate privind mentenanța și repararea (RAS – Reliability, Availability, Serviceability). Aceste server-e trebuie să permită adăugarea online de memorie și plăci I/O, să ofere PFA (Predictive Failure Analysis) pentru modulele de memorie ECC, precum și posibilitatea de de-alocare dinamică a nucleelor de procesare și înlocuirea acestora cu nuclee de procesare păstrate în rezervă.

Fiecare dintre cele 4 rack-uri destinate server-elor va găzdui câte un server de tip 2.

4.1.1.1.3 Resurse stocare date

Sunt necesare două tipuri de tehnologii de stocare a datelor: stocare a datelor pe hard-disk-uri clasice, pentru un volum mare de date și stocare a datelor pe discuri de tip SSD (Solid State Disk), pentru date care necesită viteză mare de accesare. Resursele de stocare vor fi asigurate de unul sau două sisteme de stocare centralizată tip SAN care să asigure un total de minim 4 controllere redundante.

4.1.1.1.4 Unitate de backup pe bandă

Unitatea de backup pe bandă va fi compusă din 4 unități de bandă LTO 6 și interfață FC. Necesarul de benzi este de 1024 (o bandă LTO6 = 2,5TB). În configurația furnizată, biblioteca de benzi trebuie să permită cel puțin 1100 benzi.

4.1.1.1.5 Stații de lucru pentru administrare

Stațiile de lucru pentru administrare sunt echipamente portabile de tip laptop ce vor asigura suportul tehnologic administratorilor ICI în vederea administrării sistemului ICIPRO. Aceste sisteme sunt descrise din punct de vedere al caracteristicilor tehnice în cadrul capitolului 5.

4.1.1.1.6 Echipamente multifuncționale de mare capacitate

Echipamentele multifuncționale de mare capacitate vor asigura necesarul prelucrării unei cantități mari de documente conform necesarului proiectului. Acestea vor putea scana și imprima rapid documente multiple într-un mod facil și flexibil, prin intermediul rețelei interne. Aceste echipamente sunt descrise din punct de vedere al caracteristicilor tehnice în cadrul capitolului 5.

4.1.1.2 **Sistem de comunicații**

Sistemul de comunicații trebuie să răspundă necesităților de performanță ale aplicațiilor moderne într-un mod eficient, atât din punct de vedere al numărului de echipamente, cât și al

cablurilor de conectare necesare. Din acest considerent autoritatea contractantă consideră că este necesară implementarea unei infrastructuri convergente de comunicații.

Rețeaua de date ce va fi implementată pentru centrul de date ICIPRO trebuie să asigure o lățime de bandă de 10Gbps pentru toate interfețele de rețea ale server-elor. Se va implementa o infrastructură de comunicații de tip converged network, care să permită utilizarea legăturilor de 10Gbps atât pentru traficul de date între server-e cât și legătura server-elor cu echipamentele de stocare a datelor prin tehnologie FCoE (Fiber Channel over Ethernet). Legăturile dintre echipamentele de comunicații și echipamentele de stocare a datelor se vor baza pe tehnologie FC (Fiber Channel).

4.1.2 Infrastructura software

Infrastructura software se bazează pe două componente majore: componenta de virtualizare a resurselor hardware (componenta de tip *hypervisor*) și sistemele de operare.

Componenta de virtualizare trebuie să constea dintr-o platformă de virtualizare dedicată, bazată pe Hypervisor propriu, fără dependență de un anume sistem de operare. Aceasta va fi instalată direct pe platforma hardware și va beneficia de suportul acestei platforme atât la nivelul capacității de procesare, cât și la nivelul opțiunilor de conectică și integrare cu restul elementelor de infrastructură.

Platforma de virtualizare trebuie să fie compatibilă cel puțin cu următorii producători hardware recunoscuți: IBM, Dell, HP, Fujitsu, Sun, Intel. De asemenea, hypervizorul pe care aceasta platformă se bazează trebuie să fie independent de producătorul sau de metoda de stocare internă/externă disponibilă în platforma de procesare și/sau stocare pe care rulează.

Platforma de virtualizare trebuie să permită folosirea următoarelor tipuri de sisteme de operare de tip server în mașinile virtuale:

- Microsoft Windows Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012, Microsoft Windows 2012 R2
- Linux: RHEL, Debian, SLES, Oracle, CentOS, Ubuntu, Open SUSE

Mașinile virtuale definite în platforma de virtualizare trebuie să poată beneficia concomitent de suportul a minim 32 procesoare virtuale, minim 256GB de RAM și acces la totalitatea porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile în infrastructura.

Componenta de virtualizare, împreună cu soluția de management și provizionare și cu sistemul de comunicații, trebuie să ofere un mecanism ce asigură că reţeaua și sistemele nu sunt compromise de calculatoare (mașinile virtuale) virusate, izolând și/sau depanând calculatoarele (mașinile virtuale) care nu se conformează politicilor de securitate stabilite.

Infrastructura software a soluției trebuie să includă sisteme de operare licențiate astfel încât să acopere toate resursele de calcul (procesoarele) din cadrul soluției, astfel încât utilizarea în regim IaaS a platformei implementate să nu implice costuri suplimentare ulterior finalizării proiectului de implementare. Sistemele de operare incluse în infrastructura hardware trebuie să permită o flexibilitate cât mai mare cu privire la aplicațiile care pot rula în cadrul lor, incluzând posibilitatea de a rula aplicații dezvoltate pe cele mai larg răspândite platforme de dezvoltare, respectiv platforma Java și platforma Microsoft .Net.

Pentru a asigura o eficiență cât mai mare în administrare, sistemele de operare de tip server trebuie să ofere o interfaţă unică pentru configurarea și monitorizarea serverului, cu programe de tip expert pentru optimizarea sarcinilor comune de administrare a serverului. De asemenea, sistemele de operare trebuie să permită mutarea elementelor interactive din faza configurării în faza ulterioară instalării, eliminând astfel necesitatea interacțiunii administratorului la instalarea sistemului de operare. Pentru a eficientiza operațiunile de rutină de administrare, sistemul de operare trebuie să ofere un instrument de tip shell cu linie de comandă și limbaj de script.

Din punct de vedere al conectivității, sistemele de operare trebuie să asigure suport deplin pentru protocolul IP în versiunile v4 (IPv4) și v6 (IPv6). În acest sens, sistemele de operare trebuie să ofere capabilități de NLB (Network Load Balancing) inclusiv pe IPv6, cu suport pentru mai multe adrese IP dedicate, ceea ce ar permite găzduirea mai multor aplicaţii în acelaşi cluster NLB.

În vederea sporirii nivelului de securitate în utilizarea resurselor hardware, sistemul de operare trebuie să permită instalări minimale, în care sunt instalate numai rolurile și caracteristicile de care este strict nevoie, minimizând nevoile de întreținere și reducând zonele de atac de pe server.

4.1.3 Managementul resurselor virtualizate

Sistemul de management al resurselor virtualizate trebuie să pună la dispoziție următoarele categorii de funcționalități:

- Provizionarea și managementul serviciilor IT în mediul virtualizat;
- Monitorizarea aplicațiilor (sisteme de operare, middleware, baze de date);

- Managementul configurațiilor mașinilor virtuale (de ex. managementul actualizărilor în sistemul de operare găzduit în mașina virtuală);
- Managementul sistemului de virtualizare;
- Optimizarea performanței și capacităților, prin intermediul instrumentelor analitice, panourilor de bord și al alertelor;
- Posibilitatea de crea și pune în aplicare planuri de recuperare (recovery plans), cu posibilitatea extinderii acestora prin scripturi.

4.2 Arhitectura funcţională

Arhitectura funcțională reprezintă structura funcționalităților soluției, precum și relațiile dintre modulele funcționale ale soluției și utilizatori, administratori și sistemele externe. Diagrama de mai jos sintetizează arhitectura funcțională a sistemului.

Figura 3 - Arhitectura funcțională ICIPRO

Așa cum se poate observa în această diagramă, platforma de virtualizare a resurselor hardware stă la baza funcționării platformei de tip Cloud. Această platformă va asigura abstractizarea resurselor hardware din perspectiva serviciilor, ceea ce duce la o flexibilitate și eficiență remarcabile în alocarea resurselor hardware către serviciile găzduite în platformă.

Serviciile publice implementate în cadrul proiectului și găzduite în platformă vor putea fi accesate de utilizatori prin intermediul unor interfețe utilizator de tip web. Instituțiile publice care aleg să-și migreze serviciile în platforma ICIPRO vor avea acces la o interfață dedicată operațiunilor de administrare a resurselor de calcul contractate. Această interfață le va permite administrarea infrastructurii alocate pentru aceste servicii. De asemenea, printr-o interfață specifică dedicată, instituțiile publice vor putea accesa/consulta un catalog de servicii electronice și vor putea contracta utilizarea acestora în regim SaaS (Software as a Service).

Platforma de interoperabilitate va servi necesităților de interoperabilitate atât în interiorul platformei, cât și necesităților de interoperare cu sisteme externe. Această platformă va facilita

integrarea între sisteme prin protocoale standard, deschise, larg adoptate în arhitecturile de tip SOA (Service Oriented Architecture).

Modulul de gestiune a utilizatorilor va gestiona atât datele de identificare ale acestora (nume cont, parolă de acces, alte date de identificare), cât și drepturile de acces ale acestora. Acest modul se va baza pe protocoale specifice deschise, cum ar fi LDAP (Lightweight Directory Access Protocol).

4.2.1 Componentele funcționale ale sistemului

4.2.1.1 **Serviciul Date Deschise**

Serviciul „Date deschise" este destinat implementării unei platforme integrate de consolidare, standardizare și unificare a datelor de interes public generate și/sau gestionate de instituțiile publice. Implementarea acestui serviciu va include proiectarea unui model standardizat de date și a unei interfețe programatice prin care instituțiile publice vor putea încărca date de interes public în acest serviciu pentru a putea fi expuse în mod uniformizat către public și mediul de afaceri.

Acest serviciu va suporta următoarele categorii de formate de date:

- Date relaționale (de ex. sub formă de tabel);
- Documente în format XML, HTML, PDF;
- Imagini în formate larg răspândite cum ar fi JPG, PNG, TIFF;
- Materiale video în formate larg utilizate cum ar fi MPEG4, DivX, xVid etc.;
- Date în formate specifice GIS (Geographic Information System);

Datele preluate în serviciul „Date deschise" vor fi publicate într-un portal web cu acces public, într-un mod standardizat, cu o interfață utilizator intuitivă, ergonomică.

4.2.1.2 **Serviciul Biblioteca Virtuală**

Acest serviciu este destinat instituțiilor publice care necesită o platformă de arhivare și publicare a documentelor electronice. Prin această platformă instituțiile publice (de ex. bibliotecile publice,

instituțiile de învățământ, instituțiile administrației publice) vor putea stoca documente de interes public în format electronic. Aceste documente vor fi publicate prin intermediul unui portal web cu acces public, prin intermediul căruia cetățenii și mediul de afaceri le vor putea consulta.

Arhiva electronică de documente implementată în cadrul acestui serviciu va asigura stocarea documentelor în condiții profesionale de securitate și siguranță, cu asigurarea drepturilor de administrarea la nivel de document pentru proprietarul documentului.

4.2.1.3 **Platforma de interoperabilitate**

Platforma de interoperabilitate trebuie să asigure mecanisme de interoperabilitate specifice SOA (Service Oriented Architecture). În acest sens, această platformă trebuie să includă un registru de servicii web, o platformă de tip Enterprise Service Bus și instrumente de monitorizare a schimburilor de mesaje.

Implementarea acestei platforme va presupune popularea registrului de servicii web cu serviciile web dezvoltate în cadrul proiectului și a altor servicii web preluate în platforma ICIPRO în cadrul proiectului. De asemenea, implementarea acestei platforme va trebui să demonstreze posibilitatea de integrare cu servicii electronice externe. În acest sens, va fi asigurată integrarea prin mecanisme specifice SOA cu Serviciul Electronic de Achiziții Publice (SEAP).

Implementarea integrării se va realiza din perspectiva ICI. Astfel, se va defini și se va realiza modelul de date și se va crea un serviciul web prin intermediul căruia administratorul SEAP va putea publica date de interes public.

Așa cum este menționat și în descrierea Serviciului Date Deschise, platforma va fi folosită exclusiv pe baza inițiativei instituțiilor publice din România care doresc să participe la platforma Date Deschise, folosind modelul de date și interfețele care vor fi realizate și puse la dispoziție în cadrul proiectului.

4.2.1.4 **Platforma pentru managementul utilizatorilor și a accesului la sistem**

Managementul utilizatorilor și al drepturilor de acces al acestora la sistem trebuie să fie asigurat și gestionat prin intermediul unui serviciu de tip director LDAPv3. Acest serviciu va fi folosit atât pentru gestiunea utilizatorilor interni ai ICI, cât și pentru gestiunea utilizatorilor serviciilor externe ICI găzduite în platforma Cloud.

Acest serviciu trebuie să ofere o interfață de tip self-service prin intermediul căreia utilizatorii își vor putea actualiza profilul de utilizator, incluzând posibilitatea de actualizare a parolei de autentificare.

Acest serviciu trebuie să permite autentificarea utilizatorilor atât cu credențiale de tip nume utilizator/parolă, cât și prin certificate digitale sau autentificare biometrică.

4.2.1.5 **Interfața de administrare a serviciilor**

Interfața de administrare a serviciilor puse la dispoziție de ICIPRO trebuie să pună la dispoziție instrumente grafice pentru provizionarea serviciilor de infrastructură ale centrului de date virtual. De asemenea, printr-o interfață grafică utilizator de tip self-service instituțiile publice trebuie să poată consulta și contracta servicii electronice implementate pe baza platformei IaaS - ICIPRO, într-un mod standardizat.

Unealta de provizionare dedicată infrastructurii IaaS trebuie să aibă capabilități de tip multitenant și să conțină un portal pentru administratori, un portal pentru utilizatori (tenants), să ofere capabilități de provizionare de servicii de cloud web cu suport pentru un framework web (precum ASP.NET, PHP) și cel puțin o platformă bazată pe evenimente și I/O non-blocante pentru construirea de aplicații distribuite, mașini virtuale Windows și Linux, baze de date de tip SQL și să ofere automatizare prin rularea de taskuri și integrare cu soluția de automatizare de procese de administrare propusă.

Instrumentul de administrare a serviciilor electronice găzduite pe platforma ICIPRO va pune la dispoziție o interfață de tip portal web cu capabilități de tip self-service. Această interfață trebuie să permită personalizarea portalului de self-service și construirea unei interfețe prietenoase cu utilizatorul și prezentarea automată a funcționalităților disponibile acestuia în funcție de profilului său.

Accesul utilizatorilor la funcționalitățile de tip self-service trebuie să se poată face exclusiv într-un mod controlat, fie direct prin intermediul modulului de acces din soluție, fie indirect folosind o platformă externă pentru controlul accesului (de ex. un alt portal).

Soluția trebuie să pună la dispoziție un mecanism de tip SSO (Single Sign-On) pentru portalul de tip self-service, precum și o funcționalitate de tip SSO Proxy prin care utilizatorul să poată accesa un serviciu extern la care are acces folosind mecanismul de SSO din portalul de self-service. Modulul dedicat SSO trebuie să suporte protocoale deschise de tip SOAP/XML (servicii web) și SAML pentru a facilita integrarea cu sisteme externe.

Interfața de administrare a serviciilor electronice (aplicațiilor) găzduite pe platforma ICIPRO trebuie să permită adaptarea design-ului grafic al portalului de tip self-service pentru a implementa cerințe de imagine specifice clientului.

Interfața de administrare a serviciilor electronice (aplicațiilor) găzduite în platforma ICIPRO trebuie să asigure suport multi-limbă. Utilizatorul trebuie să poată selecta limba în cadrul portalului de tip self-service.

Soluția de administrare a serviciilor trebuie să pună la dispoziția utilizatorilor funcționalități de achiziție a serviciilor (consultarea unui catalog de servicii, alegerea serviciilor dorite, configurarea acestora pentru a putea fi utilizate). În cadrul acestor funcționalități trebuie să se poată defini grupuri (pachete) de servicii care vor putea fi de asemenea făcute disponibile pentru achiziționare.

În vederea asigurării posibilității de auditare a activităților efectuate în cadrul portalului de tip self-service, acesta va trebui să înregistreze (să jurnalizeze) aceste activități, cu posibilitatea ulterioară de raportare pentru trasabilitatea activității în cadrul portalului și pentru obținerea de date statistice legate de activitatea utilizatorilor. Rapoartele predefinite trebuie să includă minim următoarele tipuri de rapoarte:

- Raport pe aplicații/servicii
- Raport pe utilizatori
- Raport pe achiziții
- Raport de activitate în platformă
- Statistici web.

Modulul de raportare trebuie să permită adaptarea rapoartelor pre-definite și definirea unor noi rapoarte.

Această platformă trebuie să pună la dispoziția utilizatorilor un modul de ajutor online pe mai multe canale: manuale/ghiduri de utilizare, întrebări frecvente și răspunsurile aferente.

Platforma de administrare a serviciilor/aplicațiilor trebuie să ofere mecanisme standardizate, automatizate pentru integrarea de noi servicii/aplicații în platformă. Pentru integrarea de noi

servicii platforma trebuie să pună la dispoziție documentație tehnică, incluzând set de întrebări frecvente și răspunsuri, exemple de cod sursă pentru integrare în diverse limbaje de programare (de ex. Java, Microsoft .Net, etc.).

Platforma trebuie să pună la dispoziție o interfață de tip API (Application Programming Interface) pentru gestionarea utilizatorilor, a catalogului de produse, a modulului de achiziționare, precum și pentru integrarea cu noi furnizori de servicii și rapoarte.

4.3 Arhitectura tehnică

Arhitectura tehnică concepută pentru soluția ICIPRO este sintetizată în diagrama de mai jos.

Figura 4 - Arhitectura tehnică

Pornind de la faptul că soluția se bazează pe două tipuri de server-e, soluția tehnică va pune la dispoziția utilizatorilor două seturi de resurse virtualizate. În grupul de resurse virtualizate denumit „IaaS tip 1" în diagrama de mai sus vor fi definite în cadrul proiectului server-e virtuale pentru:

- Platforma SOA – care va asigura capabilitățile de interoperabilitate între serviciile instalate pe platforma ICIPRO, precum și interoperabilitatea cu sisteme externe, interoperabilitate bazată pe standarde deschise larg utilizate în arhitecturi de tip SOA (servicii web)
- Platforma IAM – care va asigura gestiunea identității utilizatorilor și a drepturilor de acces ale acestora, precum și servicii de autentificare unică (SSO – Single Sign On)
- Serviciul Date Deschise implementat în cadrul proiectului
- Serviciul Biblioteca virtuală implementat în cadrul proiectului
- Serviciile ICI migrate pe această platformă
- Componenta de management al serviciilor electronice găzduite pe platforma ICIPRO

Grupul de resurse virtualizate denumit „IaaS tip 2" în diagrama de mai sus este destinat serviciilor care necesită o putere sporită de calcul (număr mare de procesoare, capacitate mare de memorie).

Pe lângă resursele virtualizate care constituie platforma IaaS care face obiectul principal al acestei soluții, există o serie de componente cum ar fi:

- server-ele de baze de date necesare sistemului de management și provizionare , platformei SOA și sistemului de gestiune a identității și accesului utilizatorilor (IAM – Identity and Access Management); aceste server-e nu vor fi virtualizate
- Server-ele de servicii de tip director; aceste server-e nu vor fi virtualizate
- Server-ele necesare sistemului de management și provizionare

Trebuie observat faptul că pentru a spori performanța infrastructurii de comunicații destinate platformei și serviciilor ICIPRO, autoritatea contractantă consideră necesară implementarea unei rețele separate dedicate managementului sistemului.

4.3.1 Sistemul de management și provizionare

Sistemul de management și provizionare include componente care necesită rularea direct pe server-e fizice și componente care rulează în bune condiții pe mașini virtuale. Din această cauză, arhitectura sistemului de management și provizionare grupează aceste componente în două grupuri, așa cum este prezentat în diagrama de mai jos.

Figura 5 - Arhitectura sistemului de management și provizionare

Componentele care sunt planificate a rula pe server-e fizice au necesități sporite de performanță I/O sau sunt necesare bunei funcționări a platformei de virtualizare.

Este notabil faptul că în dorința de a furniza servicii certificate digital (servicii incluse în cadrul acestui proiect și/sau servicii ce urmează a fi implementate pe acest sistem), autoritatea contractantă solicită implementarea unei autorități de certificare digitală, cu o autoritate de certificare rădăcină (Root CA) care va rămâne offline imediat după inițializarea infrastructurii de chei publice și cu o structură de înaltă disponibilitate a sub-autorității de certificare, structură care va pune la dispoziție și informații legate de starea certificatelor, fie prin mecanisme de tip CRL fie prin protocol OCSP.

Subsistemul de management al configurațiilor software este responsabil pentru gestionarea catalogului de aplicații existent în cadrul platformei și pentru instalarea/actualizarea acestora pe server-e.

Componenta de management al serviciilor va permite administratorilor platformei ICIPRO o gestiune riguroasă a activităților de administrare și a incidentelor înregistrate în cadrul sistemului.

Componenta de management al backup-ului va fi responsabilă pentru implementarea politicii de backup și restaurare la nivelul platformei ICIPRO.

Server-ele DHCP vor genera și furniza adrese IP (prin protocolul DHCP) în cadrul platformei.

Componenta de monitorizare va fi configurată pentru a monitoriza disponibilitatea și performanța platformei ICIPRO, punând la dispoziție mecanisme de alarmare a administratorilor în cazul constatării unor incidente sau a unor abateri de la parametrii normali de funcționare ai platformei.

Componenta de provizionare și management al infrastructurii virtualizate va permite atât definirea/gestionarea manuală cât și automată a mașinilor virtuale și a parametrilor acestora.

4.3.2 Arhitectura sistemului de comunicații

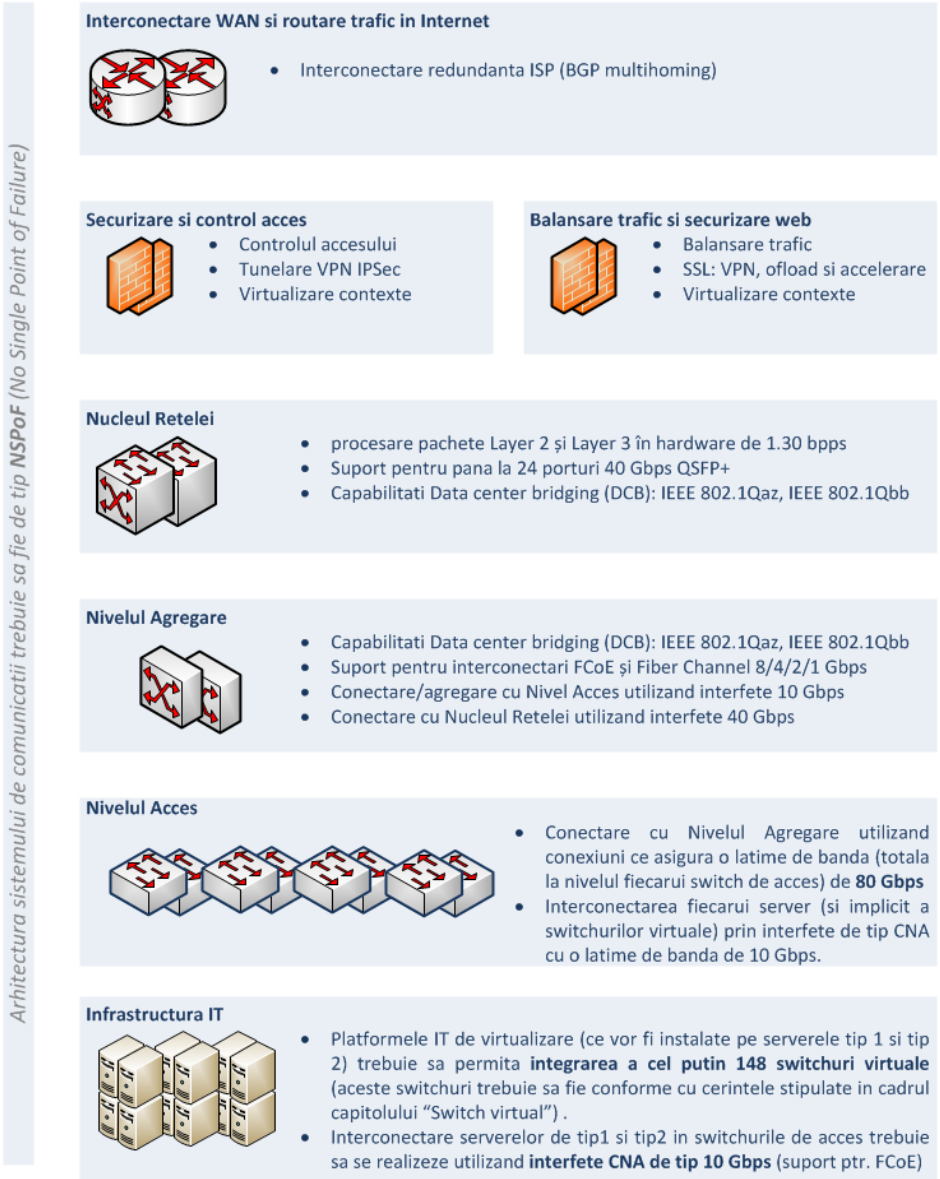
Structura infrastructurii de comunicații trebuie să fie una larg adoptată în implementarea de infrastructuri de comunicații pentru centrele de date. În diagrama de mai jos este sintetizată infrastructura de comunicații necesară funcționării în condiții optime a platformei de Cloud Computing. Infrastructura de comunicații necesară funcționării în condiții optime a platformei de Cloud Computing va fi realizata pe trei nivele: nucleul rețelei (core layer), nivelul de agregare (aggregation layer) și nivelul de acces (access layer).

Nucleul rețelei (core layer) trebuie sa conțină două echipamente de tip switch cu funcționalități de L2 și L3 ce vor asigura transmiterea traficului in cadrul centrului de date la viteze foarte mari. Cele două echipamente vor fi conectate în arhitectură redundantă pentru a asigura un grad înalt de disponibilitate.

Nivelul de agregare (aggregation layer) va fi compus din 2 echipamente de tip switch cu capabilități de tip converged network (care să permită utilizarea legăturilor de 10Gbps atât pentru traficul de date cât și pentru traficul de FCoE). Echipamente vor fi conectate în arhitectură redundantă pentru a asigura un grad înalt de disponibilitate.

Nivelul de acces (access layer) va fi compus din 12 echipamentele de tip switch, ce asigură conectarea serverelor la infrastructura de comunicații prin intermediul interfețelor de tip converged network (care să permită utilizarea legăturilor de 10Gbps atât pentru traficul de date între servere cât și legătura serverelor cu echipamentele de stocare a datelor prin tehnologie FC).

Pe lângă cele trei nivele se vor oferta și echipamente care să asigure accesul la o rețea de tip WAN/Internet și echipamente de securitate, monitorizare și management.



Soluția trebuie să includă toate cabinetele de comunicații și accesoriile necesare pentru amplasa corect toate echipamentele de rețea în camera serverelor.

5 CERINȚE FUNCȚIONALE ȘI NON-FUNCȚIONALE

Soluția ofertată trebuie să îndeplinească următoarele cerințe generale:

- Soluția ofertată pentru implementarea Centrului de date trebuie să fie integrată, beneficiind de soluții tehnice avansate, modulare și scalabile, construite pe baza unor standarde deschise, de actualitate.
- Toate echipamentele infrastructurii de suport vor fi din categoria soluțiilor pentru centre de date și vor fi din clasa de eficiență energetică **ridicată**.
- Toate echipamentele furnizate trebuie să respecte cerințele tehnice specificate în capitolul "Cerințe tehnice pentru sistemele de suport ale Centrului de date" și să poată fi monitorizate din aplicația de management centralizat.
- Soluţia pentru Centrul de date trebuie să includă toate componentele hardware și software necesare realizării unei soluţii integrate și funcţionale incluzând cel puţin, dar fără a se limita la: rack-uri și accesorii de management fluxuri de aer, sistem de protecţie a alimentării cu energie electrică (UPS) și distribuție electrică integrată, sistem de răcire, sistem de monitorizare a mediului (temperatură, umiditate, scurgeri de lichide), sistem de administrare, operare și management.
- Soluția ofertată trebuie să permită adăugarea ulterioară de noi module de infrastructură de suport fără a fi nevoie de reproiectarea în totalitate a soluției.
- Pentru soluția de Centru de date se vor utiliza standarde deschise, neproprietare pentru a permite interconectarea viitoare facilă cu alte sisteme și pentru a permite adăugarea ulterioară de noi facilități infrastructurii de suport.

5.1 Cerinţe funcţionale ale sistemului

În cadrul acestei secțiuni sunt prezentate funcționalitățile detaliate ale sistemului, atât din punct de vedere al platformei hardware a sistemului, cât și al componentelor software necesare pentru atingerea obiectivelor proiectului.

5.1.1 Serviciul Date Deschise

Inițiativa implementării unui serviciu de tip „Date Deschise” a apărut din dorința de aliniere a nivelului de transparență și responsabilitate ale instituțiilor publice din România cu practicile existente la nivelul Uniunii Europene. Astfel, pornind de la constatarea existenței European Union Open Data Portal (www.open-data.europa.eu), în cadrul acestui proiect se dorește implementarea unui instrument similar de prezentare integrată prin intermediul unui portal web a datelor de interes public generate de instituțiile publice din România. Astfel de date vor putea fi utilizate fără restricții în scopul activităților de informare și cercetare necomerciale.

Pentru buna funcționare a acestui portal este necesară proiectarea, implementarea și publicarea unui model de date și a unei interfețe programabile publice prin care instituțiile publice vor putea publica date de interes public în acest portal. De asemenea, este necesară proiectarea, implementarea și publicarea unei interfețe (a unui protocol) prin care acest portal va putea consuma date publicate de instituțiile publice. Aceste interfețe/protocoalele vor trebui să asigure autenticitatea informațiilor preluate în portal, astfel încât utilizatorii portalului să poată identifica sursa acestor informații, precum și momentul în care acestea au fost preluate în portal.

Implementarea acestui serviciu se rezumă la proiectarea, construirea și punerea în funcțiune a serviciului. Acest portal va fi populat exclusiv pe baza inițiativei instituțiilor publice din România care doresc să participe la platforma Date Deschise, folosind modelul de date și interfețele care vor fi realizate puse la dispoziție în cadrul proiectului.

Portalul Date Deschise va afișa pentru fiecare articol sau set de date publice numărul de vizualizări înregistrat.

Portalul va oferi utilizatorilor capabilități avansate de căutare în text, cu posibilitatea căutării după diferite criterii: oricare dintre cuvintele introduse, toate cuvintele introduse, toate cuvintele introduse în secvența dată. Funcția de căutare în portal va oferi posibilitatea ordonării rezultatelor după relevanță, numărul de vizualizări, alfabetic (crescător și descrescător), data ultimei modificări aduse articolelor/seturilor de date.

Acest serviciu va suporta următoarele categorii de formate de date:

- Date relaționale (de ex. sub formă de tabel)
- Documente în format XML, HTML, PDF
- Imagini în formate larg răspândite cum ar fi JPG, PNG, TIFF
- Materiale video în formate larg utilizate cum ar fi MPEG4, DivX, xVid etc.
- Date în formate specifice GIS (Geographic Information System)

Pentru fiecare set de date publicat în portal, vor fi puse la dispoziția utilizatorilor portalului metadate care să descrie setul de date: Scurtă descriere, sursa (instituția care a generat setul de date), Starea setului de date (de ex. variantă în lucru, variantă completă), tipul setului de date (de ex. Statistic, Inițiativă legislativă, hartă etc.), note ale autorilor, date de contact ale autorilor.

Fiecare articol/set de date va putea fi publicat în multiple formate, portalul urmând să permită utilizatorului alegerea formatului în care dorește să vizualizeze/descarce articolul sau setul de date.

Pentru a facilita navigarea în conținutul portalului, platforma portalului trebuie să permită organizarea articolelor/seturilor de date în structuri ierarhice, fie după data publicării, fie după instituția care publică articolul/setul de date, fie după domeniul (tipul) articolul/setului de date.

Portalul va pune la dispoziția utilizatorilor un modul în care aceștia să poată formula o solicitare pentru un articol sau un set de date. Acest modul va facilita interacțiunea dintre utilizatorul solicitant și instituția nominalizată pentru a satisface solicitarea.

Portalul va expune o secțiune interactivă în care va publica un top al instituțiilor autoare de articole/seturi de date publicate în portal. Această secțiune va permite utilizatorilor navigarea în conținutul portalului prin click pe numele instituției autoare (care va conduce la o pagină din care pot fi consultate toate articolele/seturile de date publicate de instituția respectivă).

Portalul va expune o secțiune de tip tag cloud care va prezenta cuvintele cel mai des întâlnite în articolele, cu dimensiuni corelate cu numărul de apariții ale cuvintelor respective (cuvintele cu o frecvență mai mare vor fi afișate cu litere de dimensiune mai mare). Prin această secțiune utilizatorii vor putea efectua căutări în conținutul portalului după cuvântul indicat prin click.

5.1.2 Serviciul Biblioteca Virtuală

Serviciul Biblioteca Virtuală este un serviciu destinat instituțiilor publice care necesită o platformă de gestiune a conținutului ce va permite arhivarea și publicarea documentelor electronice. Documentele publicate prin acest serviciu vor putea fi accesate prin intermediul unei interfețe web.

Pentru fiecare instituție care alege să folosească acest serviciu, vor fi disponibile două secțiuni: una cu acces liber, deschisă publicului larg, și una cu acces restricționat disponibilă doar instituției respective. Astfel, în acest serviciu vor putea fi încărcate atât documente de interes public cât și documente de uz intern ale instituțiilor (de ex. Regulamentul de Ordine Interioară). Pentru secțiunea de uz intern, sistemul trebuie să asigure un acces controlat al utilizatorilor la diferitele sub-secțiuni, pe bază de autentificare a utilizatorilor și acces în conformitate cu profilul de utilizator.

Arhiva electronică de documente implementată în cadrul acestui serviciu va asigura stocarea documentelor în condiții profesionale de securitate și siguranță, cu asigurarea drepturilor de administrarea la nivel de document pentru proprietarul documentului.

Pentru a veni în întâmpinarea instituțiilor care nu dispun de resursele necesare pentru gestionarea unor arhive electronice de dimensiuni și complexitate reduse, serviciile de încărcare în arhiva electronică a documentelor vor fi efectuate de personal desemnat de autoritatea contractantă. În acest sens, platforma software pentru arhiva electronică trebuie să fie licențiată pentru un număr minim de 20 utilizatori cu drepturi de a contribui cu conținut la arhiva electronică.

Pentru instituțiile care necesită gestionarea unor arhive electronice de dimensiuni și/sau complexitate sporite, activitățile de gestiune a secțiunilor de arhivă electronică dedicate acestor instituții platforma software trebuie să asigure un număr minim de 80 licențe utilizator. Aceste licențe utilizator vor fi utilizate direct de angajați ai acestor instituții.

Platforma trebuie să nu impună constrângeri privind numărul de utilizatori care accesează în mod exclusiv citire conținutul arhivei (arhivelor) electronice.

Această platformă trebuie să permită accesarea conținutului atât printr-o interfață web, cât și prin aplicații client dedicate dispozitivelor mobile inteligente (de tip tabletă sau smartphone). De asemenea, pentru activitățile de gestiune a arhivei, platforma trebuie să pună la dispoziție și un client desktop.

Interfața web pusă la dispoziție de acest serviciu trebuie să fie aliniată la standarde și tehnologii moderne, larg acceptate în industrie, cum ar fi: HTML, XHTML, XML, JSR 168, SOAP, WSDL. De asemenea, pentru autentificarea utilizatorilor și controlul accesului acestora la conținutul arhivei, platforma de management al conținutului electronic trebuie să suporte protocoale deschise de tip LDAP. Interfața trebuie sa se afișeze in funcție de drepturile de acces și rolurile asociate utilizatorilor.

Pentru preluarea documentelor în arhivă, platforma de gestiune a conținutului trebuie să includă un motor de derulare a fluxurilor de lucru, completat de o interfață web de proiectare/definire a fluxurilor de lucru. Pentru fluxurile de lucru definite trebuie să se poată crea formulare care să poată fi completate de-a lungul activităților care sunt îndeplinite de participanții la flux. Aceste formulare trebuie să poată fi create utilizând un designer grafic web based, integrat în soluție. Componenta de gestiune și derulare a fluxurilor de lucru trebuie să se poată integra cu sisteme de notificare de tip email.

Platforma de gestiune a conținutului trebuie să permită înregistrarea documentelor împreună cu un set de atribute (metadate) care să faciliteze organizarea documentelor și regăsirea lor ulterioară. Platforma trebuie să pună la dispoziția utilizatorilor instrumente moderne de căutare a documentelor, atât după setul de atribute al acestora, cât și prin identificarea în conținutul documentelor de text care satisface criteriile de căutare. De asemenea, motorul de căutare inclus în platformă trebuie să ofere informații legate logic de cererea de căutare. Sistemul trebuie să ofere posibilitatea de a reutiliza indecșii de căutare, de a filtra rezultatele căutărilor dacă setul de documente rezultat este prea mare, precum și de a sorta rezultatele căutărilor. Criteriile de căutare trebuie sa poată fi după metadate, comentarii, versiune, adnotări și conținut. De asemenea trebuie sa permită păstrarea de profile de căutare și definirea de căutări personalizate precum și sa aibă facilitați de rafinare a rezultatelor afișate. Rezultatele căutărilor sa poată fi vizualizate sub forma de lista sau sub forma arborescenta.

Sistemul trebuie să permită gestionarea documentelor în diferite versiuni de conținut sau metadate.

Sistemul trebuie să pună la dispoziția utilizatorilor funcționalități care să permită vizualizarea documentelor precum și a atributelor acestora, incluzând informații legate de versiunile înregistrate. De asemenea, sistemul va pune la dispoziție facilitatea de realizare de preview al unui document prin transformarea documentului în format TIFF sau PDF spre exemplu.

Pe lângă interfețele utilizator, platforma trebuie să pună la dispoziție și interfețe programate de tip WebDAV pentru accesarea arhivei. De asemenea, sistemul trebuie să ofere un client integrat în Windows Explorer. Utilizatorii trebuie să pot lucra cu depozitul de documente direct din mediul sistemului de operare. Acesta trebuie să ofere funcționalități de check-in și check-out documente, versionare și editarea informațiilor de indexare. Documentele și directoarele trebuie să poată fi șterse, copiate și mutate.

Sistemul trebuie să poată fi integrat cu suitele de tip office răspândite Microsoft Office și Open Office.

Sistemul trebuie să ofere facilități de management de înregistrări (Records Management) conform ISO15489 și Moreq2. Aceste funcționalități trebuie să fie accesibile din interfața de bază și nu dintr-o interfață separată.

Structura de documente trebuie să poată fi organizată arborescent și să permită definirea de noi niveluri în cadrul arhivei electronice.

Sistemul trebuie să permită adăugarea de adnotări de tip imagine (stamp) la un document (de exemplu pentru marcare ca draft a unui document). Aceste adnotări trebuie să poată fi publice (vizibile tuturor), sau private.

Platforma trebuie să ofere suport pentru importul în aplicaţie a unui fişier sau a mai multor fişiere prin folosirea de metode de tip drag and drop.

Sistemul de gestiune a conținutului trebuie să fie independent de platforma sistemului de operare, putând rula atât pe Windows, cât și pe Linux sau Unix.

Sistemul trebuie să pună la dispoziție un mecanism de Audit, care să furnizeze rapoarte la nivel general și individual. Sistemul trebuie să ofere funcţionalităţi native de semnătura digitală, criptarea documentelor pe 128 biţi și utilizarea de chei de criptare;

Sistemul trebuie să ofere facilități de recunoaștere automată de tip OCR (Optical Character Recognition), BCR (Bar Code Recognition).

5.1.3 Platforma de interoperabilitate

Platforma de interoperabilitate trebuie să fie o soluție de middleware și integrare (procese, reguli de operare, tranzacții și date) ce trebuie sa ofere capabilități de gestionare a proceselor și operaționalizare a activităților, conducând spre dezvoltarea unei arhitecturi de tip SOA (Service Oriented Architecture) și realizarea unei infrastructuri de:

- Interconectare a aplicațiilor existente în cadrul organizațiilor – EAI (Enterprise Application Integration)
- Interconectare a aplicațiilor din organizații diferite, partenere – integrare de tip Business-to-Business (B2B)
- Definire și administrare a proceselor și regulilor de business – BPM (Business Process Management)

Soluția trebuie sa ofere minim următoarele funcționalități:

- Trebuie sa ofere posibilitatea de comunicare cu aplicații externe, prin intermediul adaptoarelor;
- Adaptoarele trebuie sa gestioneze protocoale proprietare și sa suporte conversia la și de la diverse formate de date.
- Sistemul trebuie sa includă adaptoare cel puțin pentru: aplicații de tip ERP, baze de date Oracle prin JDBC/ODBC, SQL Server, Websphere/Weblogic, FILE, HTTP, XML, SMTP, POP3, SOAP, Oracle AQ/ MSMQ/ Websphere MQ;
- Mesajele trebuie primite și trimise prin interfețe de tip inbound și outbound. Interfețele trebuie sa ofere capabilități sigure, scalabile de parsare și manipulare a mesajelor precum: codare și decodare, scheme de validare a mesajelor, grupare și dezasamblare a mesajelor, capabilități de tipul single-sign-on, criptare și decriptare, semnare și validarea semnăturii;
- Compunerea serviciilor și orchestrarea lor trebuie sa poată fi realizata în mod declarativ (folosind instrumente și forme vizuale), în vederea implementării automate a proceselor de business și a fluxurilor din sistem;
- Soluția trebuie sa dispună de un motor de orchestrare, iar acesta trebuie să simplifice implementarea modelelor standard de integrare, cum ar fi rutarea dinamica a mesajelor și agregarea serviciilor;
- Motorul de orchestrare trebuie sa ofere suport pentru rularea proceselor de business de lungă durată, prin funcționalități native de asigurare a persistenței și management al stărilor sistemului, precum și prin corelarea răspunsurilor asincrone la mesaje;

- Soluția trebuie să ofere capabilități de management și rutare configurabilă de documente;
- Soluția trebuie să ofere posibilitatea de integrare a unui set de aplicații eterogene
- Soluția trebuie să ofere opțiuni complexe de integrare între diverse organizații partenere folosind un set de standarde larg acceptate;
- Soluția trebuie să ofere posibilitatea definirii și modificării regulilor de business direct de către analiștii de sistem, fără intervenția specialiștilor IT / dezvoltatorilor;
- Soluția trebuie să ofere posibilitatea administrării proceselor de business, reutilizării de cod, modularitate, facilități de dezvoltare rapidă;
- Soluția trebuie să permită versionarea și monitorizarea implementării regulilor de business;
- Soluția trebuie să ofere un modul dedicat pentru monitorizarea activității, proceselor și regulilor de sistem, care să ofere vizibilitate asupra corectitudinii și integrității acestora;
- Modulul de monitorizare a activității trebuie să poată fi folosit cu ușurință de utilizatori, fără a fi necesară dezvoltarea de cod, folosind inclusiv instrumente de tip Office și instrumente de tip Business Intelligence;
- Soluția trebuie să ofere posibilitatea expunerii rezultatelor monitorizării pe site-uri Web de tip portal, în aplicații de tip Office și rapoarte;
- Soluția trebuie să ofere capabilități de administrare a aplicațiilor, a adaptoarelor, de urmărire a mesajelor, a proceselor și a serviciilor în medii distribuite, având facilități de scalabilitate, de înaltă disponibilitate și de balansare a resurselor hardware.

5.1.4 Platforma pentru managementul utilizatorilor și a accesului la sistem

Platforma pentru managementul utilizatorilor și a accesului la sistem trebuie să fie un modul integrat de management al identităților și al drepturilor de acces, care trebuie să ofere minim următoarele funcționalități:

- Sincronizarea identităților, managementul certificatelor și parolelor precum și provizionarea utilizatorilor într-o singură soluție care se integrează cu infrastructuri eterogene;

- Managementul integrat al identității și integrare nativa cu LDAP (Active Directory sau ONE LDAP, sisteme de mesagerie (Exchange sau IBM Lotus), sisteme de tip ERP;
- Posibilitatea extinderii funcționalităților cu autorități de certificare de la același producător cu integrare nativă și fără dezvoltări ulterioare;
- Să permită folosirea dispozitivelor de tip smartcard sau token și folosirea lor împreună cu certificatele digitale pentru autentificare sigură;
- Să ofere posibilitatea modificării grupurilor și listelor de distribuție, atât static cât și în mod dinamic, direct din soluția de management al identităților (grupuri, liste de distribuție și grupuri de securitate);
- Să ofere capabilități de tip "self-service" pentru utilizatori pentru managementul identităților, cât și pentru managementul grupurilor sau listelor de distribuție din care face parte și care să fie oferite într-un portal web;
- Să asigure integrarea provizionării identităților, credențialelor și resurselor bazată pe fluxuri;
- Să ofere o abordare integrată pentru gestionarea credențialelor de autentificare complexe (certificate digitale, smart cards), pentru provizionarea și sincronizarea conturilor de utilizator în cadrul mai multor sisteme și platforme eterogene (de ex. crearea automată a căsuțelor de e-mail), să ofere utilitare de tip „self-help", permițând administratorilor delegarea de activități către utilizatorii finali (de ex. funcționalități de resetare a parolelor), să prevină problemele generate în urma părăsirii organizației de către un utilizator (conturi orfane), să ofere un cadru pentru implementarea de politici de control și urmărire a identităților și datelor de acces, să permită auditarea și obținerea de rapoarte;
- Să asigure funcționalități de tip „single-sign-on" pe portalul web folosit pentru administrarea identității (Web-based SSO) care să autentifice utilizatorii, în cadrul aceleiași sesiuni de browser web, pe mai multe aplicații, permițând accesul acestora fără a li se cere credențiale în cadrul fiecărei aplicații distincte, indiferent de platformele pe care rulează aceste aplicații. Această funcționalitate trebuie să permită colaborarea B2B (business-to-business) cu partenerii agreați, permițând fiecărei organizații client să folosească propriile conturi locale pentru autentificare și acces.

- Să ofere servicii personalizabile pentru crearea și gestiunea certificatelor digitale folosite în sistemele de securitate software, să permită asocierea identității unei persoane, dispozitiv sau serviciu cu o cheie privată, să ofere funcționalități pentru gestionarea înrolării sau revocării certificatelor, să permită delegarea înrolării pe bază de template-uri de certificate.
- Să permită dezvoltarea unor reguli de business. Sistemul trebuie să se integreze nativ cu soluția de tip director ofertată;
- Să ofere funcționalități de audit și raportare;
- Să ofere Role Based Access Control și sa ofere maparea și organizarea rolurilor conform ierarhiei organizației;

Soluția ofertată și livrată trebuie să includă conectori pentru interconectarea cu cel puțin următoarele sisteme:

- sisteme de operare și servicii de director: Microsoft Active Directory; Windows Azure Active Directory; IBM Tivoli Directory Server; Novell eDirectory; Sun Directory Server (Netscape/iPlanet/SunONE); LDAP Data Interchange Format (LDIF); LDAP v3;
- aplicații: XML-based systems; DSML-based systems;
- baze de date: Microsoft SQL Server; IBM DB2; Oracle;
- sisteme bazate pe fișiere formatate.

5.2 Cerinţe privind soluţia hardware

Rolul funcţional al componentelor de infrastructură ale soluţiei a fost prezentat în cadrul capitolului 4 al acestui document. În cadrul acestei secţiuni vor fi prezentate caracteristicile tehnice ale componentelor de infrastructură hardware ale sistemului.

5.2.1 Cerințe generale

Toate cerințele tehnice sunt minimale și obligatorii.

Toate echipamentele ofertate trebuie sa fie compatibile cu standardul de alimentare cu energie electrică din România: tensiune 220-230V curent alternativ la frecvența de 50 Hz.

Toate echipamentele ofertate trebuie sa fie noi, din producția ultimelor 12 luni.

Pentru fiecare echipament în parte se vor include în ofertă toate accesoriile și cablurile de conexiune/interconectare necesare funcționarii și interconectării acestora în arhitectura generală, indiferent dacă acestea au fost sau nu solicitate în mod expres în acest caiet de sarcini.

Ofertanții vor prezenta documente doveditoare din partea furnizorilor echipamentelor care să ateste faptul că echipamentele (inclusiv modelele) incluse în ofertă nu sunt scoase din fabricație și nu sunt anunțate ca fiind “end of life” la date depunerii ofertei.

Infrastructura hardware va fi găzduită în dulapuri metalice (rack-uri) standard cu lățimea de 19 țoli care oferă un spațiu de 42 unități standardizate de spațiu (42U). Pentru a se asigura condiții optime de găzduire și răcire (flux de aer) pentru echipamentele de tip server și echipamentele de stocare a datelor, este necesar ca aceste echipamente și aceste dulapuri să aibă un același producător sau să provină de la producători compatibili.

5.2.2 Cerințe specifice echipamente

5.2.2.1 Server tip 1

Caracteristici	**Valoare**
Dimensiuni	Înălțime 1U, lățime half-witdh – astfel încât două astfel de server-e să ocupe 1U în șasiul metalic
Procesor	
Nuclee de procesare	Minim 8, minim 2 fire de execuție per nucleu
Memorie cache	20MB
Frecvența de lucru	Minim 2,10GHz
Cantitate:	2 bucăți
Memorie RAM	Minim 8GB DDR3 utili pentru fiecare nucleu de procesare din procesor
Stocare internă	Minim 250 GB spațiu stocare pentru găzduirea mecanismelor de virtualizare
Interfețe de conectare	2 interfețe de tip CNA (Converged Network Adapter), fiecare cu o capacitate de 10 Gbps
Scalabilitate internă	
Nuclee de procesare	Până la minim 20 de nuclee de procesare

Memorie RAM	Până la minim 256 GB memorie
Sloturi PCI	Minim 1 slot PCI-Express 3.0 16x
Stocare internă	Minim 4 sloturi hot-plug pentru unități de stocare de 2,5”
Caracteristici de înaltă disponibilitate (HA)	
Stocare internă	Capacitatea utilă protejată prin RAID 1 sau similar
Condiții de funcționare	Să poată funcționa la o temperatură de până la 40°C
Sisteme de operare și platforme de virtualizare suportate	Microsoft Windows 2008/R2, Microsoft Windows 2012/R2, VMware ESXi 5, Sisteme de operare de tip Linux

5.2.2.2 Server tip 2

Caracteristici	**Valoare minimă**
Dimensiuni	Înălțime: maxim 8U
Procesor	
Nuclee de procesare	Minim 10, minim 2 fire de execuție per nucleu
Memorie cache	Minim 24MB
Frecvența de lucru	2GHz
Cantitate:	4 bucăți
Memorie RAM	Minim 8GB (DDR3 min. 1600MHz) utili pentru fiecare nucleu de procesare din procesor
Stocare internă	Minim 250 GB spațiu stocare pentru găzduirea mecanismelor de virtualizare
Interfețe conectare	4 interfețe de tip CNA (Converged Network Adapter), fiecare cu o capacitate de 10 Gbps
Scalabilitate internă	
Nuclee de procesare	Până la minim 60 de nuclee de procesare
Memorie RAM	Până la minim 4TB memorie
Sloturi PCI	Minim 12 sloturi PCI-Express 3.0 16x
Stocare internă	Minim 8 sloturi hot-plug pentru unități de stocare de 2,5”
Caracteristici de înaltă disponibilitate (HA)	
Managementul sistemului	Service procesor și system clock redundante PFA (Predictive Failure Analysis)
Procesor	Dealocarea dinamică (fără reboot) a nucleelor de procesare la comanda PFA Înlocuire dinamică a nucleelor de procesare cu nuclee alocate ca rezervă
Memorie	Dealocarea dinamică (fără reboot) a paginilor de memorie la comanda PFA

Interfețe I/O	Sloturi I/O hot plug
Stocare internă	Capacitatea utilă protejată prin RAID 1 sau similar
Flexibilitate în utilizare	
Nuclee de procesare	Adăugare dinamică (fără reboot) de nuclee de procesare
Memorie RAM	Adăugare dinamică (fără reboot) de plăci pentru module de memorie
Condiții de funcționare	Să poată funcționa la o temperatură de până la 40°C
Sisteme de operare și platforme de virtualizare suportate	Microsoft Windows 2008/R2, Microsoft Windows 2012/R2, VMware ESXi 5.x, Sisteme de operare de tip Linux

5.2.2.3 Resurse de stocare date

Capacitățile totale de stocare sunt următoarele:

- Hard-disk-uri clasice

Arhitectura	Activa-Activa astfel încât un LUN sa fie accesibil prin toate controloarele simultan, cu virtualizare atât pentru spațiul de date cat și pentru spațiul de rezerva. Virtualizarea se va efectua prin mecanisme interne unității de stocare.
Tip HDD suportate	SAS, S-ATA, SSD în incinte SFF sau/și LFF Suport pentru minim 450 de discuri distribuite în minim 2 nivele de performanta pe discuri SAS(10k/15k) și S-ATA(7.2k)
Capacitate instalata	- 128TB capacitate neta, disponibila spre utilizare după configurarea mecanismelor de protecție RAID 5 pe discuri cu viteza de minim 10000rpm - 168TB capacitate neta, disponibila spre utilizare după configurarea mecanismelor de protecție RAID 5 pe discuri cu viteza de minim 7200rpm - Pentru fiecare tip de HDD inclus în matricile RAID se vor instala în plus unități hot-spare minim 5% din cantitatea totală.
RAID	RAID 0, 1, 5 și 6

Nr Controloare	4 instalate
Cache	Minim 48 GB instalat în unitatea de stocare
Conectivitate	Minim 4 porturi 8Gbps FC cu SFP-uri incluse, livrate în configurația solicitată, cu posibilitate de upgrade la minim 22 porturi de 8 Gbps FC; Posibilitate de upgrade la minim 8 porturi Ethernet de 10GB oferind suport pentru iSCSI și FCoE. Echipamentul trebuie să permită instalarea și utilizarea simultană a interfețelor iSCSI 10 GB și FC 8GB.
Conectivitate SAN	Minim 8 x 8GB FC instalat
Tipuri de discuri suportate	- discuri SFF SAS sau FC: de capacitate minima: 300GB la viteza 15000rpm, - discuri SAS sau FC de capacitate minima 900GB la viteza 10000rpm - discuri LFF SAS Nearline, sau SATA de capacitate minimum 2TB la viteza 7200rpm - discuri SSD de capacitate minima 400 GB. - suport pentru minim 120 de discuri de tip SSD SLC
Spațiu fizic	Spațiul ocupat maxim 4U per unitate de expansiune indiferent de tipul de discuri folosite. Minim 18 Hdd-uri per sertar indiferent de tehnologia folosita.
Scalabilitate	minim 850 TB spațiu brut, neprotejat RAID (raw) și minim 450 de discuri
Management sistem	Prin unitate de management dedicata
Form factor	Rackabil
Asigurarea disponibilității	Controller-e duale, capabile sa susțină funcționalitățile întregului ansamblu în caz de defectare de tip activ-activ astfel încât o singura unitate logica sa poate fi accesata de ambele controloare în același timp Sistemul ofertat va fi configurat pentru asigurarea unei înalte disponibilități cu “No Single Point of Failure” pentru controloare, memorie cache, ventilatoare și surse de alimentare

	Echipamentul trebuie să asigure conectarea către fiecare sertar de discuri prin intermediul a două cai de acces redundante. Conectivitatea internă a discurilor trebuie să fie de tip punct la punct. Sistemul trebuie să permită instalarea, în același sistem de stocare, a discurilor SAS, SSD și Nearline SAS/SATA, fără ca acest lucru să impună restricții de performanță. Mecanisme de protecție a datelor existente în memoria cache prin scriere pe o memorie de tip non-volatila, în cazul unor căderi de tensiune electrica. Modelul propus trebuie să suporte și să permită intermixarea unităților de expansiune cu discuri de 3.5 inch cu cele cu discuri de 2.5 inch. Conectarea discurilor trebuie să fie asigurată cu suport pentru tehnologie HotSwap – extragerea, completarea sau înlocuirea să poată fi realizată on line. Echipamentul ofertat va furniza suport de upgrade firmware on-line pentru controller-e și discuri Surse de alimentare redundante, cu baterii integrate pentru protecția cache-ului. Suport nativ fără echipamente suplimentare pentru replicare locala și/sau la distanta prin intermediul protocolului iSCSI Posibilitatea de upgrade de firmware fără scoaterea sistemului din funcțiune Sistemul trebuie sa fie protejat de o unitate de alimentare cu tensiune de siguranța (UPS) cu o putere minima de 3kVA
Funcționalitățile echipamentului	Aplicație care asigura provizionarea sistemului de stocare în funcție de cerințele aplicațiilor cu posibilitate de definire a unor rutine de provizionare pe diverse grupuri de aplicații, precum și raportarea

	statistica în funcție de utilizarea discurilor per aplicație. Capabilități de tip „thin provisioning” licențiate pentru întreaga capacitate a echipamentului, astfel încât în cazul unor upgrade-uri ulterioare sa nu fie necesara achiziționarea unor noi licențe. Echipamentul trebuie sa permită realizarea a unui total de cel puțin 450 de copii instantanee pe fiecare volum de date disponibile pentru citirea de către aplicații. Pentru a asigura capacitatea de scalabilitate ulterioară printr-un centru de date secundar pentru recuperare în caz de dezastru, echipamentul ofertat va implementat un mecanism care sa permită failover între 2 sau mai multe echipamente de stocare localizate în data centere diferite dpdv geografic printr-o modalitate transparenta fata de host-uri. Failover-ul va fi posibil prin mecanisme interne echipamentului de stocare. Sa permită replicarea de date intre 2 sau mai multe echipamente de stocare localizate în data centere diferite dpdv geografic prin intermediul protocolului IP cat și FC. Procesul de replicare va utiliza avantajele oferite de tehnologia de tip “thin provisioning” oferita de către echipamentul de stocare. Facilitate de „storage tiering” manual și/sau automat în funcție de nevoile aplicațiilor. Sistemul trebuie sa permită gruparea datelor în funcție de necesitățile de performanta ale aplicațiilor pe cel puțin trei nivele distincte de performanta. Capabilitatea de transport automat al datelor intre mai multe echipamente, printr-o modalitate transparenta pentru aplicații, cu scopul de a menține o încărcare uniforma pentru întreg ansamblul. Sistemul trebuie sa permită implementarea mecanismelor de

	protecție a nivelului de performanta necesar unui volum de date prin definirea unor politici de priorități în funcție de performanta disponibila a sistemului (Quality of Service) Posibilități de management prin sesiuni de tip telnet, SSH și SMI-S Suport pentru realizarea de snapshot-uri consistente pentru următoarele aplicații și baze de date: Microsoft SQL, Microsoft Exchange, Oracle, VMware vSphere. Sisteme de operare suportate: Microsoft Windows, VMWare, IBM AIX, HP-UX, Sun Solaris, Linux. Funcționalitățile descrise mai sus, thin provisioning, realizarea de copii instantanee locale, replicare la distanta, failover intre 2 echipamente, ierarhizarea în funcție de performanta (storage tiering), funcționalitatea de transport automat al datelor intre echipamente, QoS, trebuie sa fie disponibile pentru întreaga capacitate a sistemului oferit, astfel încât eventualele creșteri ulterioare de capacitate sa nu necesite costuri suplimentare pentru activarea sau licențierea acestor funcționalități. Toate driverele sau licențele aferente conectării oricărui tip de host trebuie sa fie incluse in oferta indiferent de numărul acestora și de tipul sistemului de operare. Echipamentul ofertat trebuie sa ofere funcționalitățile standard ale masivelor de stocare, cum ar fi: - administrarea structurii RAID - structura de administrat volume - mirroringul volumelor folosite de baza de date etc., care vor fi implementate intern celor doua controller-e.

- Discuri de tip SSD

Arhitectura	Activa-Activa astfel încât un LUN sa fie accesibil prin toate controller-ele simultan, cu virtualizare atât pentru spațiul de date cat și pentru spațiul de rezerva. Virtualizarea se va efectua prin mecanisme interne unității de stocare.
Tip HDD suportate	Solid State Drive SLC și MLC Suport pentru minim 210 discuri de tip SSD de capacitate minima 200GB
Capacitate instalata	38TB capacitate neta, disponibila spre utilizare după configurarea mecanismelor de protecție RAID 5 Pentru fiecare tip de HDD inclus în matricile RAID se vor instala în plus unități hot-spare minim 5% din cantitatea totala.
Performanta	Pentru familia de echipamente ofertate trebuie sa existe cel puțin un test de performanta publicat de către o entitate independenta (Storage Performance Council sau echivalent) care sa ateste o performanta de cel puțin 500.000 IOPS cu un timp de răspuns mai mic de 1 milisecunda.
RAID	RAID 0, 1, 5 și 6
Controllere	2 instalate, suport pentru 4 controllere instalate
Cache	Minim 112GB instalat în unitatea de stocare
Conectivitate	Suport pentru conectivitate prin oricare din protocoalele Fibre Channel, iSCSI, FCoE
Conectivitate SAN	Minim 8 * 8GB FC instalat
Management sistem	Prin unitate de management dedicata
Form factor	Rackabil
Asigurarea disponibilității	Controller-e duale, capabile sa susțină funcționalitățile întregului ansamblu în caz de defectare de tip activ-activ astfel încât o singura unitate logica sa poate fi accesata de ambele controloare în același

	timp Sistemul ofertat va fi configurat pentru asigurarea unei înalte disponibilități cu “No Single Point of Failure” pentru controloare, memorie cache, ventilatoare și surse de alimentare Mecanisme de protecție a datelor existente în memoria cache prin scriere pe o memorie de tip non-volatila, în cazul unor căderi de tensiune electrica. Suport de upgrade firmware on-line pentru controller-e și discuri Surse de alimentare redundante, cu baterii integrate protecția cache-ului Suport nativ fără echipamente suplimentare pentru replicare locala și/sau la distanta prin intermediul protocolului iSCSI Posibilitatea de upgrade de firmware fără scoaterea sistemului din funcțiune Sistemul trebuie sa fie protejat de o unitate de alimentare cu tensiune de siguranță (UPS) cu o putere minima de 3kVA
Funcționalitățile echipamentului	Asigura provizionarea sistemului de stocare în funcție de cerințele aplicațiilor cu posibilitate de definire a unor rutine de provizionare pe diverse grupuri de aplicații, precum și raportarea statistica în funcție de utilizarea discurilor per aplicație. Funcționalitate de tip „thin provisioning” licențiată pentru întreaga capacitate a echipamentului, în cazul unor upgrade-uri ulterioare nefiind necesara achiziționarea unor noi licențe. Echipamentul trebuie sa permită realizarea a unui total de cel puțin 450 de copii instantanee pe fiecare volum de date disponibile pentru citirea de către aplicații. Sistemul trebuie sa permită implementarea mecanismelor de protecție a nivelului de performanta necesar unui volum de date prin definirea unor politici de priorități în funcție de performanta

	disponibila a sistemului (Quality of Service) Capabilitatea de transport automat al datelor intre mai multe echipamente, printr-o modalitate transparenta pentru aplicații, cu scopul de a menține o incarnare uniforma pentru întreg ansamblul. Funcționalitățile descrise mai sus, thin provisioning, realizarea de copii instantanee locale, replicare la distanta, failover intre 2 echipamente, ierarhizarea în funcție de performanta (storage tiering), funcționalitatea de transport automat al datelor intre echipamente, QoS, trebuie sa fie disponibile pentru întreaga capacitate a sistemului oferit, eventualele creșteri ulterioare de capacitate sa nu necesite costuri suplimentare pentru activarea sau licențierea acestor funcționalități. Posibilități de management prin sesiuni de tip telnet, SSH și SMI-S Suport pentru realizarea de snapshot-uri consistente pentru următoarele aplicații și baze de date: Microsoft SQL, Microsoft Exchange, Oracle, VMware vSphere. Aplicație licențiată care permite realizarea de snapshot-uri consistente pentru baza/bazele de date ofertate. Sisteme de operare suportate: Microsoft Windows, VMWare, IBM AIX, HP-UX, Sun Solaris, Linux. Toate driverele sau licențele aferente conectării oricărui tip de host sa fie incluse indiferent de numărul acestora și tipul sistemului de operare. Funcționalitățile standard ale masivelor de stocare, cum ar fi: - administrarea structurii RAID - structura de administrat volume - mirroringul volumelor folosite de baza de date etc., vor fi implementate intern celor doua controllere.

Conectivitatea către servere a celor 4 controllere va fi asigurată de un total de 48 porturi cu o viteză de minim 8 Gbps fiecare.

Memoria cache totală pe cele 4 controllere va fi de cel puțin 128 GB.

5.2.2.4 Unitate de backup pe bandă

Tehnologie	Soluție modulara (rack/frame) de tip enterprise, scalabila care sa permită creșterea capacității de stocare (număr drive-uri și casete) prin adăugarea de noi module.
Număr driver-uri	Minim 4 Ultrium 6 Fibre Channel instalate. Sa permită intermixare de drive-uri diferite.
Sloturi	Minim 1100 de sloturi în configurația propusa.
Conectivitate	Fibre Channel.
Specificații tehnice minimale	Sa permită partiționarea resurselor Display LCD pentru operare
Management și administrare	Sa permită partiționarea dinamica a bibliotecii, adăugarea și eliminarea în mod transparent a capacității de stocare fata de host-uri, configurarea capacitații de stocare fără întreruperea funcționarii Ajută la reducerea riscului de date prin monitorizarea activității bibliotecii și furnizarea de alerte privind sănătatea și integritatea unitățile de bandă și mass-media Monitorizarea activității bibliotecii și furnizarea de alerte privind integritatea casetelor și a driver-urilor Optimizarea resurselor pentru echilibrarea utilizării Identificarea resurselor supra-solicitate pentru a putea evita uzura

	prematură Informații privind utilizarea mediilor de stocare și estimări privind necesarul de casete care trebuie achiziționate Informații privind performanta sistemului
Posibilitate upgrade	Echipamentul trebuie sa fie upgradabil la minim: • 90 drive-uri • 10.000 de slot-uri • 70 sloturi I/O Posibilitatea de a conecta mai multe biblioteci intr-un singur sistem centralizat. Posibilitatea utilizării de module (rack/frame) cu densitate mare de sloturi (minim 1300 sloturi)
Media	1040 casete LTO 6 cu etichete cu coduri de bare
Garanție	Minim 36 luni

5.2.2.5 Stații de lucru pentru administrare

Caracteristici	**Valoare minimă**
Descriere	Stație de lucru mobilă de tip Notebook PC
Procesor	Minim Intel Core i5 sau echivalent, minim 3 GHz, minim 2 nuclee de procesare
Memorie cache	Minim 6 MB
Memorie RAM	Minim 8 GB SDRAM DDR3
Unitate de stocare	Minim 256 GB SSD

Unitate optica	DVDRW interna
Placa video	Integrata
Placa audio	Integrata
Placa rețea	Integrata 10/100/1000 Gigabit Ethernet,
Porturi	2 x USB / 1 x RJ45/ 1 x port video/ 1 x Audio
Ecran	Minim 14”, maxim 16”, retroiluminare cu LED, rezoluție minim 1600x900
Baterie	Minim 50Wh
Caracteristici de securitate	- Posibilitatea de a seta parole diferite pentru BIOS și hard disc
Sistem de operare și software	Windows 8 Professional sau echivalent, OEM cu licența. Drivere pe suport optic și DVD pentru restaurarea sistemului.
Conformitate cu standarde europene	Certificare CE conform directivelor UE
Greutate	Maxim 2,5 kg

5.2.2.6 Echipamente multifuncționale de mare capacitate

Caracteristici	**Valoare minimă**
Format pagină suportat	A3, A4, A5, A6
Tehnologie	Laser Color
Funcții	Fax Copiere Scanare Imprimare
Port-uri	USB, LAN
Volum lunar maxim	100.000 pagini
Rezoluție	1200x1200 dpi imprimare; 600x600 dpi scanare; 600x600 dpi copiere
Viteza imprimare	color/alb-negru minim 40 ppm A4
Accesorii incluse	Duplex, ADF

5.2.2.7 Sistem de comunicații

5.2.2.7.1 Nivelul acces

Switch-ul pentru acces servere trebuie să aibă următoarele caracteristici tehnice:

- 32 de interfețe 1/10 gigabit ethernet și FCoE de tip SFP+ pentru conectare la echipamente de tip server ce suportă interfețe CNA (Converged Network Adapter)
- 8 interfețe de tip 10 gigabit ethernet și FCoE de tip SFP+ pentru conectare la echipamentele de tip switch (porturi de uplink);
- Rata de procesare a pachetelor în hardware de 590 mpps;
- Capacitate de switching pentru uplink de 160 Gbps full duplex;
- Să aibă capabilități de FCoE;
- 2 surse de alimentare configurate redundant cu posibilitatea de hot-swap;
- Module de ventilatoare cu posibilitatea de hot-swap;
- Să aibă capabilități de Data Center bridging (DCB);
- Protocoale și facilități:
    - SFF-8461
    - SFF 8431
    - 802.1q
    - 802.3ae
    - Jumbo frames (dimensiune pachet de 9216 bytes)
    - 802.1p
    - Configurare QoS per port
    - 8 cozi de prioritizare în hardware per port
- Management: SNMP v2, SNMP v3, RMON, XML, management prin intermediul echipamentului switch agregare acces (din punctul de vedere al managementului switchurile vor fi considerate ca o extensie a switch-ului de agregare acces);

- Echipamentul va fi livrat cu 16 module SFP+ de 10 gigabit pentru fibra multimode ce vor fi folosite pentru asigurarea interconectării dintre echipamentele de tip switch de pe nivelul de agregare și switch-ul de acces;
- Echipamentul va fi livrat cu 26 cabluri și conectorii SFP+ aferenți, pentru asigurarea conexiunilor dintre switch și porturile server-elor.
- Echipamentul va fi livrat cu 8 cabluri și conectorii SFP+ aferenți, pentru asigurarea conexiunilor dintre switch-ul acces și switch-ul agregare acces.
- Dimensiune: 1U;

5.2.2.7.2 Nivel agregare

Switch-ul pentru agregare acces trebuie să aibă următoarele caracteristici tehnice:

- Echipament modular cu 48 de porturi fixe 1/10 Gigabit Ethernet SFP+, 4 porturi QSFP+ de 40 Gbps și 2 sloturi pentru module adiționale din care unul va fi echipat cu un modul cu 24 interfețe de tip SFP+ 1/10 Gigabit Ethernet SFP+ și 2 porturi QSFP+ de 40 Gbps
- Tehnologie de switching: cut-through;
- Rata de procesare layer 2 și layer 3 în hardware de 2.50 Tbps;
- Să aibă capabilități de Data Center bridging (DCB): IEEE 802.1Qaz, IEEE 802.1Qbb;
- 4 surse de alimentare configurate redundant cu posibilitatea de hot-swap;
- 4 module de ventilatoare configurate redundant cu posibilitatea de hot-swap;
- Protocoale și facilități:
    - Să aibă capabilități de FCoE și Fiber Channel 8/4/2/1 Gbps;
    - Protocoale de rutare IPv4 și IPv6: static, OSPF, BGP;
    - BFD (Bidirectional Forwarding Detection);
    - Jumbo frames (dimensiune pachet de 9216 bytes)
    - 30.000 rute layer 3 de tip Ipv4 și 6.000 de rute layer 3 de tip IPv6;
    - 6000 grupuri IGMP snooping;

- 200.000 de adrese MAC și intrări ARP combinate;
- Configurare QoS per port
- 6 cozi de prioritizare în hardware per port pentru trafic unicast
- 6 cozi de prioritizare în hardware per port pentru trafic multicast
- 3500 liste de control a accesului (ACL);
- 3500 de intrări VRF;
- Interfețe VLAN 4000;
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.1w
- IEEE 802.1s: 64 de instanțe MSTP
- IEEE 802.3ad
- IEEE 802.3x
- RFC 896
- DHCP snooping
- DHCP relay
- Virtual Router Redundancy Protocol (VRRP)
- Multicast: PIMv2 sparse mode, IGMP v2, IGMP v3;
- posibilitate de limitare a numărului de pachete de broadcast, multicast și unicast;
- FC-BB-5;

- Management: in-band, out-of-band, AAA, RADIUS, RBAC, SNMP v2, SNMP v3, RMON, NETCONF, CLI (linie de comandă), SSHv2, syslog, NTP, administrare separată între funcțiile de LAN și cele de SAN. Echipamentul va putea asigura managementul switch-urilor de

acces (din punctul de vedere al managementului switchurile de acces care conectează server-ele vor fi considerate ca o extensie a switch-ului de agregare acces);

- Echipamentul va fi livrat cu 4 module QSFP+ de 40 Gbps;
- Echipamentul va fi livrat cu 24 module SFP+ 8 Gbps Fiber Channel;
- Echipamentul va avea activate facilitățile de Fiber Channel pentru cele 24 porturi;
- Dimensiune: 2U;
- Garanție: 3 ani;

5.2.2.7.3 Nivel core (nucleul rețelei)

5.2.2.7.3.1 Switch core L2/L3

Echipamentul va avea următoarele caracteristici tehnice:

- Echipament modular cu 11 sloturi pentru module cu performanțe posibile de 20 Tbps.
- Echipamentul va fi configurat astfel:
    - 1 modul de supervizare cu următoarele caracteristici:
        - Procesor quad-core;
        - Memorie RAM 32 GB;
        - Memorie flash 16GB;
        - Port de management 10/100/1000 ethernet;
        - Port de consolă serial;
        - 2 porturi USB pentru conectare dispozitive de stocare;
    - 3 module pentru asigurarea de mai multe canale de comunicație în paralel pentru modulul de supervizare și modulele cu porturi. Cele 3 module vor asigura împreună o capacitate de 550 Gbps per slot.
    - Un modul cu 24 de porturi 40 Gbps QSFP+ cu următoarele performanțe și caracteristici:

        - Rata de procesare pachete layer 2 și 3 în hardware de 1.30 bpps;
        - 60.000 de adrese MAC;
        - 4000 VLAN-uri;
        - 60.000 Adrese IPv4;
        - 16.000 ACL-uri;
        - Jumbo frames (dimensiune pachet de 9216 bytes)
- 2 surse de alimentare configurate redundant cu posibilitatea de hot-swap;
- 3 module de ventilatoare configurate redundant cu posibilitatea de hot-swap;
- Protocoale și facilități:
    - Protocoale de rutare IPv4 și IPv6: static, OSPF, BGP;
    - Multicast: PIMv2 sparse mode;
    - Jumbo frames;
    - IEEE 802.1p;
    - IEEE 802.1q;
    - IEEE 802.1w;
    - IEEE 802.1s;
    - IEEE 802.3ad;
    - IEEE 802.1Qbb;
    - Liste de acces la nivel 2 bazate pe adrese MAC.
    - Liste de acces la nivel 3 și 4 pentru IPv4 și IPv6;
    - DHCP snooping
    - Virtual Router Redundancy Protocol (VRRP)

- IGMPv2, IGMPv3;

- Management: in-band, out-of-band, AAA, RADIUS, RBAC, SNMP v2, SNMP v3, RMON, NETCONF, CLI, SSHv2, syslog, NTP.
- Echipamentul va fi livrat cu 4 module QSFP+ de 40 Gbps;
- Echipamentul va fi livrat cu 2 module QSFP+ de 40 Gbps care se pot conecta la 4 porturi de 10 Gbps SFP+ inclusiv cu cablurile aferente;
- Dimensiune: 9U;

5.2.2.7.3.2 Acces WAN și echipamente de management, monitorizare și securitate

5.2.2.7.3.2.1 Server pentru managementul și virtualizarea serviciilor de rețea

Infrastructura de Cloud Computing trebuie sa beneficieze de o platformă hardware dedicată care sa asigure implementarea (și virtualizarea) serviciilor de rețea. In acest sens se impune furnizarea a doua servere dedicate (in configurație redundanta) cu respectarea următoarelor cerințe minimale (la nivelul fiecărui server):

- 2 x procesoare: 2 GHz, 8 nuclee, 20 MB cache
- Memorie 8 x 8-GB DDR3 1600-MHz RDIMM
- 2 interfețe Gigabit Ethernet
- 10 Gigabit Ethernet SFP+ de tip CNA
- Controller RAID (suport pentru RAID 10)
- HDD: 4 x 1-TB SATA, 7200-rpm
- 16-GB Flash drive
- Controller management:
    - Conformitate IPMI 2.0
    - O interfața management 10/100/1000 Ethernet
    - Interfața CLI și Web

- Interfața pentru conectare consola KVM (2 porturi USB, 1 VGA, 1 port serial)
- Rackabil: maxim 1 RU
- Temperatura de operare: până la 40°C
- Umiditate: 10 - 90% fără condens

Platforma hardware pentru managementul și virtualizarea serviciilor de rețea trebuie sa permită rularea independenta (virtuala) a următoarelor module dedicate:

- **Modul virtual de supervizare** a **switchurilor virtuale**
- **Modul virtual de securizare**, care prin intermediul politicilor de securitate sa permită definirea de zone și contexte de securitate distincte
- **Modul virtual de analiza a rețelei** care sa permită monitorizarea gradului de încărcare/utilizare a rețelei de către entitățile găzduite in sistem (stații de lucru, servere, mașini virtuale, aplicații etc.)
- **Modul management LAN**
    - Se va furniza un software de management dedicat pentru operațiuni de LAN și SAN in centre de date ce va oferi o platformă comună de administrare a facilităților de routing, switching și storage prin automatizarea proceselor de provizionare, detectarea degradării performanțelor prin monitorizarea componentelor de SAN și LAN, precum și simplificarea diagnozei echipamentelor de rețea. Software-ul va avea următoarele facilități:
    - Platforma de tip client-server;
    - Template-uri predefinite pentru provizionarea componentelor de LAN și SAN
    - Template-uri customizabile
    - Editor de template-uri
    - Interfețe de monitorizare a funcționării componentelor de tip LAN și SAN;
    - Vizualizarea performanțelor în timp real sau pe baza statisticilor istorice pentru echipamentele centrului de date;

- Posibilitatea de definire de rapoarte cusomizabile
- Urmărirea porturilor utilizate în vederea stabilirii resurselor consumate;
- Posibilitatea de vizualizare a comunicației prin echipamentele fizice de rețea pe care o mașină virtuală o folosește pentru a accesa SAN-ul;
- Afișează hărți de layer 2
- Afișează în timp real harți cu situația operațională a infrastructurii centrului de date;
- Posibilitatea de export a rapoartelor;
- Posibilitatea de descoperire automată a echipamentelor de infrastructură și stocarea informațiilor despre acestea într-un inventar.
    - Posibilitatea de validare a configurațiilor (și vizualizare a modificărilor) înaintea aplicării acestora
    - Arhivarea configurațiilor cu posibilitatea de comparare/vizualizare a acestora
    - Posibilitate de realizare de backup centralizat al configurațiilor precum și realizarea de update software centralizat
    - API pentru integrarea cu aplicații third party

5.2.2.7.3.2.2 Switch virtual

Soluția ofertata trebuie sa permită instalarea și configurarea de switchuri virtuale (cel puțin 148 – aferente celor 148 platforme de virtualizare ce vor rula pe serverele Tip1 și Tip2) care sa asigure următoarele funcționalități minimale:

- DHCP snooping
- Dynamic Address Resolution Protocol (ARP) Inspection
- VLAN-uri
- Private VLANs
- Prevenire bucle

- Multicast
- Link Aggregation Control Protocol (LACP)
- SNMP, RADIUS
- ACL (liste de control al accesului)
- QoS
- VXLAN

5.2.2.7.3.2.3 Firewall

Echipamentul va avea următoarele caracteristici tehnice:

- 8 porturi RJ 45 ethernet 10/100/1000;
- 4 porturi de 10Gbps tip SFP/SFP+;
- Memorie flash 8GB;
- Memorie RAM 24 GB;
- Port dedicat de management gigabit ethernet;
- 2 surse de alimentare configurate redundant;
- Performanțe și facilități:
    - NGFW (Next-Generation Firewall)
    - Rată de procesare pachete pe secundă 2.800.000 (calculată pentru pachete cu dimensiune de 64 bytes)
    - Firewall throughput (multiprotocol) 5 Gbps;
    - VPN 3DES sau AES throughput 2 Gbps;
    - Conexiuni concurente 1.800.000;
    - Conexiuni noi pe secunda 100.000;
    - Interfețe de tip VLAN 1.000;

- Contexte virtuale de securitate minim 2;
- Disponibilitate ridicată de tipul Active/Active sau Active/Standby;
- Facilități NAT de tipul static, dinamic, PAT, one-to-one, many-to-one;
- Liste de acces pentru filtrarea traficului;
- Protecție împotriva atacurilor bazate pe fragmente IP;
- Posibilități de clasificare a traficului prin tehnologii QoS;
- Posibilități de aplicare a unor limite pentru conexiunile TCP și UDP în vederea protejării față de atacuri de tip DoS;
- Suport pentru IKEv1 și IKEv2;
- Inspectarea protocoalelor cum ar fi: FTP, H.323, H.225, , RTSP, SMTP, DNS, HTTP
- Posibilitatea de aplicare a politicilor de acces bazate pe numele de utilizator sau rolul acestora;
- Filtrare URL;

- Să suporte jumbo frames;
- Protocoale de rutare: RIP, OSPF;
- Rutare multicast;
- Suport pentru IPv6;
- Management: CLI, GUI, SSH v2, SNMP v2c, SNMP v3, Syslog;
- Suport pentru NTP;
- Dimensiune: 2U;
- Echipamentul va fi livrat cu 4 module 10 Gigabit Ethernet SFP+;

5.2.2.7.3.2.4 Platforma pentru balansare a traficului şi securizare Web

Pentru asigurarea unui nivel cat mai ridicat de disponibilitate și securitate serviciilor găzduite se impune furnizarea unei platforme de balansare a traficului cu respectarea următoarelor funcționalități minimale:

Funcționalități software:

- Suport pentru implementarea de contexte virtuale (pe aceeași platforma hardware)
- Balansare trafic Layer 4
    - suport pentru următoarele protocoale: DNS, TCP, UDP, HTTP, HTTPS, SIP
    - algoritmi: round robin sau funcție de numărul de pachete, lățime de banda, număr conexiuni sau timpi de răspuns
- monitorizare servere: PING, TCP, URL, scripturi
- Protecție împotriva atacurilor de tip DoS la Layer 4 și Layer 7
- Balansare baze de date
- Liste de control al accesului la Layer 3 și Layer 4, translatarea adreselor (NAT)
- Filtrarea conținutului la Layer 7 și posibilitate de rescriere URL/HTTP
- Posibilitate de conectare remote utilizând SSL VPN
- Gestionarea și accelerarea traficului SSL
- Multiplexare TCP și SQL
- Accelerarea/optimizarea conexiunilor TCP
- TCP buffering
- Protocoale dinamice de routare: OSPF, RIPv1/v2, BGP
- Disponibilitate: Activ/Pasiv, Activ/Activ, VRRP
- Funcționalități de rețea Layer 2: VLAN 802.1Q, Link Aggregation 802.3ad

- Suport IPv6
- Management: interfața Web securizata, CLI, Telnet, SSH, Consola

Caracteristici hardware:

- Throughput compresie: minim 2 Gbps
- Throughput: minim 4 Gbps;
- Cereri HTTP/secunda: minim 500.000;
- Tranzacții SSL/secunda: minim 7.000;
- Throughput SSL: minim 3 Gbps;
- Utilizatori concurenți VPN: minim 10.000;

5.2.2.7.3.2.5 Switch layer 2 10/100/1000

Echipamentul va avea următoarele caracteristici tehnice:

- 24 de porturi RJ45 ethernet 10/100/1000 și 4 porturi SFP de tip gigabit ethernet;
- Rata de forward a pachetelor (calculată pentru pachete cu dimensiune de 64 bytes) de 41.7 milioane de pachete pe secunda;
- 8000 Adrese MAC suportate;
- Suporta transmiterea de frame-uri cu o dimensiune de cel puțin 9200 bytes;
- Memorie flash pentru stocarea sistemului de operate: 64 MB;
- Să suporte 254 de vlan-uri;
- Să suporte 254 de grupuri IGMP;
- Protocoale și facilități:
    - IEEE 802.3ad – Link Aggregation Control Protocol;
    - IEEE 802.1s – Multiple Spanning Tree Protocol**;**
    - IEEE 802.1w – Rapid Spanning Tree Protocol;

- IEEE 802.1q – VLAN tagging;
- IEEE 802.1p – CoS prioritization;
- IEEE 802.1x – Port Based Network Access Control;
- RFC 1492, RFC 2474, RFC 951, RFC 3376, RFC 2597, RFC 2598, RFC 1256, RFC 1981;
- IGMP – Internet Group Management Protocol;
- NTP – Network Time Protocol;
- MVR – Multicast VLAN Registration;
- patru cozi de ieșire per port pentru QoS;

- Management:
  - port de consola pentru management, CLI, SSH v2, HTTP, HTTPS, SNMP v2c, SNMP v3, RMON;
- Securitate:
  - RADIUS;
  - 802.1x Port Based Network Access Control;
  - posibilitate de limitare a numărului de pachete de broadcast, multicast și unicast per port;
  - posibilitate de securizare a accesului pe porturile configurate in mod access sau trunk pe baza adresei de MAC sursă;
  - posibilitatea de limitare a numărului de adrese MAC învățate pe un port;
  - liste de acces per port pentru interfețele de layer 2;
  - multiple nivele de securitate pentru prevenirea modificării neautorizate a configurației echipamentului;
  - DHCP Snooping;

- Dimensiune: 1U.

5.2.2.7.3.2.6 Router WAN

Echipamentul va avea următoarele caracteristici tehnice:

- Echipament modular cu minim 3 sloturi
- Echipat cu 3 module de tip SPA cu un port de tip 10Gigabit Ethernet cu următoarele specificații:
    - Suport pentru Jumbo frames (9188 bytes)
    - 8000 VLAN-uri per modul , 4000 VLANuri per port pentru 802.1q
    - 802.1ad QinQ termination
    - 2000 Adrese MAC per modul
    - QoS
    - Putere consumata 20W
    - compatibil cu module de tip XFP
- Echipamentul va fi livrat cu 3 module XFP de tip 10GBASE-SR
- 6 porturi Gigabit Ethernet de tip SFP integrate
- doua surse de alimentare configurate redundant
- Procesor de rutare integrat in șasiu, cu următoarele caracteristici:
    - Produce și distribuie informații de forwarding către procesorul de tip ESP
    - procesor cu 4 nuclee
    - Memorie 4-GB DRAM upgradabila pana la 16 GB DRAM
    - Performante: 500,000 rute IPv4 sau 500,000 rute IPv6
    - Capabilități hot-swappable și field-replaceable

- Procesor de tip ESP (Embedded Services Processor) integrat in șasiu, cu următoarele caracteristici:
    - Throughput 10 Gbps upgradabil prin licență pana la 36 Gbps
    - Suport pentru OIR (Online Insertion Removal) sau similar
    - Suport pentru tehnologii de redundanta (NSF) Nonstop Forwarding și SSO (Stateful Switchover) sau similar
    - Management prin Telnet (CLI), port de consola sau SNMP (RFC 2665)
- Software pentru servicii avansate de tip enterprise
- Rack-abil 2 RU.

5.3 Cerinţe privind infrastructura software de bază

Software-ul de bază include sistemele de operare pentru servere, software-ul RDBMS, software-ul pentru gestiunea procesului de backup, precum și aplicaţiile specifice de administrare sau operare a componentelor hardware incluse în proiect.

5.3.1 Infrastructura de virtualizare

Infrastructura de virtualizare trebuie să satisfacă cerințele din capitolul „4.1.2 Infrastructura software” legate de platforma de virtualizare. Suplimentar, infrastructura de virtualizare trebuie să satisfacă următoarele cerințe:

- Să nu impună o limită cu privire la numărul de mașini virtuale ce pot fi definite pe infrastructura hardware implementată;
- Să ofere posibilitatea replicării mașinilor virtuale și datelor de pe un echipament de stocare pe altul, precum și posibilitatea de efectuare de copii de siguranță (backup) ale mașinilor virtuale în timp ce acestea rulează;
- Să se poată implementa mai multe sisteme de operare – Linux și Windows – în paralel pe un singur server fizic;

5.3.2 Sisteme de operare

Sistemul de operare ofertat trebuie să ofere minim următoarele funcționalități:

- Suport pentru integrare cu serviciu de director și suport pentru:
    - Optimizarea fluxului de lucru al administratorului pentru găsirea rapidă a obiectelor din director;
    - Asistenţă mai bună și mai eficientă în găsirea obiectelor în directoare mari;
    - Impact redus asupra serviciilor director în reţea;
    - Suport pentru implementare serviciu de director în virtualizare;
    - Suport pentru clonarea serverelor cu rolul de serviciu de director;
    - Abilitatea de face o căutare în jos la o unitate organizatorică (OU - Organization Unit) din cadrul directorului;
    - Capacitate flexibilă de interogare pentru găsirea obiectelor în director, bazată pe atributele acestora;
    - Să permită folosirea serviciilor de director pentru administrarea identităţilor și servicii de meta-director în scopul îmbunătăţirii administrării;
    - Serviciul de director pentru administrarea identităţilor va trebui să suporte LDAPv3.
- Aplicaţiile privilegiate de director pentru administrarea identităţilor trebuie sa fie capabile să obțină rezultate multiple, particularizate ale directorului pentru administrarea identităţilor;
- Monitorizarea, operațiunile și restaurarea directorului pentru administrarea identităţilor să poată fi delegate;
- Serviciile de director pentru administrarea identităţilor să permită replicarea conținutului;
- Serviciul de director trebuie să prezinte posibilitatea de modificare a topologiei infrastructurii, configuraţiei și procedurilor operaţionale printr-un proces de administrare a schimbării, iar modificările să poată fi delegate;

- Structura de director să poată fi administrată direct de un utilizator sau de o aplicaţie;
- Să ofere posibilitatea modificării accesului serviciului de director și a procedurilor de administrare;
- Serviciul de director de management al identităţilor trebuie să aibă o singură rădăcină (un singur root);
- Spațiul de nume al serviciului de director pentru administrarea identităţilor să poată fi partiționat într-un mod care să reflecte sau nu structura organizațională a organizației.
- Convenția de nume a organizației să identifice unic persoanele folosind un identificator numeric unic ca valoare pentru atributul Relative Distinguished Name;
- Serviciul de director să permită adăugarea sau modificarea definițiilor claselor de obiecte și a topologiei spațiului de nume;
- Serviciul de director să permită definirea politicilor de securitate aplicabile obiectelor gestionate în cadrul serviciului;
- Serviciul de director trebuie să ofere posibilitate de acces anonim, acces cu autentificare simplă și mecanisme puternice de autentificare prin LDAP;
- Să ofere posibilităţi de audit al accesului la serviciul de director și al modificărilor aduse serviciului de director;
- Serviciul de director sa ofere abilitatea de a stoca certificate și CRL-uri;
- Sa asigure integrare cu serviciul de DNS ;
- Oferă posibilitatea de a efectua legături multiple prin Lightweight Directory Access Protocol pe o conexiune, în scopul autentificării utilizatorilor
- Adaugă posibilitatea de a dezactiva comprimarea traficului de replicare între controlerele de domeniu care se află în situri diferite
- Suport pentru dezactivarea definiţiilor, atributelor și claselor din schema de director, astfel încât atributele și clasele să poată fi redefinite dacă s-au strecurat erori la definirea inițială

- Să permită administratorului Eliminarea restricțiilor RDN (Relative Distinguished Name) incompatibile cu standardul de director X.500;
- Să permită memorarea și reproducerea zonelor DNS memorate în partiţia de aplicaţie a directorului;
- Să permită mutarea elementelor interactive din faza configurării în faza ulterioară instalării, eliminând necesitatea interacțiunii administratorului la instalarea sistemului de operare;
- Să ofere o interfaţă unică pentru configurarea și monitorizarea serverului, cu programe de tip expert pentru optimizarea sarcinilor comune de administrare a serverului.
- Să ofere un shell opţional cu linie de comandă și limbaj de script, care să ajute administratorii să automatizeze sarcinile de rutină de administrare a sistemului pe mai multe servere.
- Să ofere instrumente de diagnosticare puternice, care vă oferă vizibilitate permanentă asupra mediului serverului, fizic și virtual, pentru a identifica și rezolva rapid problemele care apar.
- Să permită instalări minimale, în care sunt instalate numai rolurile și caracteristicile de care este strict nevoie, minimizând nevoile de întreținere și reducând zonele de atac de pe server.
- Să implementeze Internet Protocol versiunea 6 (IPv6);
- Să ofere Load Balancing (NLB) și pe IPv6 și să includă suport pentru mai multe adrese IP dedicate, ceea ce ar permite găzduirea mai multor aplicaţii în acelaşi cluster;
- Să permită virtualizarea rolurilor de server sub formă de maşini virtuale (VM) separate care rulează pe aceeaşi maşină fizică, fără a fi necesara achiziţia de software de la terţi;
- Să ofere posibilitatea replicării mașinilor virtuale către gazde situate în locații aflate la distanță; capabilitatea de replicare să poată fi oferită între gazde care sunt membri ai unui cluster sau gazde independente;
- Să ofere posibilitatea replicării mașinilor virtuale și datelor de pe un echipament de stocare pe altul;

- Să ofere suport pentru până la 256 procesoare logice, 1024 procesoare virtuale și 4 TB memorie la nivelul gazdei;
- Să ofere suport pentru 32 procesoare virtuale și 1 TB memorie la nivelul mașinilor virtuale;
- Să ofere suport pentru clustere cu 32 de noduri și 2048 de mașini virtuale;
- Să ofere suport pentru disc virtual în mașina virtuală până la 32 TB de date;
- Să ofere suport pentru 1024 de mașini virtuale pe o gazdă;
- Să ofere suport pentru redundanță la nivelul plăcii de rețea cu până la 16 de plăci de rețea în regim de „teaming”;
- sa se poată implementa mai multe sisteme de operare –Linux și Windows – în paralel pe un singur server;
- Sa ofere clustering-ul gazdelor sau al maşinilor virtuale și backup-ul maşinilor virtuale în timp ce acestea rulează ;
- Să permită programelor accesate de la distanță să fie deschise cu un singur clic și să fie utilizate ca și cum ar rula pe calculatorul utilizatorului final.
- Să permită replicarea setărilor site-urilor Web pe mai multe servere Web, fără a fi necesară configurări suplimentare.
- Să ofere administrarea delegată a aplicaţiilor și a site-urilor pentru control personalizat asupra diferitelor componente ale serverului Web.
- Să includă suport pentru administrarea integrităţii serverului Web, alături de instrumentele complexe de diagnosticare și depanare ce permit vizibilitatea și urmărirea cererilor care rulează pe serverul Web.
- Izolare a pachetelor de aplicaţii pentru a menţine site-urile și aplicaţiile izolate, crescând securitatea și stabilitatea.
- Suport CGI pentru rularea aplicaţiilor PHP, a script-urilor Perl și a aplicaţiilor Ruby.
- Sistemul de operare trebuie să permită rularea aplicațiilor web bazate pe tehnologii Java și Microsoft .Net;

- Să ofere suport pentru protocol HTML 5 și WebSocket;
- Să ofere un depozit central pentru stocarea certificatelor digitale folosite pentru protecția site-urilor web;
- Să ofere posibilitatea administrării la distanță pentru mai multe servere web dintr-o singură consolă;
- Să ofere posibilitatea de a găzdui servicii web în regim partajat de tip „multi-tenant” pentru mai multe site-uri web în regim de izolare;
- Să ofere posibilitatea de a măsura consumul de resurse al serverelor web partajate;
- Să ofere posibilitatea de a limita consumul de resurse de procesor, memorie sau lățime de bandă consumate de serverul web;
- Să ofere un mecanism ce asigură că reţeaua și sistemele nu sunt compromise de calculatoare virusate, izolând și/sau depanând calculatoarele care nu se conformează politicilor de securitate stabilite;
- Să ofere un mecanism de protecție împotriva aplicațiilor periculoase;
- Să ofere flexibilitate criptografică crescută, suportând algoritmi de criptare standard și definiţi de utilizator, permiţând crearea, stocarea și preluarea mai facilă a cheilor criptografice;
- Să permită o metodă mai sigură pentru autentificarea locală a utilizatorilor de la sucursale și birouri de la distanţă, cu ajutorul unei replici read-only a bazei de date LDAP principale;
- Să permită stabilirea mai simplă de relații acreditate între parteneri cu directoare de identități și de acces diferite care rulează în reţele diferite, permițând autentificarea unică (SSO) în rețele;
- Să conțină un modul pentru monitorizarea stării autorităților de certificare (CA);
- Să conțină un serviciu pentru prevenirea scurgerilor de informații confidențiale din interiorul organizației către exterior prin intermediul fișierelor;

- Să ofere protecție împotriva furtului de date și a expunerii hardware-ului serverului dacă este pierdut sau furat, oferind posibilitatea ștergerii sigure a datelor când server-ele nu mai sunt necesare;
- Să ofere sistem de clasificare a informațiilor pentru informații partajate prin configurarea automată a politicilor de acces prin politici de grup aplicate prin intermediul serviciului de tip director;
- Licențierea inclusă trebuie să permită dreptul de a utiliza un număr nelimitat de mașini virtuale ce pot rula pe mașina respectivă.

5.3.3 Sistem pentru gestiunea bazelor de date relaționale

Instrumentele de management și provizionare a infrastructurii de tip cloud ce urmează a fi implementate în cadrul proiectului necesită un sistem de gestiune a bazelor de date compatibil, care să ofere un suport performant, scalabil, sigur și de înaltă disponibilitate pentru bazele de date relaționale.

Soluția de gestiune a bazelor de date trebuie să ofere următoarele capabilități:

- Serverul de baza de date trebuie să permită folosirea a peste 48GB memorie.
- Serverul să permită folosirea a minim 16 nuclee de procesare (core-uri)
- Disponibilitate ridicată și mentenanță:
    - Sistemul trebuie să permită atingerea unui nivel de disponibilitate de peste 99,99%, prin definirea unor configurații de tip cluster pentru server-ele de baze de date
    - Posibilitatea efectuării backup-ului în multiple fișiere simultan pentru a putea efectua operația pe discuri diferite în paralel.
    - Posibilitatea efectuării backup-ului direct într-o soluție de cloud public, respectând normele de securitate

- Posibilitatea de a crea, modifica, șterge index-ul concurent cu activitățile utilizatorilor
- Posibilitatea de a crea un snapshot al bazei de date
- Modificarea schemei online
- Posibilitatea abonării la alerte în cazul unor evenimente din baza de date.

- Gestionare facilă a obiectelor bazelor de date:
  - Instrumente de dezvoltare a obiectelor din baza de date: soluția trebuie să ofere unelte de dezvoltare pentru modulele ETL (Extract, Transform, Load), pentru design-ul bazelor de date atât relaționale cât și multidimensionale, pentru design-ul rapoartelor.
  - Unelte pentru administrarea bazelor de date și a proceselor uzuale care se execută asupra bazelor de date precum și al rapoartelor
  - Posibilitatea de definire și gestionare a obiectelor bazei de date (tabele, indecși, proceduri stocate, triggere) direct din instrumentele folosite de dezvoltatori pentru scrierea aplicațiilor
  - Posibilitatea de a oferi compresia datelor folosind suport UCS-2 Unicode
  - Loc central care oferă posibilitatea administrării entităților de date și ierarhiilor din multiple baze de date cu posibilitatea versionării
- Performanțe ridicate ale sistemului de baze de date:
  - Criptarea transparentă a datelor, a fișierelor de date și a fişierelor jurnal fără să fie necesară modificarea aplicaţiei. Funcționalitățile de criptare sunt necesare pentru îndeplinirea cerinţelor și respectarea reglementărilor generale cu privire la confidenţialitatea datelor. Criptarea trebuie să ofere inclusiv instrumente de căutare în datele criptate utilizând sisteme de regăsire într-un interval sau căutarea parţială, fără modificarea aplicaţiilor existente.
  - Auditarea operațiilor:

- auditarea trebuie să includă informaţii despre momentul în care au fost citite datele, în plus faţă de orice modificare a datelor.
- Produsul trebuie sa ofere caracteristici precum configurarea îmbunătăţită și managementul auditurilor în server.
- Produsul sa definească specificaţiile de audit în fiecare bază de date, astfel încât configurația auditului să poată fi adaptată pentru diversele bazele de date.
- Posibilitatea de a filtra evenimentele auditate; posibilitatea de a customiza operația de audit în funcție de evenimentele din baza de date

- Posibilitatea adăugării online a resurselor de memorie la mașinile fizice care găzduiesc bazele de date, pentru scalarea la cerere a acestora.
- Colectarea datelor de performanţă:
  - facilități de optimizare și depanare a performanţei server-ului de baze de date, pentru a furniza administratorilor o perspectivă interactivă cu privire la performanţă
- Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de server prin captarea, filtrarea și reglarea evenimentelor generate de procesele de server. Evenimentele trebuie sa poată fi captate și exportate în diferite formate de ieşire, inclusiv în formatul utilizat de sistemul de operare gazdă, pentru corelarea cu aplicațiile sistemului de operare și ale bazelor de date, permițând astfel o monitorizare completă a sistemului.
- Comprimarea backup-urilor până la 50% prin comprimare rapidă a backup-urilor bazelor de date.
- Asigurarea continuității activității organizației: duplicarea datelor prin tehnologii de tip data mirorring
- Livrarea automata a log-urilor bazei de date către Data Recovery Center

- Implementarea structurilor de date complexe:

- Posibilitatea nativa de modelare a structurilor de date de tip arbore: metode încorporate pentru crearea și operarea pe noduri ierarhice.
- Posibilitatea stocării datelor binare mari, precum documente și imagini, ca parte integrantă a bazei de date, păstrând în același timp consecvența tranzacțională.
- Căutare complexă la nivel de text, folosind indecși specializați; efectuarea rapida a căutărilor în acest tip de date
- Managementul performant al coloanelor cu valori rare: modalități eficiente pentru administrarea spatiilor necompletate dintr-o bază de date relațională, astfel încât valorile de tip NULL să nu consume spaţiu fizic.

- Utilizarea unei platforme avansate pentru dezvoltarea de aplicații complexe de procesare a evenimentelor (CEP):
  - Posibilitatea de dezvoltarea de aplicații bazate pe evenimente folosind platforma de procesare a evenimentelor pentru a se permite interogări continue și latenta de milisecunde.
- Sistemul trebuie sa permită implementarea administrării bazate pe politici pentru:
  - Definirea și managementul politicilor de configurare a sistemului
  - Monitorizarea și prevenirea modificărilor asupra sistemului prin crearea de politici împotriva configurării
  - Detectarea problemelor de conformitate cu politicile direct din interfața de administrare a server-ului
  - Posibilități de virtualizare
- Soluția SGBD oferita sa ofere posibilitatea instalării, fără costuri adiționale, a unui număr nelimitat de baze de date distincte în mașini virtuale alocate serverului licențiat.
- Soluția trebuie sa nu impună nicio restricție din punct de vedere licențiere aferentă numărului de utilizatori ce se pot conecta la SGBD.

- Soluția de gestiune a bazelor de date trebuie licențiată pentru utilizarea completă a resurselor disponibile (numărul total de nuclee de procesare) în mașinile fizice pe care urmează a fi instalată

5.3.4 Managementul resurselor virtualizate

Soluția ofertată trebuie sa fie una unitară, integrată. Va include toate componentele necesare pentru a funcționa corect (baza de date, șabloane de management etc.) și a administra soluția propusa.

Componenta pentru provizionarea și managementul serviciilor IT în mediul virtualizat trebuie să ofere minim:

- Trebuie să ofere funcționalități pentru automatizarea creării, monitorizării și deployment-ului resurselor într-un Data Center;
- Trebuie să ofere funcționalități pentru automatizarea proceselor, a operațiunilor IT și conectarea diferitelor sisteme fără cunoașterea limbajelor de programare sau scriere de cod;
- Trebuie să ofere unelte de creare, testare, debugging și implementare a script-urilor într-o infrastructura eterogena;
- Trebuie să pună la dispoziția administratorilor o unealta grafica de creare a scripturilor;
- Trebuie să ofere posibilitatea realizării unei arhitecturi redundante prin implementarea mai multor servere pentru rularea automatizata a scripturilor;
- Se vor oferi conectori pentru integrarea cu platforme diferite de management: HP Service Manager, HP Operations Manager, HP iLO și OA, VMware vSphere, Representational State Transfer (REST), Sharepoint 2013, Active Directory, Exchange, System Center 2012 R2 Configuration Manager, System Center 2012 R2 Operations Manager, System Center 2012 R2 Data Protection Manager, System Center 2012 R2 Service Manager, System Center 2012 R2 Virtual Machine Manager, FTP, IBM Tivoli Netcool/OMNIbus etc.;
- Consola de editare a scripturilor trebuie sa ofere activități standard ce pot fi folosite pentru crearea scripturilor împreuna cu activități specifice fiecărui conector de integrare;

- Trebuie să ofere posibilitatea înlănțuirii de activități realizate din interfața grafica de design a scripturilor;
- Activitățile standard trebuie sa permită rularea scripturilor .Net, comenzi ssh sau monitorizare trap-uri SNMP, monitorizare servicii, monitorizare fișiere de log sau procese, monitorizare WMI, management fișiere;
- Prin conectorul de integrare cu soluția de management al datacenterului virtual, trebuie sa se poată proviziona mașini virtuale Windows și Linux pe baza template-urilor existente în consola respectiva;
- Prin conectorul cu soluția de service desk, trebuie sa se poate folosi scripturile din soluția de automatizare în activități de helpdesk dar și sa se poată crea obiecte în soluția de service desk;
- Trebuie să ofere suport pentru integrare conectori de la producători terți;
- Trebuie să ofere suport pentru stocarea scripturilor într-o baza de date relațională;
- Trebuie să ofere posibilitatea integrării cu un sistem de provizionare mașini virtuale integrate cu consola de management a datacenterului virtual;
- Trebuie să ofere un framework de integrare cu interfața grafica pentru provizionarea de servicii de cloud integrate cu soluția de management a datacenterului virtual;
- Trebuie sa poată rula mai multe scripturi în paralel;
- Trebuie să ofere consola web pentru administrarea scripturilor, accesibila printr-o conexiune criptata;
- Trebuie să ofere posibilitatea instalării pe un server fizic sau separarea modulelor componente ale soluției pe mai multe servere și asigurarea redundantei soluției;
- Trebuie să ofere Capabilități de check-in, check-out și testare pentru editarea, salvarea și testarea funcționării scripturilor;
- Trebuie să ofere posibilitatea integrării instrumente de calcul tabelar pentru vizualizarea sau crearea de rapoarte;

- Trebuie să ofere posibilități de realizare de log-uri în timp real ce oferă informații despre script-urile rulate;
- Trebuie să ofere log-uri istorice despre script-urile rulate;
- Trebuie să ofere log-uri istorice de audit;
- Trebuie să ofere log-uri de evenimente ale componentelor soluției
- Trebuie să ofere log-uri de audit și log-uri de diagnosticare;
- Trebuie să ofere un instrument de verificare a instalării soluției conform celor mai bune practici recomandate de producătorul soluției;
- Produsul trebuie sa fie livrat împreună cu baza de date necesară funcționarii sale corecte.

Componenta de monitorizare a aplicațiilor (sisteme de operare, middleware, baze de date) trebuie să ofere minim:

- Monitorizarea serverelor din cadrul datacenter-ului și alertare în cazul apariției unei erori, probleme de performanta, întrerupere în funcționare la nivel de aplicație, serviciu de aplicație, server, dispozitive de rețea (switch, routere, imprimante etc.);
- Posibilitatea de a lansa automat acțiuni de remediere în cazul apariției unei erori;
- Posibilitatea de a arhiva centralizat jurnalele de securitate ce conțin istoricul accesului utilizatorilor la servere;
- Administrarea evenimentelor de la sisteme de operare, printr-un jurnal de evenimente care colectează și raportează problemele și informațiile generate referitoare la sistemele și aplicațiile din rețeaua organizației;
- Administrarea evenimentele din: Red Hat Enterprise Server, centOS, Debian Linux, Ubuntu Linux, Oracle Linux, Suse Linux Enterprise Server, Windows, Oracle Solaris Server, IBM AIX Server, HP-UX Server.

- Monitorizarea switch-urilor, router-elor, imprimantelor și altor echipamente prin SNMP cu suport pentru SNMP v1,v2 sau v3; monitorizare virtual local area networks (VLAN) și grupuri Hot Standby Router Protocol (HSRP);

- Monitorizarea sistemelor Linux/Unix cu suport pentru RedHat Enterprise Server inclusiv versiunile 4, 5 și 6 (x86/x64), Suse Linux Enterprise Server inclusiv versiunile 9(x86), 10 SP1 (x86/x64),11 (x86/x64); Oracle Linux 5 și 6 (x86/x64), Ubuntu Linux Sever 10.04 și 12.04 (x86/x64), centOS Server 5 și 6 (x86/X64), Debian Linux 5, 6 și 7 (x86/x64); IBM AIX 5.3, 6.1 (POWER), 7.1 (POWER); HP UX versiuni 11i v2 și v3 (PA-RISC și IA64), Oracle Solaris inclusiv versiunile 9(SPARC), 10 (SPARC și x86), Solaris 11 (SPARC și x86).

- Monitorizarea proactivă și generarea de mesaje de avertizare prin capacitățile distribuite care urmăresc și monitorizează informațiile și trimit problemele la telefoane mobile, prin e-mail sau prin alte medii externe; Aceste avertizări trebuie sa poată lansa task-uri automate care sa duca la rezolvarea problemelor;

- Raportarea și analiza tendințelor, necesare pentru urmărirea problemelor în timp și generarea rapoartelor detaliate despre starea de funcționare generală a mediului administrat;

- Exportul rapoartelor în formate uzuale precum pdf, doc, etc.

- Include pachetele de management specifice pentru soluțiile ofertate;

- Monitorizarea avansata a aplicațiilor distribuite pe mai multe servere; monitorizarea aplicații .Net și Java cu suport pentru Apache Tomcat 5, 6 și 7, Java JDK 5 și 6, tehnologii Web cu suport pentru Generic Servlet, Struts, Struts2, Axis2

- Posibilitatea definirii în mod grafic a componentelor unui serviciu;

- Monitorizarea și raportarea evenimentelor, urmărirea nivelului de sănătate al sistemului

- Crearea unor rapoarte și alerte pentru administratori privind problemele cu impact asupra sistemelor și utilizatorilor;

- Bune practici pentru descoperirea, monitorizarea, depanarea și rezolvarea problemelor pentru o componenta specifica (sistem de operare, aplicație);

- Posibilitatea realizării unei comunicații autentificate și criptate intre serverul de management și agenți;
- Posibilitatea definirii nivele de securitate diferite și accesa separat consola de administrare;
- Monitorizarea aplicațiilor distribuite pe mai multe servere precum și definirea în mod grafic a componentelor unui serviciu;
- Monitorizează și raportează evenimentele, permite urmărirea nivelului de sănătate al sistemului precum și oferirea unui dashboard centralizat ce oferă informațiile critice despre resursele IT “business critical”;
- Integrare cu serviciul tip director astfel încât prin introducerea unui nou echipament intr-un grup organizațional, el sa fie automat detectat iar agentul de monitorizare automat instalat și configurat sa comunice cu serverul de monitorizare;
- Posibilitatea de a colecta jurnalele de securitate din sistemele de operare Windows/Linux/Unix și stocarea lor într-o baza de date separata;
- Posibilitatea de a colecta jurnale de securitate bazate pe Syslog.

Componenta pentru managementul configurațiilor mașinilor virtuale trebuie să ofere minim:

- Inventarierea tuturor aplicațiilor instalate pe stații de lucru și servere;
- Evidenta frecventei folosirii aplicațiilor de către utilizatori;
- Inventarierea componentelor hardware ale serverelor cu posibilitatea de a construi rapoarte cu istoricul schimbării acestor componente;
- Posibilitatea de a automatiza instalarea sistemelor de operare și aplicațiilor pe servere;
- posibilitatea de a defini în mod grafic toți pașii necesari instalării automate a unei imagini de sistem de operare, pornind de la partiționare și formatare hard disk, alegere ediție sistem de operare, alegere aplicații instalate, injectare drivere pentru sistemul de operare;
- Instalarea centralizata a actualizărilor și a service pack-urilor pentru sisteme de operare și aplicații;

- Posibilitatea impunerii unor șabloane de configurare software la nivelul serverelor pentru asigurarea conformității;
- Managementul dispozitivelor mobile: telefoane mobile sau tablete;
- Managementul și instalarea automatizata a aplicațiilor pe dispozitivele mobile;
- Integrarea nativa cu sistemul de securizare antivirus al stațiilor de lucru și al serverelor pentru administrare dintr-o singura consola;
- Integrarea cu platforma de tip director;
- Criptarea comunicației intre agenți și servere folosind certificate digitale;
- Definirea de roluri pentru administrator și operatorii care administrează soluția cu posibilitatea de integrare a permisiunilor de acces cu platforma de tip director;
- Suport pentru colectare de date pentru clienți chiar în cazul în care clienții nu au conexiune online cu serverul de management, colectările individuale putând fi executate și raportările trimise în momentul când conexiunea cu serverul de management este restabilita.
- Posibilitatea de a face management pentru stații de lucru și servere care nu fac parte dintr-un domeniu;
- Integrare cu tehnologia de protecție a rețelei organizației prin implementarea unui sistem de control al accesului bazat pe politici și folosirea conceptelor de zona de carantina;
- Suport pentru arhitecturi distribuite și pentru managementul stațiilor de lucru și serverelor aflate în diverse locații de la nivel central prin implementarea unei arhitecturi ierarhice parinte- copil intre serverele de management din organizație;
- Inventarierea tuturor aplicațiilor instalate pe stații de lucru și servere;
- Informațiile colectate de la clienți sa fie folosite pentru raportare sa fie stocate într-o baza de date relațională (SGBD);
- Posibilitatea realizării evidentei frecventei folosirii aplicațiilor de către utilizatori;

- Suport pentru monitorizarea aplicațiilor instalate pe stațiile de lucru dar și a aplicațiilor care rulează pe stațiile de lucru fără a fi instalate;
- Suport pentru raportarea și determinarea momentelor din zi când o aplicație este intens folosita
- Suport pentru determinarea exacta a licențelor folosite în organizație prin rapoarte inteligente.
- Posibilitatea de extragere a informațiilor din baza de date relaționale (SGBD) pentru rapoarte complexe despre utilizarea aplicațiilor dar și posibilitatea de a customiza asemenea rapoarte.
- Posibilitatea inventarierii componentelor hardware ale serverelor cu posibilitatea de construi rapoarte cu istoricul schimbării acestor componente;
- Posibilitatea de a vizualiza datele complete de inventariere pentru computerele individuale. Vizualizarea computerelor individuale poate fi folosita atunci când se detectează de la distanţă probleme la nivelul computerului.
- Posibilitatea de management a dispozitivelor inteligente cu sisteme de operare mobile (cu sisteme de operare Windows Mobile, Symbian, Android sau Apple iOS);
- Posibilitatea de a automatiza instalarea sistemelor de operare;
- Posibilitatea de a automatiza instalarea aplicațiilor pe stații de lucru, servere și dispozitive mobile;
- Suport pentru instalare automatizata a sistemelor de operare de tip Windows folosind un format de imagine care nu depinde de arhitectura hardware prin care o singura imagine se poate folosi pentru mai multe platforme hardware.
- Integrare cu tehnologia de patch management Windows Server Updates Services (WSUS) și posibilitatea de creare de replici locale pentru serverele de management care vor permite instalarea de patch-uri și update-uri pentru sistemele de operare acestea fiind aprobate la nivel central al serverului de management părinte.
- Posibilitatea de a defini în mod grafic toți pașii necesari instalării automate a unei imagini de sistem de operare de tip Windows, pornind de la partiționare și formatare hard disk,

alegere ediție sistem de operare, alegere aplicații instalate, injectare drivere pentru sistemul de operare;

- Posibilitatea de a crea automatizat de la nivelul consolei de management mijloace media bootable precum set de CD sau DVD-uri bootabile pentru instalarea automatizata a sistemelor de operare și aplicațiilor;
- Posibilitatea de migrare automatizata a stațiilor de lucru cu salvarea automata și restaurarea documentelor și setărilor utilizatorului;
- Posibilitatea folosirii de pachete pentru derularea aplicaţiilor software; un singur pachet poate conţine mai multe programe, fiecare configurat pentru a rula în mod diferit;
- Posibilitatea impunerii unor șabloane de configurare software la nivelul serverelor pentru asigurarea conformității;
- Suport pentru colectarea informațiilor despre conformitate pentru clienți pentru cazurile în care clienții nu au conexiune online cu serverul de management și trimiterea raportărilor în momentul când conexiunea este restabilita,
- Posibilitatea remedierii neconformităţii cu distribuţia software care asigură computerelor pachete software sau script-uri, utilizând o colectare care este populată automat cu computere ce raportează neconformitatea;
- Posibilitatea administrării de la distanţă a computerelor folosind o consola de acces la distanta care permite utilizatorului logat la stația respectiva sa vadă orice acțiune se desfășoară la nivelul sistemului accesat de către administrator;
- Posibilitatea de a cunoaște informații despre serverele din infrastructura, chiar daca acestea sunt oprite
- Portal web pentru provizionarea automata de software;
- Posibilitatea administrării prin politici a soluției de antivirus.

Componenta pentru managementul sistemului de virtualizare trebuie să ofere minim:

- Managementul centralizat al tuturor mașinilor virtuale și gazdelor fizice bazate pe, VMWare Infrastructure 4.1, 5.0 sau 5.1, Windows Hyper-V și Citrix XEN 6.0 și 6.1 cu posibilitatea de provizionare, stocare și plasare din consola de VMM pe hosturile ESX sau XEN;
- Monitorizarea stării de sănătate și utilizare la nivel de gazde fizice și mașini virtuale;
- Monitorizarea proactiva a mașinilor virtuale, gazdelor fizice precum și a aplicațiilor ce rulează în mașinile virtuale;
- Suport pentru migrare de tip “live” a mașinilor virtuale și migrare de tip “live” pentru storage pentru migrarea online a mașinilor virtuale intre host-uri sau dispozitive de stocare;
- Suport pentru clustere cu minim 64 de noduri, management pentru minim 1000 de hosturi și pana la 25.000 de mașini virtuale;
- Scenarii de consolidare a serverelor și conversia serverelor fizice în servere virtuale fără întreruperea accesului utilizatorilor la acestea și fără costuri adiționale
- Integrarare cu soluția de actualizare automata oferita pentru procesul de patch management al mașinilor virtuale;
- Suporte în zona de networking pentru configurații de tip Site-to-Site și suport pentru Network Virtualization ce folosește Generic Routing Encapsulation (NVGRE) și integrare cu switch-uri TOR (top-of-rack);
- Suport pentru mașini virtuale de generația 2, discuri diferențiale, clonarea mașinilor virtuale în timp ce sunt pornite, modificarea online a discurilor VHDX ale mașinilor virtuale;
- Integrare și management pentru dispozitive de stocare ce suporta standardele SMI-S , SMP sau soluții de stocare bazate pe sisteme file server și protocol SMB 3.0;
- Posibilitatea de administrare și clasificare a dispozitivelor de stocare;
- Posibilitatea de administrare dinamica a mașinilor virtuale cu mutarea acestora automata pentru asigurarea performantei maxime a acestora;

- Permite optimizarea consumului de curent electric al sistemelor virtuale;
- Optimizarea resurselor hardware, simplificare management și scăderea costurilor legate de achiziții hardware, spațiu, curent electric și climatizare;
- Plasarea inteligenta a mașinilor virtuale pe gazdele fizice în funcție de necesarul resurselor hardware precum și monitorizarea inteligenta a resurselor consumate de acestea;
- Simplificarea managementului serverelor, a salvării și restaurării datelor în caz de dezastru;
- Integrare cu tehnologii de patch management pentru mașinile virtuale inclusa în consola de management
- Suport pentru șabloane de securitate și determinarea conformității pentru sistemele virtuale
- Provizionare servere de la „bare metal”;
- Suport pentru scenarii cloud și definirea de resurse de calcul, de rețea sau stocare;
- Suport pentru scenarii de cloud și utilizarea aplicațiilor cu definirea de praguri pentru calculul costurilor;
- Suport pentru profile de server de aplicații (de exemplu Web Server, DB server);
- Suport pentru definirea de servicii cu aplicații de tip „multiple tier”, printr-un designer de servicii;
- Posibilitatea de automatizare a provizionarii mașinilor virtuale prin profile de mașini virtuale cu sisteme de operare Windows sau Linux;
- Suport pentru sisteme: Redhat Linux, Suse Linux , CentOS, Oracle Linux, Debian Linux, Windows Server;
- Suport pentru instalarea de aplicații virtuale pe servere și suport pentru Windows Server 2003 R2, 2008, 2008 R2, 2012;

- Suport pentru instalarea consolei în arhitectura de înalta disponibilitate pentru asigurarea redundantei;
- Suport pentru definirea rolurilor pentru asigurarea accesului securizat la resursele virtuale de tip cloud sau host.

Componenta pentru optimizarea performanței și capacităților sistemului trebuie să ofere minim:

- Management centralizat al incidentelor IT, schimbărilor de configurații, administrarea activelor IT, conformitate;
- Posibilitatea pentru utilizatori sa creeze tichete pentru raportarea și rezolvarea rapida a incidentelor sau altor probleme (solicitări de schimbare a configurației);
- Posibilitatea colectării automate de pe servere și stațiile de lucru Windows a problemelor și alertelor și consolidarea lor ca incidente;
- O baza de date de cunoștințe de tip „knowledge base" pentru rezolvarea rapida a problemelor precum și data warehouse, raportare centralizata și rapoarte detaliate pentru toate Capabilitățile tehnologiei;
- Integrare cu servicii de tip director, suport single-sign-on astfel încât sa nu solicite extinderea schemei existente și pentru a avea un impact minim asupra serviciului de director;
- Funcționare fără agenți pentru a nu încărca suplimentar sistemele desktop sau server la care se asigura suport prin intermediul componentei;
- Management centralizat al incidentelor IT cu oferirea unui portal pentru utilizatori pentru raportarea rapida a problemelor, incidentelor sau altor solicitări (de schimbare a configurației hardware, software);
- Un portal pentru helpdesk și administrare pentru rezolvarea rapida a problemelor sau incidentelor raportate de utilizatori sau a incidentelor provenite de la stațiile de lucru și a serverelor din rețea;

- Servicii automate pentru utilizatorii care doresc să obţină tichete, astfel încât să poată sa verifice starea tichetelor, să caute soluţii în baza de cunoştinţe etc.;
- Criptarea prin folosirea SSL a conexiunilor către portal;
- O baza de date CMDB care sa permită popularea sa automata pe baza conectorilor oferiți nativ;
- Posibilitatea funcționarii printr-o conexiune de tip VPN;
- Conectori pentru integrare cu servicii de tip director și cu componentele soluției de management oferite;
- Importul automat al datelor de inventariere hardware, software și securitate.
- Capacitatea de a salva, proteja şi raporta o configurație hardware și software a unui activ IT.
- Integrare cu componenta de monitorizare astfel încât sa poate importa informații despre activele IT monitorizate precum și alertele la nivelul acestora;
- Permite validarea câmpurilor în formularele de incidente;
- Capacitatea de a furniza un panou de bord personalizabil, care conţine un rezumat al incidentelor recente (în special care afişează incidentele critice);
- Posibilitatea customizarii formularelor de incidente sau al cererilor de schimbare a configurației;
- O harta a serviciilor și a legăturilor intre componentele unei aplicații distribuite prin integrarea cu componenta de monitorizare;
- Stocarea de șabloane de configurație şi istoricul configurațiilor pentru comparaţie şi audit;
- Gestionarea manuală a activelor prin importul manual din fișiere predefinite (ex.CSV);
- Gestionarea manuală a activelor ce nu pot fi recunoscute prin intermediul reţelei (ex. monitorizează camerele digitale, faxurile, etc.);
- Proiectarea şi distribuirea schimbărilor de configurație;

- Capabilitatea de a utiliza instrumente de diagnosticare (de ex. ping, tracert etc.);
- Posibilitatea selectării/introducerii de metadate (adică – tipul schimbării, zona schimbării, zona procesului, aplicaţia dacă este cazul, infrastructura vs. aplicaţiile, zona procesului, aprobatorul, proiect/incident, coordonator etc.);
- Un mediu de programare pentru crearea unor conectori particulari pentru integrarea cu alte soluții;
- Informații pentru rezolvarea rapida a problemelor precum și pentru raportare centralizata și rapoarte exhaustive pentru toate Capabilitățile tehnologiei;
- Posibilitatea stocării incidentelor și problemelor recurente împreună cu soluţia în baza de cunoştinţe
- Rapoarte și indicatori de tip KPI (Key Performance indicators);
- Posibilitatea livrării rapoartelor prin email, web, portal, în consola, sau pe un director de fișiere partajat;
- Capacitatea de a raporta măsurătorile SLA și de performanţă pe baza tipului tichetului (mai precis, solicitare de incident, de servicii), a zonei, pentru o durată specificată, etc.
- Facilitarea generării de rapoarte flexibile și producerea unor formate de raportare comune (.csv, .xls, .txt, .pdf).

Componenta pentru recuperare date trebuie să ofere minim:

- Posibilitatea de a efectua back-up la nivel de date, server, sistem de operare și mașini virtuale la un interval minim de 15 minute, fără întreruperea accesului utilizatorilor la acestea;
- Posibilitatea de a efectua back-up disk-to-disk și disk-to-tape;
- Posibilitatea de a efectua ușor restaurarea datelor în caz de dezastru;
- Posibilitatea restaurării serverelor dintr-o singura operație, fără a fi necesara reinstalarea sistemului de operare, aplicației și datelor succesiv;

- Suport pentru backup pentru sisteme de operare;
- Permite backup pentru baza de date ofertata cu restaurare în locația originala fără a fi necesare cunoștințe avansate de SQL pentru operator; la sfârșitul operațiunii baza de date va fi montată și disponibilă;
- Restaurare în locații alternative pe același server fără a perturba utilizatorii bazei de date în lucru;
- Permite restaurarea bazei de date pe un alt server;
- Suport pentru protecția server-elor de fișiere ce utilizează Resilient File System (ReFS);
- Posibilitatea de a realiza backup la nivel de date, server, sistem de operare și mașini virtuale bazate pe la un interval minim de 15 minute, fără întreruperea accesului utilizatorilor la acestea;
- Salvare și restaurare bare metal pentru mediile virtuale standalone sau cluster;
- Protecție și backup pentru mașinile virtuale de tip Windows Server sau Linux server în timp ce mașina virtuala este pornita;
- Protecție și backup-ul pentru host-urile oferite în soluție;
- Posibilitatea de a avea arhitecturi de backup redundante prin folosirea unor servere de backup în locațiile de disaster recovery care sa ofere backup pentru serverul de backup din locația primara;
- Posibilitatea de a face backup pentru clienți din domenii de tip director diferite sau workgroupuri și sa permită autentificarea cu certificate pentru acești clienți;
- Posibilitatea de a face backup pentru clienți protejați de firewall;
- Protecția volumelor unui server ce are activata capabilitatea de deduplicare;
- Posibilitatea de a face backup pentru clienți accesibili prin VPN cu suport pentru următoarele tipuri de protocol VPN Point-to-Point Tunneling Protocol (PPTP), Secure Socket Tunneling Protocol, (SSTP), Layer 2 Tunneling Protocol (L2TP);
- Integrare cu tehnologia VSS – Volume Shadow Service;

- Rapoarte locale și consolidate asupra întregului mediu de backup cat și a operațiunilor de backup;
- Back-up disk-to-disk și disk-to-tape;
- Oferă o consola centralizata pentru managementul dintr-o singura consola a mai multor servere de backup;
- Suporta instalarea întregii soluții în mediul virtualizat.

5.4 Cerințe privind securitatea sistemului

Infrastructura sistemului va trebui să asigure prevenirea și detectarea intruziunilor din exterior.

Este necesar ca sistemul să poată garanta delimitarea mediilor virtuale oferite în regim IaaS (Infrastructure as a Service), astfel încât utilizatorii acestora să aibă siguranța că aceste medii nu vor fi afectate de alte medii virtuale existente în platforma cloud.

Vor fi elaborate și implementate politici stricte de control al accesului, cu înregistrarea (jurnalizarea) evenimentelor de acces la sistem, aplicații și date, astfel încât să poată fi auditat sistemul din perspectiva accesării acestuia.

Sistemul va trebui să expună exclusiv canale de comunicații criptate (prin https) pentru datele cu caracter sensibil, cum ar fi datele de autentificare etc.

Confidențialitatea datelor va fi asigurată prin politicile de securitate (control al accesului) ce vor fi implementate. Aceste politici vor avea obiectivul de a oferi siguranța că datele vor putea fi citite/consultate doar de către utilizatori care au căpătat în mod explicit drept de acces în acest sens.

Sistemul va trebui să implementeze canale de comunicație criptate care să prevină interceptarea transferurilor de date cu caracter sensibil.

5.5 Cerințe de integrare hardware-software

Componentele sistemului informatic vor fi astfel proiectate astfel încât să asigure o integrare completă la nivel hardware-software. Astfel, toate componentele sistemului informatic vor utiliza

tehnologii standardizate, atât la nivel hardware cât și software. Prin soluția aleasă și propusă, ofertantul va asigura compatibilitatea între configuraţiile hardware solicitate, platforma de virtualizare, sistemele de operare şi software-ul de aplicaţie care va rula pe aceste echipamente.

Ofertanții se vor asigura și vor garanta beneficiarului faptul că versiunile diferitelor aplicații software instalate sunt compatibile între ele.

5.6 Cerinţe de performanţă

Din punct de vedere al performanței, calității și fiabilității, soluția propusă trebuie sa satisfacă următoarele cerințe minime și obligatorii:

- Să fie o soluție integrată de infrastructură de suport care să asigure atingerea unui factor PUE (Power Usage Effectiveness) mediu sub 1,6 pentru Centrul de date.
- Sa asigure performanța și eficiența energetică pentru întreaga infrastructură de suport, atât pentru sistemul electric cât și pentru cel de răcire, într-o plajă largă de variație a încărcării de putere IT, specifică sistemelor High-performance computing (HPC).
- Platforma pentru infrastructura de suport a Centrului de date trebuie să asigure un grad crescut de flexibilitate, astfel încât eventuale noi cerințe ale beneficiarului să poată fi ușor aplicate.
- Pentru asigurarea unui nivel corespunzător de disponibilitate și fiabilitate a soluției oferite se solicită în mod obligatoriu satisfacerea următoarelor cerințe:
    - posibilitatea de a se asigura upgrade la redundanță 2N pentru echipamentele din sistemul electric și sistemul de răcire,
    - alarmare (anunțare) în timp real a defectelor,
    - atenționare cu privire la necesitatea efectuării mentenanței preventive a echipamentelor, la atingerea limitei de operare sau la deteriorarea parametrilor operaționali,

- posibilitatea de a se înlocui module sau subansamble defecte fără a fi necesară întreruperea operării Centrului de date.

5.6.1 Cerințe de disponibilitate

Sistemul ofertat va respecta următoarele cerințe de disponibilitate:

- Arhitectura utilizată va include facilități de scalabilitate atât la nivelul infrastructurii hardware cat și software.
- Datele cu care operează aplicaţiile vor fi stocate numai centralizat, pe echipamentul (echipamentele) special prevăzut(e) în acest sens, resursele de stocare date.
- Resursele de stocare a datelor vor utiliza facilităţi de redundanţă atât la nivelul componentelor (surse de alimentare, ventilatoare) cât și la nivelul stocării datelor (prin utilizarea unor discuri de tip hot-swap şi prin implementarea unor matrice de tip RAID care oferă redundanţă în cazul defectării unor discuri).
- Având în vedere faptul că toate datele disponibile în cadrul sistemului informatic sunt stocate în cadrul sistemului de stocare a datelor, disponibilitatea acestuia este critică pentru funcţionarea întregului sistem.
- Pentru gestiunea situaţiilor în care defectele la sistemul de stocare a datelor sunt critice și nu mai permit recuperarea datelor, a fost prevăzută în cadrul acestui proiect achiziţionarea unui echipament pentru realizarea copiilor de siguranţă pe bandă magnetică, împreună cu aplicaţia software specifică. Echipamentul prevăzut este de tip „tape library”, care permite realizarea copiilor de siguranţă pe mai multe benzi, fără a fi necesară intervenţia administratorului de sistem pentru schimbarea unei benzi atunci când spaţiul maxim de stocare al acesteia a fost atins.

Sistemul va fi utilizat 24 de ore din 24, zilnic.

Procentul de disponibilitate a sistemului va fi astfel (cerințele sunt cumulative):

- 91,67% zilnic (calculat la 24 de ore) – maxim 2 ore de indisponibilitate zilnică
- 98,89% lunar (calculat la 30 de zile) – maxim 8 ore de indisponibilitate lunară
- 99,79% anual (calculat la 365 de zile) – maxim 32 de ore de indisponibilitate anuală.

5.6.2 Cerințe de scalabilitate

Arhitectura hardware va fi astfel proiectată încât să permită creşterea capacităţii de procesare a sistemului prin adăugarea de noi servere. Mecanismele de load-balancing implementate la nivel de aplicație/echipamente de rețea trebuie să permită echilibrarea utilizării resurselor hardware

în funcţie de evoluţia numărului de solicitări concurente, prin adăugarea de noi resurse (servere fizice/virtuale, memorie, capacitate de procesare etc.), în funcție de necesităţi.

De asemenea, la nivel de storage soluția aleasa trebuie să permită adăugarea de noi incinte de instalare a discurilor, care să mărească capacitatea de stocare a acesteia.

Din punct de vedere al bazelor de date, scalabilitatea va fi dată de posibilităţile de upgrade hardware ale nodurilor de cluster.

5.6.3 Cerinţe privind timpii de răspuns

La dimensionarea componentelor hardware şi software ale soluţiei se va avea în vedere asigurarea premizelor pentru obţinerea unor criterii de performanţă care să asigure eficienţa activităţilor derulate de utilizatori. Astfel, timpii de răspuns ai sistemului informatic la solicitări standard de acces la informaţie sau de scriere de informaţii nu vor depăşi câteva secunde (maxim 3 secunde), la o încărcare maximă a sistemului. Pentru obţinerea rapoartelor operaţionale zilnice, timpii de răspuns nu vor depăşi 20 de secunde. Pentru rapoarte statistice și de istoric, se vor asigura mijloace tehnice pentru minimizarea tipului de aşteptare al utilizatorilor (de exemplu segmentarea cantităţii de date returnate și popularea ecranului cu primul set de date fără a aştepta transmiterea întregului set de date etc.)

6 CERINȚE PRIVIND SERVICIILE SOLICITATE

6.1 Servicii de management de proiect

6.1.1 Informații generale

Autoritatea contractantă dorește achiziționarea unor servicii profesionale de management de proiect care să acompanieze activitățile de implementare tehnică a proiectului ICIPRO și care să asigure cadrul metodologic necesar atât pentru implementarea cu succes a proiectului, cât și pentru respectarea cu strictețe a prevederilor contractului de finanțare.

Pe lângă asigurarea consultanței necesare autorității contractante pentru managementul eficient al procesului de implementare, furnizorul selectat va avea și sarcina de a asigure transferul de cunoştinţe în domeniul managementului de proiect către membrii echipei de proiect a autorității contractante.

Managementul de proiect (managementul contractului de finanțare) reprezintă procesul de coordonare, organizare și gestionare a activităţilor interdependente și a resurselor alocate din cadrul Proiectului, pentru a asigura atingerea obiectivelor stabilite la standardele de calitate propuse, în condiţiile existenţei unor constrângeri referitoare la timp, resurse şi costuri.

Managementul de proiect este o activitate permanentă, care se va derula pe întreaga perioadă de desfăşurare a proiectului (18 luni). În primele 6 luni de implementare a Proiectului, managementul contractului de finanțare este asigurat de echipa de management de proiect a Beneficiarului. După atribuirea contractului aferent acestei proceduri de atribuire (conform acestui caiet de sarcini), responsabilitatea principală pentru realizarea activităților de management de proiect și de monitorizare a derulării contractului de finanțare va fi asumată de către furnizorul selectat în cadrul prezentei proceduri de atribuire, care va colabora însă în acest scop cu echipele de management și tehnică a autorității contractante.

6.1.2 Organizarea structurii de management de proiect

În vederea implementării cu succes a proiectului, autoritatea contractantă a organizat atât o unitate tehnică de implementare a proiectului, cât și o echipă proprie de management.

În sprijinul echipei de management a Autorității Contractante, Prestatorul va organiza și va furniza o echipă de experți care va avea ca principală sarcină managementul contractului de finanțare. Responsabilitățile experților care, în mod minimal, trebuie să compună echipa furnizorului care va realiza managementul contractului de finanțare, sunt prezentate in cele ce urmează:

1. MANAGER DE PROIECT

- Monitorizează implementarea contractului de finanțare;

- Monitorizează implementarea tuturor sarcinilor contractuale ale ofertantului;
- Punct principal de contact pentru comunicarea cu Beneficiarul;
- Elaborează planul revizuit de activităţi și identifica principalele jaloane (milestones) ale proiectului;
- Elaborează Rapoartele de progres și le înaintează spre aprobare;
- Monitorizează managementul financiar, incluzând verificarea cheltuielilor;
- Elaborează sistemul de arhivare a documentelor şi asigura pistei de audit aferente;
- Asigură asistenţă în elaborarea cererilor de rambursare;
- Asigură accesul la documentaţia proiectului în vederea realizării auditurilor financiare şi tehnice parţiale şi finale;
- Asigură transfer de cunoştinţe și formare specifice de management de proiect către echipa de implementare a Beneficiarului.

2. MANAGER FINANCIAR

- Elaborează, împreună cu responsabilul financiar al beneficiarului, planul de cheltuieli al Proiectului;
- Verifica disponibilitatea resurselor financiare necesare iniţierii proiectului;
- Verifica cheltuielile;
- Verifica aspectele financiare ale contractelor de achiziţii publice;
- Elaborează dosarul de rambursare;
- Contribuie la elaborarea rapoartelor de progres;
- Asigură accesul la documentaţia financiar-contabilă pentru auditorul extern;
- Asigură transfer de cunoştinţe specifice de management financiar către echipa de implementare a Beneficiarului;

- Informează membrii echipei de implementare a beneficiarului în legătura cu procedurile financiare care trebuie respectate pe perioada implementării proiectului;
- Asigură consultanța financiară în implementarea proiectului
- Verifică corectitudinea documentelor justificative de plată din cadrul proiectului.

3. EXPERT IT 1

- Participa la recepţia echipamentelor hardware achiziţionate și monitorizează implementarea serviciilor de instalare;
- Monitorizează activităţile de implementare a soluţiei software achiziţionate;
- Asigură suport echipei de implementare a Beneficiarului privind implementarea soluției integrate de cloud computing;
- Asigură suport echipei responsabile cu implementarea activității de management al contractului de finanțare în privința aspectelor tehnice legate de soluția informatica și caracteristicile soluției de tip cloud implementata.

4. EXPERT IT 2

- Participa la recepţia echipamentelor hardware achiziţionate și se asigură ca acestea respectă cerințele documentației de atribuire, precum și cerințele minime legale în domeniul calității;
- Monitorizează activităţile de implementare a soluţiei software achiziţionate și se asigură ca soluția implementată respectă cerințele documentației de atribuire precum și cerințele minime legale în domeniul calității;
- Monitorizează procesul de prestare a serviciilor de amenajare a datacenter-ului;
- Asistă Beneficiarul la recepția lucrărilor de amenajare datacenter;

- Asigură suport echipei de implementare a Beneficiarului pe parcursul implementării Proiectului;
- Monitorizează implementarea soluției informatice, astfel încât să corespundă, din punct de vedere calitativ și funcțional, necesităților Beneficiarului.

6.1.3 Activități și responsabilități ale furnizorului în vederea asigurării serviciilor de consultanță pentru managementul de proiect și al contractului de finanțare

Etapele și activitățile pe care Prestatorul va trebui să le realizeze în vederea atingerii rezultatelor prevăzute pentru activitatea de management al contractului de finanțare sunt după cum urmează:

6.1.3.1 Managementul financiar al proiectului

Pentru gestionarea eficientă a bugetului alocat, până la rambursarea sumelor solicitate, se va elabora un registru de cheltuieli pentru înscrierea cronologică a tuturor cheltuielilor efectuate, defalcate în cheltuieli eligibile și cheltuieli neeligibile, precum și a detaliilor documentelor justificative și a datelor efectuării plăţilor. De asemenea, vor fi elaborate toate cererile de plată din cadrul proiectului, cererile de rambursare, conform calendarului de rambursare al contractului de finanțare, precum și toate raportările financiare solicitate de către OIPSI. În cazul în care calendarul proiectului sau al cererilor de rambursare va suferi modificări, atunci cererile de plată/rambursare vor fi realizate în funcție de noile date prevăzute în proiect. De asemenea, în cazul în care perioada de implementare a proiectului se va prelungi, atunci și responsabilitățile Furnizorului se vor prelungi în mod similar, pe toată perioada de implementare a proiectului. Dosarul de rambursare va fi pregătit în conformitate cu cerinţele specificate în contract și va conţine toate documentele justificative necesare verificării eligibilităţii cheltuielilor efectuate.

- Principalele activitățile de care Furnizorul va fi responsabil în acest context sunt următoarele:

- elaborarea unui registru de cheltuieli pentru înscrierea cronologică a tuturor cheltuielilor efectuate, defalcate în cheltuieli eligibile și cheltuieli neeligibile, precum și a detaliilor

documentelor justificative și a datelor efectuării plăţilor. Registrul va fi actualizat în permanență și va fi predat autorității contractante împreună cu fiecare raport lunar de activitate al furnizorului, aferent serviciilor de consultanță pentru managementul proiectului

- elaborarea și întreținerea permanentă a unui raport financiar de tip cash-flow (flux de numerar), care să prezinte o planificare financiară completă a proiectului, pe întreaga perioadă de implementare a acestuia și care să conțină toate cheltuielile și veniturile proiectului (aferente cererilor de plată și cererilor de rambursare), cu planificarea în timp a acestora conform graficului de execuție al proiectului și graficului de rambursare, ținând cont de termenele legale de rambursare a cheltuielilor. Raportul va fi actualizat în permanență și va fi transmis autorității contractante împreună cu fiecare raport lunar de activitate al furnizorului, aferent serviciilor de consultanță pentru managementul proiectului. Raportul va semnala orice risc de natură financiară, datorat deviațiilor de la planul aprobat inițial (întârzierea unor activități ale proiectului, devansarea unor activități ale proiectului – cu impact asupra necesității de asigurare a resurselor financiare pentru plată anticipată – și întârzierea onorării cererilor de plată și a cererilor de rambursare de către OPISI.

- elaborarea cererilor de plată în conformitate cu cerinţele specificate în contract, conţinând toate documentele justificative necesare verificării eligibilităţii cheltuielilor efectuate. Vor fi elaborate cel puțin 8 cereri de plată.

- elaborarea cererilor de rambursare și pregătirea dosarului de rambursare în conformitate cu cerinţele specificate în contract, conţinând toate documentele justificative necesare verificării eligibilităţii cheltuielilor efectuate. Vor fi elaborate cel puțin 3 cereri de rambursare: 2 cereri intermediare în lunile 10, 15 de implementare a proiectului, respectiv o cerere de rambursare finală în luna 18 de proiect. În funcție de tipul cheltuielilor incluse în fiecare cerere de rambursare, furnizorul va transmite autorității contractante, în timp util, un checklist conținând tipurile de documente justificative pe care autoritatea contractantă trebuie să le furnizeze în susținerea cheltuielilor eligibile solicitate spre rambursare. De asemenea, furnizorul va răspunde tuturor cererilor de clarificare primite din partea OIPSI cu privire la cererile de rambursare, până la rambursarea efectivă a acestor cheltuieli.

- elaborarea justificărilor financiare necesare pentru susținerea unor eventuale acte adiționale la contractul de finanțare, în special datorită unor deviații care pot apărea între prețurile la care se realizează achiziția unor bunuri și servicii și costul bugetat al acestora.
- elaborarea notificărilor privind eventualele modificări cu privire la modificarea graficului cererilor de plată sau de rambursare
- elaborarea tuturor rapoartelor financiare ale proiectului;
- verificarea tuturor documentelor de plată depuse în cadrul contractelor proiectului, din punct de vedere al: corectitudinii întocmirii, respectării ofertelor financiare și respectării bugetului proiectului;
- Toate documentele și rapoartele vor fi elaborate astfel încât să se asigure respectarea cerințelor legale și a celor contractuale cu privire la termenele care trebuie respectate pentru aceste raportări. Este în responsabilitatea Furnizorului să gestioneze calendarul obligațiilor autorității contractante din perspectiva contractului de finanțare și să atenționeze autoritatea contractantă din timp cu privire la scadența acestor obligații. De asemenea, furnizorul va preda documentele întocmite în timp util pentru a permite autorității contractante studierea acestora și aprobarea înainte de transmiterea lor către finanțatorul proiectului.

6.1.3.2 Elaborarea rapoartelor de progres

Rapoartele elaborate vor respecta întocmai cerinţele prevăzute în Ghidul Solicitantului și în contractul de finanţare semnat cu OIPSI și vor fi depuse în termenele stabilite conform contractului de finanțare, împreună cu celelalte documente solicitate în mod expres în contractul de finanţare. Rapoartele de progres vor fi predate autorității contractante în timp util pentru a permite autorității contractante studierea acestora și aprobarea înainte de transmiterea lor către finanțatorul proiectului.

Principalele activitățile de care Furnizorul va fi responsabil în acest context sunt următoarele:

- elaborarea rapoartelor de progres intermediare și finale. Prestatorul va elabora toate rapoartele trimestriale de progres, precum și un raport final, în ultima lună de proiect. În

cazul în care datorită modificărilor graficului de rambursare datele de depunere a cererilor de rambursare nu se vor suprapune cu perioadele trimestriale la care trebuie elaborate rapoartele de progres, atunci se vor elabora și rapoarte de progres care vor însoți cererile de rambursare și care se vor referi la perioadele pentru care se solicită rambursarea cheltuielilor. De asemenea, în cazul în care va fi necesară prelungirea perioadei de implementare a proiectului, atunci se vor elabora și rapoartele de progres suplimentare aferente perioadei de prelungire a proiectului.

- pe lângă rapoartele trimestriale de progres solicitate de OIPSI, furnizorul va pregăti și va transmite autorității contractante și rapoarte lunare de progres, cu două componente: evoluție generală a implementării proiectului și respectiv descrierea tuturor activităților aferente componentei de servicii de management de proiect realizate in luna respectiva. Acest raport lunar va fi însoțit de celelalte rapoarte solicitate explicit: registru de cheltuieli, raport financiar de cash flow etc.

6.1.3.3 Arhivarea documentelor aferente proiectului

Conform regulamentelor comunitare, circuitul auditului (pista de audit) reprezintă stabilirea fluxurilor informaţiilor, atribuţiile și responsabilităţile referitoare la acestea, precum şi arhivarea documentaţiei justificative complete pentru toate stadiile desfăşurării unei acţiuni, care să permită totodată reconstituirea operaţiunilor de la suma totală până la detalii individuale şi invers. Pista de audit este deci o înregistrare cronologică a activităţilor din proiect pentru a permite reconstrucţia şi examinarea succesiunii de evenimente şi/sau schimbări.

Principalele activitățile de care Furnizorul va fi responsabil în acest context sunt următoarele:

- elaborarea unei proceduri de organizare și păstrare a documentelor, pe categorii
- monitorizarea respectării de către autoritatea contractantă a procedurii de organizare și de păstrare a documentelor
- asigurarea respectării modalității de documentare a proiectului, astfel: documentele elaborate în cadrul proiectului vor fi păstrate conform următoarei reguli: 1 exemplar original şi 1 copie în format fizic, cât și în variantă electronică;

- rapoartele, cererile de rambursare şi alte documente oficiale solicitate de către OIPSI vor fi elaborate în original şi în numărul de copii stabilite prin contractul de finanţare, care vor fi predate la OIPSI, câte o copie certificată a acestora păstrându-se la sediul proiectului;
- arhivarea documentelor proiectului se va face la finalizarea proiectului; cutiile cu dosarele complete cu documentele în original vor fi păstrate într-un spaţiu protejat, împreună cu un CD/DVD cu toate documentele scanate, acesta rămânând la locaţia proiectului pe perioada legală de arhivare și păstrare (5 ani post-implementare).
- la finalul proiectului, furnizorul va avea responsabilitatea realizării unui OPIS al tuturor documentelor din arhiva proiectului, OPIS care va permite regăsirea facilă a documentelor în cadrul arhivei fizice.

6.1.3.4 Monitorizarea activităţilor proiectului

Monitorizarea este acel proces ce permite obţinerea informaţiilor necesare pentru cunoaşterea şi înţelegerea stadiului proiectului la un moment dat, precum şi tendinţele de derulare a activităţilor incluse în proiect. Monitorizarea se va face fie prin discuţii cu personalul implicat în derularea proiectului, fie prin înregistrarea rezultatelor şi a problemelor apărute, fie prin observarea activităţilor derulate. Monitorizarea se va face pe tot parcursul desfăşurării proiectului (18 luni). Monitorizarea proiectului va permite cunoașterea stadiului la zi a evoluției implementării și va oferi informațiile necesare realizării obligațiilor de raportare. Activitatea de monitorizare se va baza în mod exclusiv pe date cuantificabile, pe indicatori și surse de verificare agreate în prealabil şi pe baza termenelor şi a condiţiilor prevăzute în alte documente elaborate în cadrul proiectului.

Principalele activitățile de care Furnizorul va fi responsabil în acest context sunt următoarele:

- planificarea activităţilor şi implementarea proiectului în conformitate cu prevederile din Cererea de finanțare aprobată și din Contractul de finanţare;
- elaborarea în primele 15 zile de la semnarea contractului a unui plan detaliat al activităților contractului de finanțare, obținut prin integrarea planurilor de activități

aferente tuturor contractelor din cadrul proiectului (implementare și management de proiect, vizibilitate și publicitate, audit tehnic, audit financiar). Acest plan va cuprinde totalitatea activităților proiectului finanțat și va constitui baza pentru raportarea ulterioară a evoluției proiectului. Planul va conține atât activități de ordin tehnic, cât și activități de management (raportare, ședințe, activități financiare – inclusiv elaborarea cererilor de rambursare). Planul va include jaloane de timp pentru activitățile care marchează finalul unor etape importante ale proiectului. De asemenea, pentru toate activitățile care produc livrabile (echipamente, aplicații, rapoarte de servicii etc.) care necesită aprobarea autorității contractante, se vor marca explicit în plan termenele obligatorii pentru finalizarea activității de către responsabilul de activitate, precum și termenele pentru avizarea de către autoritatea contractantă a livrabilelor, astfel încât să se asigure respectarea termenelor obligatorii asumate prin graficul cererii/contractului de finanțare.

- monitorizarea executării activităţilor proiectului, evidenţa utilizării resurselor proiectului și obţinerea rezultatelor preconizate. Pe lângă activitățile de monitorizare ad-hoc, se vor organiza ședințe periodice (cel puțin lunare) de evaluare a stadiului implementării proiectului. Aceste ședințe sunt suplimentare ședințelor tehnice ale echipelor de implementare și vor avea ca participanți membrii echipelor de management ale autorității contractante și furnizorului. Furnizorul va documenta toate aceste ședințe în minute de ședință și va elabora și întreține un registru de acțiuni în care se vor înscrie activitățile stabilite în urma ședințelor, termenele de realizare și responsabilii. În cazul identificării unor situaţii neprevăzute care pot apărea pe parcursul desfășurării proiectului și care necesită o soluţionare urgentă, se vor convoca ședințe ad-hoc ale echipelor de management, în vederea soluționării situațiilor apărute.

- monitorizarea permanentă a gradului de realizare a indicatorilor proiectului și semnalarea imediată a oricărei situații care ar putea determina neatingerea acestor indicatori.

- prezentarea lunară a graficului de activități (planului de activități) actualizat, cu marcarea progresului înregistrat și cu marcarea eventualelor deviații față de planul aprobat.

- monitorizarea financiară, ce va urmări utilizarea corectă a fondurilor, modul de efectuare a plăţilor, încadrarea în prevederile capitolelor bugetare de cheltuieli ale proiectului. Se vor organiza lunar ședințe de analiză a bugetului și a fluxului de numerar al proiectului. În situaţia identificării unor diferenţe faţă de bugetul planificat, se vor analiza cauzele și se vor face recomandări pentru remedierea situației.

- managementul riscurilor (identificare, analiză, planificare, urmărire) prin întreţinerea unui Registru de Riscuri și planificarea măsurilor de prevenire și reducere a impactului riscurilor;

- managementul calităţii prin întreţinerea unui Registru de Calitate în care să se înscrie toate problemele apărute pe durata derulării proiectului (în cadrul testelor de acceptanţă) și prin urmărirea rezolvării acestor probleme. Registrul de Calitate actualizat va fi prezentat lunar autorității contractante, împreună cu raportul lunar de progres și de activitate.

- managementul schimbării – pregătirea şi aplicarea unei proceduri de tratare a cererilor de schimbare prin care să se asigure introducerea controlată a schimbărilor în cadrul ciclului de analiză-proiectare-dezvoltare-implementare-testare-acceptanţă;

- diagnoza proiectului (tratarea excepțiilor) pentru a vedea, în cazul apariţiei unor probleme de implementare, care sunt noile soluţii necesare continuării implementării.

- acordarea de sprijin în rezolvarea aspectelor administrative asociate contractului de finanţare, cum ar fi elaborarea unor notificări, solicitări pentru elaborarea actelor adiţionale, clarificări, modificări de grafic de execuţie sau grafic de rambursare etc.;

6.1.3.5 Verificarea respectării regulilor de vizibilitate și publicitate

Furnizorul va fi responsabil, pe întreaga perioadă de derulare a proiectului, de monitorizarea realizării măsurilor de vizibilitate și publicitate a proiectului, conform prevederilor contractului de finanțare. De asemenea, furnizorul va oferi puncte de vedere autorității contractante cu privire la materialele de vizibilitate și publicitate realizate în cadrul proiectului, în sensul verificării corectitudinii informațiilor și a respectării regulilor din manualul de vizibilitate aferent POS CCE.

6.1.4 Alte responsabilități ale furnizorului de servicii de consultanţă pentru realizarea managementului proiectului și al contractului de finanțare

Pe lângă responsabilităţile specifice ale furnizorului, detaliate anterior, acesta va avea și următoarele responsabilități de ordin general:

- execuţia la timp a activităţilor stabilite în contract, în colaborare cu reprezentanții autorității contractante. În acest sens, furnizorul va solicita din timp orice informații îi sunt necesare pentru îndeplinirea sarcinilor sale contractuale.

- Acordarea de sprijin proactiv autorității contractante pentru implementarea în condiţii optime a proiectului, cât şi furnizarea de know-how general în domeniul managementului de proiect, prin prezenţa să ori de câte ori este nevoie la locaţia proiectului, ceea ce va acţiona și în direcţia consolidării competenţelor echipei de proiect a autorității contractante în sfera managementului de proiect;

- gestionarea contractului de implementare şi asigurarea legăturii cu celelalte contracte din cadrul proiectului prin raportarea la celelalte activităţi ale proiectului, astfel încât acesta din urmă să fie implementat conform Contractului de finanţare;

- furnizarea, în timp util, a informaţiilor necesare autorității contractante cu privire la derularea proiectului. Furnizorul își va asuma responsabilitatea pentru pregătirea tuturor documentelor, materialelor, redactării de documente clare și solicitări precise de date, indicând data la care aşteaptă informaţiile solicitate, luând în calcul timpul de răspuns necesar pentru Beneficiar, astfel încât să nu se afecteze suplimentar programul de lucru al Beneficiarului și, respectiv, implementarea contractului conform calendarului stabilit;

- elaborarea tuturor documentelor cu respectarea cerinţelor prevăzute de Contractul de finanţare, Ghidul solicitantului și legislaţia în domeniu;

- organizarea, planificarea, execuţia şi monitorizarea proiectului, atât din punct de vedere tehnic, financiar, al vizibilităţii proiectului, cât şi al activităţilor de elaborare a cererilor de rambursare şi a documentaţiei aferente acestora, inclusiv elaborarea rapoartelor de progres în conformitate cu Ghidul Solicitantului;

- informarea de urgenţă a Beneficiarului cu privire la orice eveniment sau circumstanţe ce împiedica execuţia la timp și eficientă a sarcinilor sale.

6.1.5 Criterii de calitate pentru serviciile de consultanţă pentru realizarea managementului proiectului și al contractului de finanțare

Prin prestarea serviciilor solicitate, furnizorul va asigura respectarea următoarelor criterii de calitate:

- livrarea documentelor şi a rapoartelor necesare la timp, respectând cerințele impuse de Ghidul Solicitantului, Contractul de Finanţare şi anexele sale, procedurile europene, legislaţia românească relevantă, planul de activităţi și planul de jaloane (milestones);
- activităţile de informare/publicitate sunt implementate conform planului de informare/publicitate și în conformitate cu Manualul de Identitate Vizuală;
- rapoartele de progres pe baza rapoartelor de activitate ale proiectului, furnizate de către Consultant sunt aprobate de O.I.P.S.I.;
- cererile de plată și cele de rambursare sunt înaintate către O.I.P.S.I. în conformitate cu calendarul aprobat, toate clarificările solicitate de OIPSI sunt transmise la termenele solicitate, iar plăţile sunt efectuate şi certificate de Autoritatea de Certificare;
- calitatea transferului de know-how către echipa de proiect desemnată de autoritatea contractantă, prin evaluarea conţinutului materialelor prezentate în şedinţele periodice și a temelor propuse spre rezolvare membrilor echipei, precum și prin evaluarea post-implementare a prestaţiei echipei de proiect;

- transferul de cunoştinţe este corelat cu etapa specifică a implementării proiectului – echipa furnizorului va pregăti sesiuni de informare pentru a furniza informaţii relevante pentru fiecare etapă a proiectului;

- calitatea şi transparenţa sistemului de arhivare și înregistrare a informaţiilor va fi monitorizată prin evaluarea uşurinţei accesului specialiştilor care vor efectua auditurile tehnice și financiare parţiale şi finale la documente, echipamente și soluţii tehnologice.

6.1.6 Cerințe minime din punct de vedere al conținutului propunerii tehnice pentru serviciile de consultanţă pentru managementul proiectului și a contractului de finanțare

Ofertantul are obligația de a prezenta răspunsuri punctuale la toate cerinţele solicitate prin caietul de sarcini, care să arate modul concret în care vor realiza toate activităţile solicitate pentru managementul proiectului și contractului de finanțare.

Ofertantul trebuie să prezinte în cadrul ofertei cel puțin informații privind

- modalitatea de însuşire integrală a responsabilităţilor asociate activităţilor solicitate;
- viziunea proprie asupra realizării acestor activități, din care să reiasă modul în care a înţeles contextul și scopul acestora;
- prezentarea şi detalierea a cel puțin 5 aspecte considerate esenţiale de către ofertant pentru atingerea obiectivelor acestei activități;
- identificarea şi descrierea riscurilor care afectează execuţia activităților şi prezentarea unor soluţii viabile de răspuns la risc. Se vor prezenta cel puțin două riscuri pentru fiecare categorie de activități solicitată, așa cum acestea sunt descrise la Cap. 6.1.3, precum și cel puțin o măsură (recomandare) de diminuare/eliminare pentru fiecare risc identificat.
- prezentarea metodologiei de management de proiect utilizată, care trebuie să conțină cel puțin informații cu privire la: strategia de management de proiect utilizată, abordarea

proiectului privind prestarea serviciilor și realizarea activităților prevăzute în contract, activitățile de management ale proiectului, procesele de management de proiect, presupuneri și constrângeri în realizarea planului de management al proiectului, prezentarea echipei de proiect și organigrama proiectului. În cadrul metodologiei de management de proiect se vor prezenta cel puțin următoarele proceduri:

- managementul timpului, care trebuie să cuprindă cel puțin: lista de activități a proiectului, modul de urmărire în timp a activităților,

- managementul calităţii, care trebuie să cuprindă cel puțin: obiectivele de calitate ale proiectului, activitățile de asigurare și control al calității, registrul de calitate;

- managementul riscurilor, care trebuie să cuprindă cel puțin: identificarea și analiza riscurilor, definiţia probabilităţii și impactului, matricea de probabilitate și impact;

- managementul schimbării, care trebuie să cuprindă cel puțin: responsabilitățile în cadrul procesului de management al schimbării, fluxul de desfășurare al managementului schimbării;

- managementul comunicării, care trebuie să cuprindă cel puțin: părțile implicate în comunicare, modalitățile și principiile de comunicare în cadrul echipelor de proiect și între echipele de proiect, fluxurile majore de comunicare;

- managementul problemelor, care trebuie să cuprindă cel puțin: raportarea problemelor, procesul de tratare al problemelor;

- prezentarea metodologiei de monitorizare, evaluare și raportare ofertată, care să cuprindă cel puțin următoarele proceduri:

- monitorizarea prin rapoarte periodice de stare;

- monitorizarea prin rapoarte de excepţie în cazul depăşirii criteriilor planificate de timp, calitate sau buget;
- monitorizarea prin rapoarte financiare;
- monitorizarea căii critice;

- alte 3 proceduri relevante propuse de Ofertant pentru atingerea obiectivelor proiectului și serviciilor de consultanţă solicitate.

6.2 Servicii de implementare tehnică solicitate

6.2.1 Managementul implementării proiectului

6.2.1.1 Organizarea echipei tehnice de implementare

În vederea implementării cu succes a proiectului, ofertantul va organiza și va pune la dispoziția autorității contractante o echipă de experți care, prin atribuțiile și pregătirea lor, vor realiza managementul și execuția tuturor activităților tehnice specializate care trebuie realizate în cadrul proiectului.

Rolurile experților care, în mod minimal, trebuie să compună echipa de implementare a furnizorului, sunt prezentate în continuare:

1. COORDONATOR TEHNIC DE PROIECT

- Coordonează echipa tehnică de implementare a sistemului informatic pentru realizarea activităţilor de analiza, proiectare, dezvoltare, configurare, testare, implementare, integrare, instruire, suport;
- Colaborează cu factorii de răspundere, experții în materie și personalul implicat în proiect, pentru a defini arhitectura soluției informatice în conformitate cu strategia instituției, procesele, informațiile și tehnologia potrivit conceptelor arhitecturii de tip enterprise;
- Coordonează echipele tehnice de amenajare a datacenter-ului;
- Asigură corelarea interdisciplinara pentru definirea arhitecturii de sistem;
- Definește arhitectura de integrare a componentelor sistemului;

- Definește arhitectura de securitate a sistemului;
- Aplică principiile și practicile guvernanței IT;
- Identifică și monitorizează riscurile și problemele tehnice, precum și mecanismele de reacție și soluțiile de rezolvare a acestora.

2. EXPERT ANALIZĂ DE BUSINESS

- Asigură planificarea, monitorizarea și extragerea cerințelor de business, managementul și comunicarea cerințelor, analiza organizaționala și a cerințelor, evaluarea și validarea soluțiilor de business;
- Asigură analiza procedurilor și a regulamentului de organizare și funcționare al Beneficiarului în vederea stabilirii funcționalităților sistemului;
- Utilizează limbaje standardizate pentru descrierea specificațiilor software;
- Participa la ședințele de analiză cu responsabilii din partea Beneficiarului;
- Realizează documentația de analiză și specificațiile soluției;
- Realizează manualele de utilizare a soluției;
- Asigură suport pentru utilizatorii cheie din partea Beneficiarului în timpul testelor funcționale.

3. EXPERT TESTARE FUNCȚIONALĂ A SISTEMULUI

- Planifica activităţile de testare;
- Asigură testarea funcţionalităţilor sistemului implementat;
- Elaborează planurile, scenariile și cazurile de test;
- Livrează rapoartele de testare;
- Coordonarea activităţilor de testare ale echipei de testare;

- Realizează testele de acceptanţă specifice;
- Asigură funcţionarea corecta a sistemului din punct de vedere al respectării cerinţelor, consistenţei datelor, al constrângerilor de timp, al validărilor de date şi al gestiunii erorilor, inclusiv pentru funcţionalităţile existente care au fost extinse sau modificate.

4. EXPERT SECURITATE INFORMAȚIONALĂ ȘI PREVENIRE RISCURI

- Asigură securitatea proceselor și fluxurilor informaționale la nivelul sistemului implementat;
- Asigură identificarea, estimarea și evaluarea riscurilor, definirea mecanismelor de reacție împotriva riscurilor;
- Asigură proiectarea, implementarea, și urmărirea aplicării stricte a masurilor specifice obținerii transmisiilor sigure de informații;
- Planifica activităţile de testare în ceea ce privește asigurarea securității informaționale;
- Asigură identificarea și exploatarea controlata a vulnerabilităților informaționale, înainte de punerea în producție a soluției informatice.

5. EXPERT SECURITATE SISTEME INFORMATICE

- Asigură implementarea echipamentelor de securitate informatică;
- Asigură evaluarea sistemului implementat pentru conformitate cu standardele deschise de securitate informatică;
- Asigură planificarea activităţilor de testare în ceea ce privește asigurarea securității soluției;
- Asigură evaluarea vulnerabilităților sistemului implementat;
- Actualizează manualul de securitate și procedurile de securitate ale Beneficiarului;
- Identifică și asigura exploatarea controlata a vulnerabilităților sistemului înainte de punerea în producție;

- Realizează teste de penetrare pentru componentele expuse la Internet.

6. EXPERT INFRASTRUCTURĂ COMUNICAȚII

- Crează arhitectura echipamentelor de comunicații ale sistemului, luând în considerare echipamentele ofertate și reţeaua existentă la beneficiar;
- Contribuie la întocmirea planurilor de instalare și punere în funcţiune a sistemului;
- Instalează și configurează echipamentele de comunicații livrate;
- Supervizează funcţionarea echipamentelor în perioada testelor;
- Asigură securitatea rețelelor de comunicații implementate;
- Asigură suport pentru soluționarea problemelor tehnice pentru echipamentele de comunicații;
- Elaborează documentaţia cu privire la echipamentele de comunicații inclusiv a documentaţiei de administrare.

7. EXPERT INFRASTRUCTURĂ SOFTWARE DE TIP CLOUD

- Crează planul de instalare și configurare, având în vedere fluxurile și procesele de tehnologie din cadrul instituției și modalitatea în care resursele informatice trebuie organizate pentru atingerea performantei sistemului;
- Asistă la instalarea și configurarea platformelor software de bază ale sistemului;
- Monitorizează implementarea și integrarea platformei de gestiune a conținutului, astfel încât aceasta să permită înregistrarea documentelor împreună cu un set de atribute (metadate) care să faciliteze organizarea documentelor și regăsirea lor ulterioară;
- Asigură implementarea în bune condiții a soluției de cloud computing, având în vedere impactul și modificările cloud computing în managementul serviciilor informatice, precum și riscurile estimate, venind cu soluții de contracarare a acestora;

- Asigură suport pentru utilizatorii cheie din partea Beneficiarului în timpul testelor pentru a asigura funcţionarea software-ului de bază.

8. EXPERT SOLUȚII VIRTUALIZARE

- Asigură instalarea și configurarea sistemelor de operare și virtualizare ale soluției informatice;
- Asigură instalarea și configurarea soluției de management al resurselor virtualizate, și integrarea cu celelalte componente ale sistemului;
- Crează planul de instalare și configurare, având în vedere fluxurile și procesele de tehnologie din cadrul instituției și modalitatea în care resursele informatice trebuie organizate pentru atingerea performanței sistemului.

9. EXPERT ARHITECT INFRASTRUCTURĂ HARDWARE PENTRU SISTEME DE TIP CLOUD

- Crează arhitectura infrastructurii hardware de tip cloud a sistemului, luând în considerare echipamentele ofertate și reţeaua existentă la beneficiar;
- Contribuie la întocmirea planurilor de instalare și punere în funcţiune a sistemului;
- Instalează și configurează echipamentele hardware livrate;
- Supervizează funcţionarea echipamentelor în perioada testelor;
- Asigură suport pentru soluționarea problemelor tehnice pentru echipamentele hardware;
- Elaborează documentaţia cu privire la echipamentele hardware inclusiv a documentaţiei de administrare;
- Elaborează planul de instalare și configurare în raport cu constrângerile tehnice și corelat cu componente software ale sistemului, asigurând managementul serviciilor de tehnologie a informației;
- Asigură documentarea arhitecturii sistemului.

10. EXPERT PLATFORMĂ DE INTEGRARE

- Crează, împreună cu ceilalți membri ai echipei, planul de instalare și configurare a componentelor soluției informatice;
- Crează și implementează modele de integrare bazate pe servicii web;
- Monitorizează procesului de instalare a componentelor soluției informatice, asigurând integrarea tuturor componentelor, astfel încât soluția informatica implementata să asigure performanța sistemului.

11. EXPERT PLATFORMĂ DE GESTIUNE A UTILIZATORILOR

- Asigură planificarea și implementarea platformei pentru managementul utilizatorilor și a accesului la sistem;
- Asigură planificarea și implementarea metodelor de autentificare centralizată la toate componentele sistemului unde este necesar;
- Monitorizează procesului de instalare a componentelor soluției informatice, asigurând integrarea tuturor componentelor cu sistemul de gestiune al utilizatorilor, astfel încât soluția informatica implementata să asigure securitatea și performanța sistemului.

12. EXPERT SUPORT TEHNIC PENTRU SOLUȚII DE TIP CLOUD

- Asigură analiza, planificarea, administrarea, rezolvarea, monitorizarea progresului, prioritizarea cererilor de suport;
- Asigură rezolvarea cererilor de suport sau escaladarea acestora la un nivel superior pentru rezolvare;
- Identifica problemele şi propune soluţii pentru problemele identificate;
- Asigură asistentă în utilizarea corectă a soluției de tip cloud;
- Asigură suportul pentru baza de date a sistemului;

- Asigură buna funcționare a sistemului și se asigura ca resursele informatice sunt organizate astfel încât să fie atinsa performanta sistemului;
- Menţine în permanentă legătura cu clientul;
- Efectuează verificări periodice ale funcţionării sistemului.

13. PROIECTANT SISTEME DE SECURITATE

- Asigură proiectarea sistemelor de securitate fizica;
- Asigură elaborarea specificației tehnico-operative a sistemelor de securitate;
- Se asigura ca securitate trebuie să aplice prevederile legale referitoare la securitatea și sănătatea în muncă și în domeniul situațiilor de urgență.

14. INGINER SISTEME DE SECURITATE

- Organizează activitățile de instalare a sistemelor tehnice de securitate;
- Realizează sistemele tehnice de monitorizare;
- Asigură instruirea beneficiarului asupra utilizării și întreținerii sistemului;
- Responsabil cu asigurarea testării, evaluării și punerii în funcțiune a echipamentelor și sistemelor tehnice de detecție și semnalizare la efracție și control acces, a sistemelor tehnice de detectare, semnalizare și alarmare la incendiu.

15. TEHNICIAN SISTEME DE SECURITATE

- Asigură montarea și efectuarea cablajelor pentru echipamente de detecție, supraveghere video și control acces, diagnosticarea stării de funcționare a acestora;
- Realizează lucrările de montare a tubulaturii pentru sistemele tehnice de securitate;
- Asigură efectuarea lucrărilor de reparații la structurile afectate de montare / cablare.

16. TEHNICIAN SISTEME ȘI INSTALAȚII DETECȚIE INCENDIU

- Asigură instalarea, punerea în funcțiune și verificarea sistemelor și instalațiilor de semnalizare, alarmare și alerta în caz de incendiu;
- Asigură mentenanta sistemelor și instalațiilor de semnalizare, alarmare și alerta în caz de incendiu.

17. INGINER HVAC

- Asistă Beneficiarul la recepția echipamentelor HVAC;
- Asistă la activitățile de planificare a instalării sistemului HVAC;
- Monitorizează instalarea și punerea în funcțiune a sistemelor de ventilație.

6.2.1.2 Managementul activităților tehnice de implementare a furnizorului

În cadrul acestei secțiuni ne referim la activitățile de management de proiect aferente contractului de implementare a soluției tehnice corespunzătoare acestui proiect, activități care vor fi derulate intern în cadrul echipei furnizorului care va fi selectat prin această procedură de atribuire. Cerințele de management de proiect la nivelul întregului proiect finanțat (contract de finanțare) au fost prezentate anterior în cadrul secțiunii

Activitatea de Project Management trebuie să se desfăşoare conform unei metodologii recunoscute internațional de către organisme profesionale specifice de Project Management.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei de Project Management pe care o va utiliza în cadrul implementării proiectului.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice planul detaliat de prestare a serviciilor pe toată durata contractului. Planul de prestare a serviciilor trebuie să conţină, delimitat pe etape, toate serviciile solicitate.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice modalitatea în care se va realiza raportarea progresului pentru activităţile din cadrul proiectului. Se va detalia modul de raportare în ceea ce priveşte intervalele de raportare, formularele folosite, conţinutul informaţional al raportării precum şi circuitul de aprobare al raportărilor de progres.

Ofertantul trebuie să prezinte în cadrul proiectului modalitatea prin care se va realiza comunicarea între participanţii la proiect.

Ofertantul va prezenta în cadrul propunerii tehnice modul în care se vor rezolva problemele care pot să apară pe parcursul proiectului. Se vor prezenta procedurile și formularele care vor fi utilizate pentru managementul problemelor și escaladarea şi rezolvarea acestora.

Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanţă care va fi utilizat în cadrul proiectului pentru recepţiile/acceptanţele parţiale şi recepţia/acceptanţa finală. Se va prezenta planul împărţit pe etape precum şi formularele aferente recepţiilor/acceptanţelor parţiale şi recepţiei/acceptanţei finale.

Ofertantul va prezenta în cadrul propunerii tehnice și modalitatea de tratare a schimbărilor în cadrul proiectului (în limitele Caietului de Sarcini). Se va prezenta descrierea procedurii de management al schimbărilor precum și formularele care vor fi utilizate în cadrul acestui proces pe durata proiectului.

Ofertantul trebuie să îşi dimensioneze echipa de conducere a proiectului astfel încât, pe toată durata contractului, persoanele responsabile de derularea acestei activităţi să fie disponibile on-site în vederea derulării în condiţii optime a proiectului.

Oferta trebuie să includă un plan inițial de proiect cât mai detaliat posibil, care să răspundă cerințelor de etapizare și înscriere în termenele de realizare ale proiectului.

Implementarea întregului sistem trebuie să acopere următoarele etape:

- Analiza și proiectare
- Dezvoltare/configurare inclusiv testare interna
- Implementare
- Teste de acceptanta
- Intrarea în producție
- Asistenta tehnica și suport pentru perioada solicitata.

Planul inițial care va fi prezentat împreuna cu oferta trebuie să acopere toate etapele menționate mai sus.

6.2.2 Analiză și proiectare

În vederea implementării sistemului, Ofertantul va trebui să execute activităţi de analiză, proiectare și implementare desfășurate în cadrul instituției Beneficiarului.

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de analiză și proiectare și să prezinte împreuna cu oferta procedurile și instrucțiunile de lucru de analiza și proiectare implementate în cadrul propriei organizații.

Ofertanții trebuie să descrie instrumentele pe care le vor utiliza astfel încât să poată asigura:

- colectarea și evidența cerințelor

- acoperirea integrala a tematicii proiectului
- evidenţa modificărilor cerinţelor
- trasabilitatea cerinţelor pornind de la obiectivele proiectului până la specificaţiile tehnice.

Ofertanţii trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapelor de analiza şi proiectare. Descrierea trebuie să conţină cel puţin următoarele informaţii:

- formularul/formularele care vor fi utilizate pentru fiecare livrabil
- descrierea conţinutului fiecărui livrabil
- modul în care va fi interpretat conţinutul livrabilelor.

Analiza se va efectua la sediul Beneficiarului şi va avea ca finalitate un pachet de specificaţii funcţionale agreat de comun acord cu acesta.

Ca etape de analiza şi proiectare se vor avea în vedere:

- Analiza sistemului existent
    - Va consta în analiza situaţiei din momentul de faţă din cadrul instituţiei Beneficiarului prin şedinţe de analiză, chestionare etc., se vor identifica problemele pe care instituţia doreşte să le rezolve prin realizarea acestui proiect
    - Definirea cerinţelor informaţionale specifice, impuse de soluţia recomandată (identificarea utilizatorilor care au nevoie de informaţie, unde, când, în ce forma, ce conţinut.
- Proiectarea sistemului dorit
    - Vor fi detaliate cerinţele şi specificaţiile rezultate din faza de analiza pentru toate nivelurile şi componentele sistemului care va fi realizat
    - Se va stabili modelul de date
    - Se va prezenta:
        - arhitectura de sistem;
        - intrările/ieşirile în/din sistem structurate pe subsisteme (componente software) - pentru fiecare entitate (se specifică sursa/destinaţie, modalitate, canal de comunicare, volum, frecvenţa, observaţii);
        - descrierea componentelor de sistem, caracteristici funcţionale şi non-funcţionale;
    - Vor fi definite scenariile de integrare între diferitele sisteme

- Proiectarea sistemului oferă soluţia optima, urmărindu-se uşurinţa şi eficienţa realizării și implementării cerinţelor utilizatorului, în cadrul unor restricţii de ordin tehnic, organizatoric sau financiar. În procesul de proiectare implicarea utilizatorului este esenţială, în confirmarea cerinţelor informaţionale şi a priorităţilor din organizaţie, realizându-se în acest mod înţelegerea şi acceptanţa lui pentru noul sistem.

Ofertanții trebuie sa prezinte împreuna cu oferta procedurile și instrucțiunile de lucru de analiza și

proiectare pe care le vor utiliza în cadrul proiectului.

Ofertanții trebuie sa descrie instrumentele pe care le vor utiliza astfel încât sa poată asigura:

- colectarea și evidenta cerințelor
- acoperirea integrala a tematicii proiectului
- evidenta modificărilor cerințelor
- trasabilitatea cerințelor pornind de la obiectivele proiectului pana la specificațiile tehnice
- modelarea proceselor și activităților în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent).

Ofertanții trebuie sa prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapelor de analiza și proiectare. Descrierea trebuie sa conțină cel puțin următoarele informații:

- formularul/formularele care va fi utilizate pentru fiecare livrabil
- descrierea conținutului fiecărui livrabil
- modul în care va fi interpretat conținutul livrabilelor.

6.2.2.1 Etape generale

Rolul principal al fazei de analiză și elaborare a specificaţiilor este de a înţelege corect nevoile utilizatorilor, înainte de proiectarea şi implementarea unui sistem care să le îndeplinească.

Datele de intrare sunt:

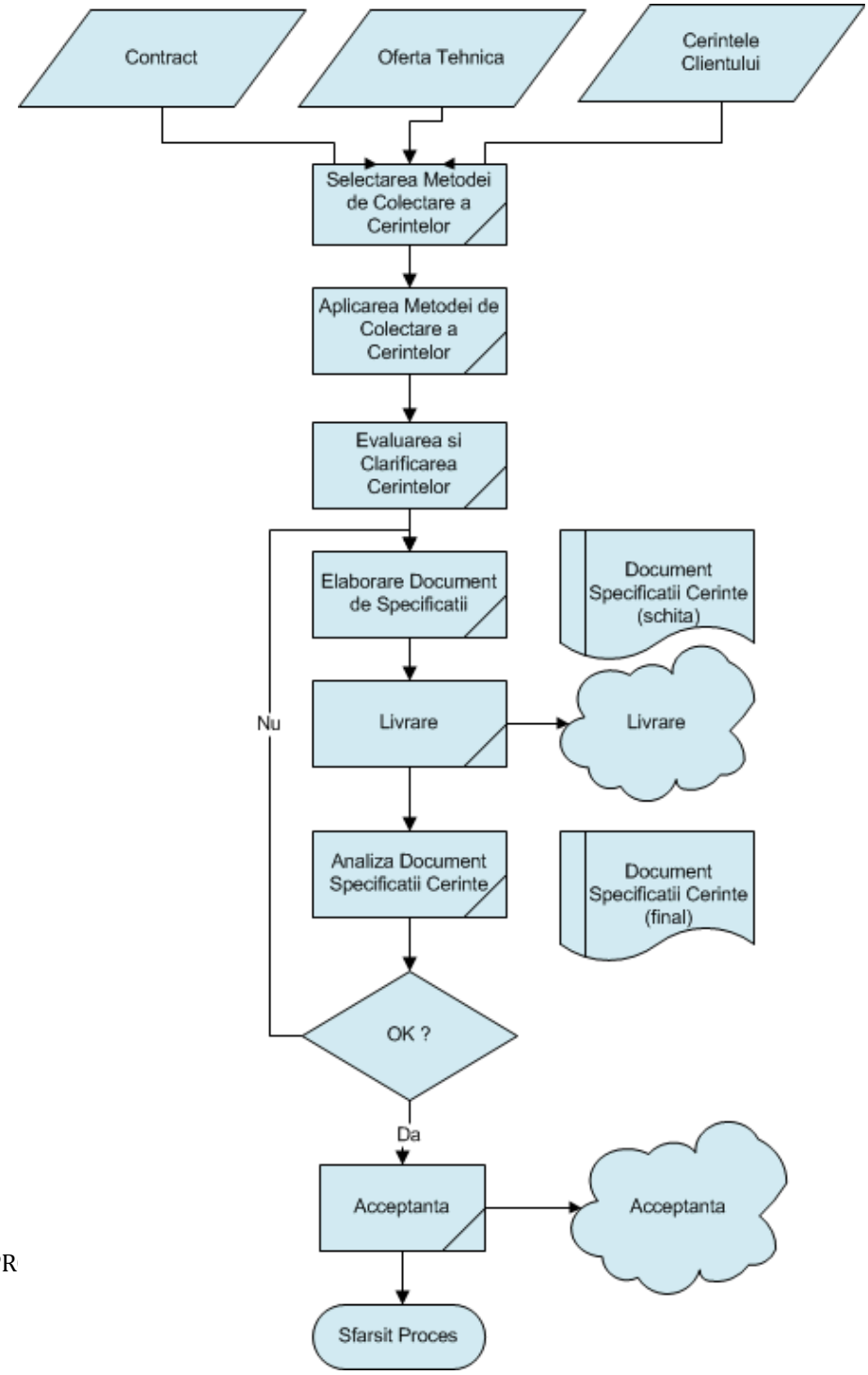
- Contractul, pentru termene și condiţii
- Propunerea tehnică, pentru aria de acoperire a proiectului
- Cerinţele clientului colectate și evaluate în timpul aceste faze.

Procesul constă din următoarele faze :

- Alegerea metodei de colectare a cerinţelor
- Aplicarea metodei alese de colectare a cerinţelor

- Evaluarea şi clarificarea cerinţelor
- Elaborarea specificaţiilor corespunzătoare cerinţelor
- Analizarea specificaţiilor corespunzătoare cerinţelor împreună cu clientul
- Aprobarea specificaţiilor corespunzătoare cerinţelor.

Procesul este reprezentat în figura de mai jos – **Fluxul Procesului de Analiză și Proiectare.**



6.2.2.2 Etape specifice

În faza de analiza se va ţine cont de cel puţin următoarele etape:

- *Stabilirea modelului de securitate*

1. Tipuri de utilizatori
2. Roluri
3. Grupuri – maparea peste organigrama existenta
4. Excepţii
5. Drepturi

- *Structura organizațională*

În scopul optimizării procesului de analiză a fluxurilor de lucru este necesar ca structura organizaţionala a instituţiei să fie foarte bine cunoscută de către furnizor şi stocată la nivelul aplicaţiei.

6.2.2.3 Analiza proceselor

6.2.2.3.1 Identificarea proceselor de lucru ce urmează a fi implementate

Se va întocmi o listă cu procesele ce urmează a fi automatizate.

6.2.2.3.2 Identificare cazuri de utilizare - Use cases

Use case diagram este un tip de diagramă din care reiese modul de utilizare a sistemului informatic - modul în care utilizatorii interacţionează cu acesta (în corespondenţă directă cu task-urile acestor utilizatori.). Utilizarea *use case diagram* nu este absolut necesară pentru a scrie o specificaţie cu use case-uri, dar este utilă pentru a crea o imagine generală asupra sistemului.

6.2.2.3.3 Identificarea actorilor

Se vor identifica actorii pentru toate fluxurile din pasul anterior. Se vor identifica și consemna rolurile generale gen: şef departament, director direcţie etc.

Pentru specificarea actorilor umani este de preferat să se folosească alias-uri în locul numelor de utilizatori/grupuri. Acest mod de abordare oferă o serie de avantaje printre care: dinamicitatea fluxurilor de lucru, elimina nevoia de a modifica fluxurile în cazul schimbărilor de persoane.

6.2.2.3.4 Identificarea paşilor

Se vor identifica:

1. Paşii manuali
2. Paşii automaţi

3. Deciziile
4. Notificările
5. Ramurile executate în paralel (punctele de split)
6. Punctele de reconectare (join)
7. Condiţiile de încetare a unui flux
8. Condiţiile de repornire a unui flux (manual/automat)

6.2.3 Dezvoltare/configurare și testare interna

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de dezvoltare/configurare și testare interna și vor demonstra integrarea acestor proceduri cu procedurile de analiza și proiectare.

Ofertanții trebuie să prezinte împreuna cu oferta procedurile și instrucțiunile de lucru de dezvoltare/configurare și testare interna implementate în cadrul propriei organizații

Ofertanții trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapelor de dezvoltare/configurare și testare interna.

6.2.4 Implementare

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de implementare.

Ofertanții trebuie să prezinte împreună cu oferta procedurile și instrucțiunile de lucru de implementare din cadrul propriei organizații și vor demonstra integrarea acestor proceduri cu procedurile referitoare la dezvoltare/configurare și testare internă.

Ofertanții trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de implementare. Descrierea trebuie să conțină cel puțin următoarele informații:

- formularul/formularele care vor fi utilizate pentru fiecare livrabil
- descrierea conținutului fiecărui livrabil
- modul în care va fi interpretat conținutul livrabilelor.

6.2.5 Testarea și asigurarea calității

Ofertantul trebuie să descrie cum va realiza monitorizarea evoluției proiectului și să descrie criteriile de calitate urmărite pe perioada desfășurării proiectului.

Ofertantul va descrie tipul și frecvența rapoartelor de monitorizare a evoluției proiectului.

Ofertantul trebuie să descrie modalitatea în care va realiza testele de acceptanță specifice.

6.2.5.1 Teste preliminare

Beneficiarul va realiza împreună cu reprezentanți ai Furnizorului teste asupra tuturor componentelor livrate în conformitate cu instrucțiunile de instalare și folosire. Criteriul de succes îl reprezintă trecerea cu succes a tuturor testelor și verificărilor recomandate de producător. După instalarea cu succes a tuturor

echipamentelor precum și a procedurilor de lucru livrate și după testele preliminare, se va semna un certificat de instalare.

6.2.5.2 Teste operaționale

Beneficiarul (cu asistența Furnizorului) va realiza toate testele pe întregul sistem și pe componentele acestuia în conformitate cu Planul de Teste realizat de Furnizor și agreat de Beneficiar.

Planul de testare va cuprinde cel puțin următoarele tipuri de teste:

- Testare unitară – se verifică în întregime logica individuală a fiecărui subsistem, se verifică respectarea de către fiecare modul a cerințelor funcționale evidențiate în documentele predate. Criteriu de succes – Subsistemul trece toate testele funcționale.
- Testarea sistemului integrat – se verifica faptul că sistemul funcționează corect din punct de vedere al consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor. Criteriul de succes – Sistemul trece toate testele funcționale.

Planul de testare de nivel înalt va fi prezentat odată cu oferta. Planul detaliat de testare, însoțit de scenariile de testare, va fi realizat de către Furnizor și aprobat de Beneficiar în perioada de analiză.

6.2.6 Teste de acceptanță

Ofertanții vor prezenta în detaliu metodologia și procedurile după care vor derula activitățile specifice de testare de acceptanta. Metodologia va fi adaptată specificului acestui proiect.

Ofertanții vor demonstra că metodologia propusă și procedurile pe care le vor utiliza acoperă integral tematica proiectului astfel încât să fie posibila testarea tuturor funcționalităților identificate în etapa de analiză și proiectare.

6.2.7 Intrarea în producție

Ofertanții trebuie să prezinte planul care va fi utilizat la trecerea în producție a sistemului.

Planul prezentat trebuie să țină cont de legăturile logice între subsisteme astfel încât să se asigure o trecere în producție coerentă. De asemenea, se va ține cont de asigurarea disponibilității serviciilor oferite în acest moment de către ICI și care vor fi migrate pe noua infrastructură.

6.2.8 Asistență tehnică și suport

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de asistenta tehnica și suport post-implementare.

Ofertanții trebuie să prezinte împreună cu oferta procedurile și instrucțiunile de lucru de asistență tehnică și suport pe care le vor utiliza în cadrul contractului.

Ofertanții trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de asistență tehnică și suport. Descrierea trebuie să conțină cel puțin următoarele informații:

- formularul/formularele care vor fi utilizate pentru fiecare livrabil

- descrierea conținutului fiecărui livrabil
- modul în care va fi interpretat conținutul livrabilelor

Serviciile de suport și mentenanță software vor deveni operaționale încă de la intrarea în producție a sistemului ofertat. Sistemul de suport va asigura, dar nu se va limita la următoarele tipuri de probleme:

- Optimizarea utilizării sistemului
- Întrebări de natură tehnică post implementare
- Preluare de bug-uri (erori la nivel software)
- Ajutor în raportare

Pentru gestionarea activității de suport în perioada de garanție, Furnizorul trebuie să pună la dispoziția Beneficiarului o aplicație software de gestionare a tichetelor. Aplicația va avea următoarele caracteristici:

- înregistrarea solicitărilor de suport și alocarea unui identificator unic fiecărei solicitări;
- posibilitatea de definire a unor categorii de apeluri de asistență;
- posibilitatea de definire și de încadrare a solicitărilor în categorii: defect, eroare, solicitare de informații, cerere de schimbare.
- posibilitatea de înregistrare a datelor de identificare ale apelantului - include atribuirea incidentului unei persoane care raportează în aplicația software (inginerul de suport), persoana care soluționează incidentul (de la orice nivel), persoana care a raportat un incident. Toate datele prezente aici includ atât date personale, cât și date de contact, activitate curentă etc., aceasta aplicație putând fi personalizata să primească detalii diferite pentru aceste puncte de reper în mod diferit și definit în totalitate de către un administrator de aplicație.
- posibilitatea de înregistrare a descrierii problemei și de atașare a unor documente suplimentare. Aplicația software să permită atașarea oricăror tipuri de fișiere (doc, xls, jpg, xml etc.) precum și postarea a unor capturi de ecran din aplicații.
- posibilitatea de alocare a unui criteriu de urgență. Aplicația software să permită clasificarea incidentelor în funcție de tipul stabilit, putând să emită notificări pe mail privind alocarea incidentelor către persoanele implicate în incident.
- posibilitatea de alocare automata a unor coduri de incident care să indice cauza probabilă a incidentului. Aplicația software să aloce coduri unice fiecărui incident. Aplicația software să permită de asemenea și gruparea pe module a incidentelor.
- posibilitatea de gestionare a informațiilor despre personalul de suport căruia i se pot aloca spre rezolvare incidentele. Aplicația software conține implicit toate datele de contact și deci persoanele, care pot fi considerate alocabile sau care pot aloca un incident. Aceste date pot fi folosite în mod facil în cazul unui audit.

- înregistrarea automată a datei și a orei primirii unei solicitări de asistență.
- posibilitatea de definire a criteriilor de calitate și performanta pentru rezolvarea diferitelor categorii de solicitări de asistență.
- posibilitatea de atenționare automată în momentul depășirii unor praguri temporale de rezolvare a diferitelor categorii de solicitări de asistență.
- posibilitatea de definire a unor fluxuri de evoluție a solicitărilor de suport, în cazul în care ele trec prin mai multe nivele de competență până în momentul finalizării.
- posibilitatea de escaladare a cererilor de suport.
- posibilitatea de înregistrare a datelor de contact pentru responsabilii pentru activitățile de suport de nivel 1, 2 și 3 pentru diferitele componente ale sistemului informatic.
- posibilitatea de definire a unor rapoarte personalizate folosind criterii cum ar fi: tipul de incident, nivelul de urgență, timpul de rezolvare, persoana și locația de unde a fost semnalat un incident, modulul sau funcția care a cauzat incidentul, numărul de incidente, etc.
- ofertantul va include certificările personalului ce va opera aplicația pentru înregistrarea și urmărirea evenimentelor, din care să reiasă ca personalul ofertantului a fost instruit și este certificat de producător să utilizeze aplicațiile.
- sa permită în orice moment accesul la baza de date a personalului autorizat al sistemului pentru verificarea modului de tratare a incidentelor și pentru rularea de rapoarte de performanță a serviciului de suport. Accesul se va face numai pentru citire și nu va fi condiționat în niciun fel de către operatorii sau administratorii serviciului.

6.2.9 Asigurarea și controlul al calităţii pe durata proiectului

Ofertantul trebuie să prezinte în cadrul propunerii tehnice o descriere a procedurilor de asigurare și control al calităţii aplicabile proceselor pe care le va utiliza în cadrul contractului.

Ofertantul trebuie să aloce în planul de proiect timpi suficienţi de verificare și validare din punct de vedere calitativ pentru serviciile prestate în cadrul contractului și pentru livrabilele/documentele rezultate. Ofertantul va lua în considerare necesitatea prestării unui număr corespunzător de zile-om pe durata proiectului, de către personalul specializat în asigurarea şi controlul calităţii.

Trebuie să fie incluse în oferta următoarele proceduri de lucru: Procedura de asistență tehnică, mentenanță și suport, Procedura de livrare, Procedura de acceptanță, Procedura de ședințe, Procedura de management al schimbării, Procedura de dezvoltare, Procedura de analiza și design, Procedura de analiza generala, Procedura de analiza detaliata, Procedura de control al livrărilor, Procedura de testare a livrabilelor soft, Procedura de implementare, Procedura de control al înregistrărilor, Procedura de control al produsului neconform. Neprezentarea în oferta a acestor documente va duce la respingerea ofertei.

Ofertanții trebuie să includă în oferta și varianta preliminară a planului de calitate pentru derularea proiectului. Planul de calitate trebuie să conțină cel puțin următoarele informații:

- descrierea fazelor, etapelor și activităților din cadrul proiectului
- descrierea pachetelor de lucru și a livrabilelor rezultate în urma prestării serviciilor
- descrierea criteriilor de acceptanta pentru livrabile, pachete de lucru, faze, etape, etc.
- formulare care vor fi utilizate în cadrul proiectului

6.3 Servicii de amenajare pentru datacenter

Pentru a se putea asigura un mediu de funcționare de nivel profesional ridicat pentru componentele TIC, proiectul are în vedere amenajarea unui spațiu tehnic (centru de date) la un nivel profesional ridicat, în măsură să asigure alimentarea corespunzătoare cu energie electrică, climatul necesar, securitatea fizică, prevenirea și protecția împotriva incendiilor și controlul accesului fizic al persoanelor la echipamentele de tip server incluse în proiect.

Centrul de date necesar proiectului va fi amenajat într-un spațiu modular dispus pe două nivele într-o clădire special construită și amenajată. Sunt puse la dispoziție următoarele spații modulare destinate găzduirii echipamentelor IT și de comunicații (atât cele achiziționate prin proiect cât și cele viitoare):

- Un modul de 53m^2 capacitate 23 rackuri
- Un modul de 53m^2 capacitate 20 rackuri
- Un modul de 69m^2 capacitate 25 de rackuri
- Un modul de 69m^2 capacitate 22 rackuri
- Un modul de 69m^2 capacitate 25 rackuri
- Un modul de 27m^2 capacitate de 8 rackuri

Toate aceste module sunt situate în subsolul unei clădiri în construcție cu destinație finală DataCenter, fiind concepută pentru a suporta toate cerințele tehnice specifice unei astfel de destinații. Împărțirea modulară este data de către pereții despărțitori și structura de rezistență a clădirii. Planurile spațiilor DataCenter-ului care prezintă relevanță pentru proiect sunt disponibile spre consultare la sediul autorității contractante. De asemenea, spațiile care fac obiectul amenajării se pot vizita, în baza unei solicitări scrise adresate autorității contractante și a unei planificări comunicate de către autoritatea contractantă tuturor ofertanților care și-au manifestat interesul în acest sens. Astfel, solicitările de vizitare vor fi transmise către Autoritatea contractantă în termen de maxim 2 săptămâni de la data publicării documentaţiei de atribuire în SEAP, iar Autoritatea contractantă va programa aceste vizite și va informa ofertanții interesați cu privire la data programată pentru vizită.

- Pentru găzduirea echipamentelor de tip UPS este pusa la dispoziție o încăpere pe același nivel (subsol) de 54m^2
- Pentru găzduirea echipamentelor de răcire/ventilație se pune la dispoziție o încăpere de 136m^2, aflată la parterul clădirii.

Toate echipamentele externe ale sistemelor infrastructurii de suport fizic vor fi amplasate în imediata apropiere a clădirii care conține Centrul de date.

Cu excepția altor precizări explicite de mai jos, ofertanții vor lua în considerare faptul că vor trebui să amenajeze conform cerințelor care urmează numai spațiile folosite in scopul proiectului.

6.3.1 Planificarea Centrului de date

În această fază, utilizând rezultatele etapei de evaluare se va realiza planificarea Centrului de date în concordanță cu cerințele specifice ale beneficiarului și asigurând maximizarea eficienței energetice pentru toate subsistemele de infrastructura fizică și TI.

Faza de planificare va utiliza datele din etapa de analiză pentru a pregăti elementele necesare pentru proiectul final:

- Configurațiile hardware și de infrastructură, configurațiile rețelei de date, inventarul pentru servere, echipamente de stocare, rețea și alte echipamente TI;
- Infrastructura existentă a clădirii pentru asigurarea puterii și capacității de răcire, împreuna cu schemele arhitecturale și a instalațiilor de suport fizic;
- Evaluările realizate on-site ale clădirii, oferind informații adiționale de planificare, incluzând necesarul de spațiu pentru echipamentele de suport, stabilindu-se elementele arhitecturale, structurale, mecanice și electrice ale noului Centru de date.

6.3.2 Proiectarea detaliată a Centrului de date

Rezultatele activităților din faza de planificare vor fi utilizate în documentarea proiectării detaliate, astfel încât să poată fi obținute aprobările necesare, iar implementarea Centrului de date să poată fi efectuată fără sau cu modificări minime ale proiectului de execuție.

Pe parcursul fazei de proiectare detaliile din etapa de planificare vor fi materializate în planuri detaliate de implementare pentru instalarea cablării electrice, a sistemului de conducte pentru sistemul de răcire, de amplasare a echipamentelor, a detaliilor arhitecturale (pereți, uși), echipamentelor de monitorizare mediu, a specificațiilor tehnice pentru sistemul de ICI

detecție/stingere incendii și cerințelor de asigurare a securității fizice. Faza de proiectare a soluției va acoperi următoarele zone și va trebui să fie materializată printr-un proiect de execuție în concordanță cu reglementările și standardele în vigoare:

- Arhitectura: Planurile de amplasare și detaliile pentru pereți, tavane, spații, compartimentări; elementele generale ale proiectului de construcție;
- Sisteme mecanice: detalii, scheme și specificații pentru sistemul de climatizare, sistemul hidraulic și planurile pentru realizare, amplasare echipamente, planificare;
- Sistemele electrice: scheme și specificații pentru echipamentele electrice, amplasare, planificare, scheme monofilară și detalii, incluzând sistemele de susținere în cazul căderilor de tensiune etc.;
- Recomandări pentru sistemele de securitate fizică (control acces și de detecție/stingere incendii).

6.3.3 Implementare, punere în funcțiune și testarea Centrului de date

Proiectul de implementare va include următoarele elemente:

- Asigurarea de către furnizor a amenajărilor de arhitectură și construcții, pereții, ușile și celelalte lucrări de pregătire ale spațiului precum și pardoseală supraînălțată și demararea serviciilor de instalare a echipamentelor infrastructurii de suport în Centrul de date.
- Se vor instala sistemul de suport cabluri, cablurile și circuitele electrice din sala de calculatoare pentru a suporta necesarul de putere a Centrului de date, asigurându-se integrarea în sistemele electrice existente ale clădirii.
- Se vor instala echipamentele externe ale sistemului de răcire, sistemul de conducte ale circuitului hidraulic și sistemul de control al mediului din Centrul de date.
- Se vor instala rack-urile pentru echipamente, echipamentele interioare ale sistemului de răcire, sistemul UPS și distribuția electrică protejată la rack-urile de echipamente, livrate în cadrul proiectului și se testează infrastructura de suport, se instalează și testează soluțiile de monitorizare.

6.3.4 Cerințe tehnice minimale pentru proiectarea și implementarea Centrului de date

În proiectare și implementare se vor respecta cerințele următoarelor standarde și normative, după caz:

- ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centres:
    - Scopul standardului este de a oferi cerințele și recomandările pentru proiectarea și implementarea de Centre de date.
    - Standardul se adresează proiectanților care au nevoie de o înțelegere cuprinzătoare a proiectării Centrelor de date, incluzând planificarea locației, proiectarea sistemului de cablare și a rețelei de date.
    - Standardul specifică proiectarea cablării, a rețelei, a locației, conține anexe informative conținând bune practici și recomandări pentru cerințele de disponibilitate, definirea spațiilor, a rack-urilor și cabinetelor.
- EN 50173-5 Data Centre Cabling:
    - Scopul standardului este de a oferi un sistem de cablare generic pentru centre de date, care sa suporte o gama largă de aplicații existente sau emergente pentru LAN, SAN și WAN, care sa fie scalabil astfel încât să suporte creșterea viitoare pe durata de viață planificată a centrului de date și să fie suficient de flexibil pentru a face modificări ușor și eficient.
- ANSI/TIA-568-C.0, Generic Telecommunications Cabling for Customer Premises:
    - Standardul definește planificarea și instalarea unui sistem de cablare structurată pentru toate tipurile de premise ale clienților. El specifică un sistem care suportă o cablare de telecomunicații generică într-un mediu care îmbină o diversitate de produse și de producători.
    - Standardul specifică cerințele pentru un sistem de cablare de telecomunicații generic, incluzând:
        - Structuri ale sistemului de cablare,
        - Topologii și distante,
        - Instalare, performanță și testare,
        - Transmisie prin fibră optică și cerințe de testare.
- ANSI/TIA-568-C.l, Commercial Building Telecommunications Standard:

- Standardul definește planificarea și instalarea unui sistem de cablare structurata într-o clădire comercială și între clădirile comerciale din cadrul unui campus.
- Standardul definește structurile sistemului de cablare incluzând:
  - Facilitățile de intrare a furnizorilor de comunicații,
  - Sălile de echipamente,
  - Sălile de telecomunicații,
  - Cablare backbone,
  - Cablare orizontală,
  - Zona de lucru (spațiul care conține prizele de comunicații).

- ANSI/TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling and Components Standard:
  - Standardul include specificațiile pentru componente și cablare, precum și cerințele de testare pentru cablarea cu cupru (perechi torsadate), incluzând categoria 3, 5e, 6 și 6A.
- ANSI/TIA-568-C.3 Optical Fiber Cabling Components:
  - Scopul standardului este de a specifica cerințele de performanță pentru cablu și componente de fibră optică pentru cablarea cu fibră optică.
- ANSI/TIA/EIA-569-B Commercial Building Standard for Telecommunications Pathways and Spaces:
  - Scopul standardului este de a asigura operabilitatea, flexibilitatea, administrarea și longevitatea sistemului de cablare într-un mediu complex de transmisii de telecomunicații de voce și date (voce, date, video, securitate, semnale de control, etc.) descriind elementele de proiectare arhitecturală a sistemelor de suport pentru cabluri și spatiilor dedicate pentru echipamentele de telecomunicații.
- ANSI/TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure:

- Standardul se referă la administrarea infrastructurii de comunicații pentru clădire, incluzând documentația de bază și actualizarea periodică a planurilor, etichetelor și înregistrărilor. Administrarea va fi în sinergie cu sistemele de voce date și video precum și cu celelalte sisteme de semnalizare din clădire, incluzând sistemele de securitate, audio, alarme și management al energiei.

- J-STD-607-A Commercial Building Grounding and Bonding Requirements for Telecommunications:
  - Standardul specifică o infrastructură uniformă de împământare și legare la masa în clădirile comerciale.

- ISO/ IEC 11801, Generic Cabling for Customer Premises:
  - Standardul specifică un sistem de cablare generic, independent de aplicație, capabil să suporte o gamă largă de aplicații. El oferă o schemă flexibilă de cablare, astfel încât modificările sunt atât ușor de realizat cât și economice. Standardul de cablare generică:
    - Specifică o structură de cablare care suportă o largă varietate de aplicații,
    - Specifică clasele de canal E și F, bazate pe componente cu performanțe mai mari, capabile să suporte aplicații viitoare,
    - Specifică cerințele componentelor și specifică implementările de cablare care asigură legături permanente și canale care satisfac sau depășesc cerințele pentru clasele de cablare.

- BS EN 62040 Specification for UPS Systems
- BS EN 62040-1-1 UPS Safety Requirements
- IEC 60529 Degrees of Protection provided by Enclosures
- EN 61000 Electro Magnetic Compatibility Standard
- EMC Directive 89/336/EEC

6.3.5 Cerințe pentru proiectare și implementare a Centrului de date

Centrul de Date va fi proiectat și implementat conform recomandărilor standardului ANSI/TIA-942, minimum clasificarea **TIER 2.**

Pentru sistemele electrice și mecanice (sistemul de răcire) de suport se vor alege soluții care să asigure consum minim de energie și eficiență energetică în funcționare, chiar în condiții de încărcare de putere echipamente TIC de 30-40%. Se cere dimensionarea corecta a sistemelor infrastructurii de suport a Centrului de date, fiind unanim acceptat că supradimensionarea ar duce la creșterea masivă a pierderilor și la ineficiența energetică. Soluția propusă pentru Centrul de date trebuie să fie adaptabilă, flexibilă și modulară și să permită instalarea de rack-uri de servere cu mari densități de putere, fără oprirea sau modificarea configurației inițiale de rack-uri, doar prin creșterea capacității de putere și de răcire și prin soluții de izolare a culoarului de aer cald sau rece. Soluția trebuie să asigure integrarea în rack-uri de servere cu densități de putere de până la 15 KW / rack, pentru unele rack-uri, și să asigure parametrii optimi de mediu (capacitate de răcire și flux de aer rece) pentru configurații de rack-uri cu diverse puteri (mici, medii și mari).

Sistemele de securitate fizică vor fi proiectate și dimensionate astfel încât să respecte specificațiile din standardului ANSI/TIA-942 precum și legislația română în domeniu.

6.3.6 Cerințe tehnice pentru sistemele de suport ale Centrului de date

6.3.6.1 Arhitectură și construcții

Sala de calculatoare

Spațiul sălii de calculatoare va fi amenajat în următoarele condiții:

- Pereții interiori și exteriori ai sălii de calculatoare finisați, finisarea lor asigurând:
    - protecția antiincendiu (F90 minimum),
    - izolarea termică (cu vată minerală),
    - barieră antivapori
    - acoperiți cu vopsea antistatică.
- Tavanul și grinzile vor fi predate finisate, placate cu gips-carton și vată minerală, și acoperite cu vopsea antistatică. Tencuielile interioare gletuite se vor realiza fie prin închiderea porilor cu un strat subțire (1mm) pasta de var cu adaos de ipsos (glet de var), fie cu un strat de ipsos de 2 mm (glet de ipsos) netezite fin. Zugrăvelile se aplica pe

suprafețe tencuite, gletuite cu glet de ipsos și pregătite cu strat izolant - amorsa pentru a preîntâmpina absorbția.

- Ușile prin care se delimitează perimetrul Centrului de date vor fi metalice, antifoc, cu același grad de protecție ca și al pereților. Vor fi instalate uși antifoc, cu dimensiuni deschidere minime 900 x 2130 mm, cu deschidere spre sensul de evacuare în caz de incendiu. În interior ușile vor fi dotate cu bara antipanică, pentru deschiderea lor. Toate ușile Centrului de date vor fi prevăzute cu dispozitive de deblocare de tip electromagnetic, conectate la sistemul de control de acces și detecție/stingere incendii.

- Stratul suport al pardoselii în spațiul Centrului de date va realizat din sapa autonivelantă și va fi predat uscat și curat (desprăfuit) și acoperit cu vopsea antistatică.

Amenajările descrise anterior vor fi realizate în toate spațiile cu destinație de găzduire a echipamentelor IT și de comunicații identificate anterior (cele 6 module/camere de servere), în camera destinată UPS-urilor și în camera de la parterul clădirii care va găzdui echipamentele instalației de răcire.

Pardoseala tehnologică

Se vor realiza pardoseli supraînălțate ce vor fi realizate pe o structură suport, metalică ce va suporta minimum 1200 kg/mp. Înainte de instalarea pardoselii supraînălțate, stratul suport al pardoselii va fi acoperit cu vopsea antistatică. Aceasta vopsea va fi compatibilă cu rășina epoxidică utilizată pentru lipirea suporților verticali ai structurii pardoselii supraînălțate. Pardoseala supraînălțată va avea înălțimea minimă de 40 cm. Aceasta va fi proiectată astfel încât să acomodeze instalațiile specifice ale sistemului de răcire.

Structura portantă de suport va fi formata din coloane verticale reglabile cu cap profilat pentru a fixa traversele orizontale cu șuruburi și picior profilat pentru fixare în planșeu cu șuruburi, din oțel ambutisat, protejat anticoroziv, traverse orizontale, realizate din otel profilat, protejat anticoroziv care se fixează cu șuruburi de capul profilat al coloanei reglabile.

Panourile pardoselii supraînălțate vor fi cu dimensiuni standard de 600x600 mm, realizate din conglomerat, ignifuge și antistatice.

Pardoseala supraînălțată se va instala în tot subsolul clădirii (spațiul DataCenter): cele 6 camere (module) cu destinația de camere de servere, camera destinată UPS-urilor, holuri, precum și în camera de la parterul clădirii în care se vor instala echipamentele aferente sistemului de răcire.

Planul de amplasare a echipamentelor

Echipamentele IT și de comunicații din sala de calculatoare vor fi amplasate în rack-uri standard de servere de 19" cu lățimea de 60-75 cm și adâncimea minimă de 100 cm și în rack-uri de comunicații de 19" cu lățimea de minimă de 75 cm și adâncimea minimă de 100 cm, cu înălțimea de minimum 42 U.

Rack-urile de servere și comunicații vor fi așezate în rânduri continue, respectându-se realizarea de culoare calde și reci pentru circulația fluxurilor de aer și minimizarea amestecului aerului cald cu cel rece. Culoarul rece (situat în fața rack-urilor) va avea lățimea de minimum 110 cm, iar culoarul cald (din spatele rack-urilor de servere) va avea lățimea minima de 90 cm.

La intrarea în sala de calculatoare, în dreptul ușii de acces se va lăsa un spațiu liber minim de 120x120 cm, spațiu necesar manipulării și transportului rack-urilor și echipamentelor în sau din sala de calculatoare.

Ofertantul va prezenta soluția de amplasare care să permită, în condițiile dimensiunilor sălii, extinderea Centrului de date prin amplasarea unui număr maxim de rack-uri de servere și comunicații.

6.3.6.2 Sistemul de alimentare electrică și protecție la căderi de tensiune

Alimentarea cu energie electrică a Centrului de date va fi realizată de la tabloul general al clădirii. Pentru echipamentele vitale, în tabloul electric general al clădirii vor exista conexiuni protejate la căderi de tensiune prin generatorul Diesel de rezervă al complexului (furnizat de către ofertant). În sala de calculatoare a Centrului de date vor fi instalate tablouri electrice pentru alimentarea cu energie electrică a echipamentelor, astfel:

* un circuit trifazic pentru conectarea sistemului UPS redundant, care va alimenta rack-urile de echipamente, echipamentele sistemelor de securitate, cu o putere de maximum 120 KVA,
* un circuit trifazic care va alimenta echipamentele externe ale sistemului de climatizare..

Circuitele electrice de la tabloul general al clădirii vor fi aduse la locul de instalare al tablourilor electrice de către Ofertant, care va realiza tabloul sau tablourile electrice de distribuție, va asigura echiparea cu circuitele de protecție necesare și va asigura conectarea echipamentelor furnizate, inclusiv conectarea dual a rack-urilor de echipamente.

întrucât compartimentările arhitecturale sunt definitivate la nivelul subsol și priza de pământ este realizata, instalațiile prevăzute se vor conecta la aceasta priza. Conectarea se va face in cel puțin 2 locuri, independente de conectările altor instalații (de ex: paratrăsnet, curenți tari).

Fiecare rack trebuie sa fie dotat cu o bara de împământare care sa conecteze toate echipamentele din rack-ul respectiv.

Rezistenta de dispersie a prizei de pământ trebuie sa fie mai mica de 1 Ohm. Se va măsura rezistenta de dispersie a prizei de pământ, iar in cazul in care aceasta condiție nu este îndeplinita, se va executa o priza de pământ independenta in exteriorul clădirii. Toate cabinetele metalice vor fi legate la centura de împământare a clădirii.

6.3.6.2.1 Alimentare electrică de rezervă

Circuitele electrice pentru Centrul de date vor fi protejate la căderi de tensiune de către un grup de generatoare Diesel.

Sistemul de alimentare electrică și protecție la căderi de tensiune va fi dimensionat pentru încărcare inițială de cel puțin 250 kVA, pentru sarcina IT și Comunicații instalată prin proiect. Va fi luată în considerare o marjă de eroare de 10-15%. La dimensionarea sistemului de alimentare electrică și protecție la căderi de tensiune se vor lua în considerare și echipamentele infrastructurii de suport care vor asigura continuu condițiile de mediu și operare pentru Centrul de date, respectiv alimentare protejată pentru echipamentele infrastructurii de suport (sistemul de răcire) care trebuie să funcționeze continuu, chiar și în intervalul de la căderea tensiunii de rețea și pornirea și preluarea sarcinii de către sistemul electric de rezervă (grupul generator Diesel standby).

Circuitele electrice pentru Centrul de date vor fi protejate la căderi de tensiune de către doua generatoare Diesel.

6.3.6.2.2 Sistemul UPS (uninterruptible power supply) cu distribuție electrică modulară integrată

Rack-urile de echipamente din Centrul de date vor fi protejate la căderi de tensiune de un sistem UPS (Uninterruptible Power Supply). Sistemul UPS oferit trebuie să fie eficient din punct de vedere energetic într-o plajă largă de încărcare la ieșire și să aibă integrat sistemul de distribuție electrică pentru rack-urile de echipamente.

Sistemul UPS trebuie să respecte specificațiile tehnice de mai jos, care sunt considerate minimale:

- Să utilizeze o arhitectură modulară și scalabilă, atât pentru putere cât și pentru timpul de susținere pe baterii, instalată în rack-uri cu dimensiunile fizice ale rack-urilor standard de servere, pentru a putea fi integrat în rândurile de rack-uri de echipamente.
- Să conțină bypass de mentenață și sistem de distribuție electrică pentru sarcinile IT și comunicații integrate în sistemul UPS.
- Să dispună de accesorii opționale care să facă posibilă integrarea într-o soluție de răcire pentru densități mari de putere împreună cu rack-urile de echipamente protejate.
- Să aibă eficiența AC-AC pentru sarcina la ieșire între 25% și 100% mai mare de 94%,
- Sa fie în tehnologie on-line.
- Va fi dimensionat cu o capacitate inițială de minimum 80 KW, în redundanța N+1 și va permite upgrade pentru o capacitate de minimum 100 KW.
- Modulele de putere trebuie să permită upgrade de capacitate în pași de maximum 15- 20 KW, iar adăugarea de module de putere și baterii sau înlocuirea modulelor defecte să poată fi efectuată fără oprirea sistemului UPS.
- Amprenta la sol, în configurația finală, nu o va depăși pe cea a unui rack de servere standard, pentru un timp de susținere de minimum 6 minute la încărcare de 80 KW. Pentru creșterea timpului de susținere trebuie să aibă opțiunea de instalare de rack-uri adiționale, similare cu cele ale sistemului UPS, pentru baterii.
- Tensiune alternativă nominală la intrare: 220/380, 230/400, 240/415 V cu L1, L2, L3, N, PE (R, S, T, nul, împământare), selectabilă
- Plaja de variație admisibilă a tensiunii alternative de intrare: 340 - 477 la 100% încărcare.
- Plaja de variație frecventă la intrare: 40-70 Hz.

- Factor de putere la intrare: > 0,99 la încărcare mai mare de 25%.
- Distorsiune curentului la intrare fără filtre adiționale: < 5% la 100% încărcare.
- Tensiune alternativă nominală la ieșire: 220/380, 230/400, 240/415 V cu LI, L2, L3, N, PE (R, S, T, nul, împământare), selectabilă.
- Distorsiunea tensiuni la ieșire: < 2%.
- Stabilizarea tensiuni alternative la ieșire: +/- 1% pentru încărcare 100% liniară, +/- 3% pentru încărcare 100% neliniară
- Distorsiuni armonice ala tensiunii la ieșire: <2% THD maximum pentru încărcări liniare, <5% THD maximum pentru încărcare 100% neliniară.
- Operare în condiții de suprasarcina: 10 minute la 125% încărcare, 60 secunde la 150% incarnare.
- Să conțină bypass static integrat. Acesta va asigura transferul fără întrerupere a sarcinii de pe UPS pe intrarea de bypass dacă este necesară mentenanță sistemului sau dacă sistemul UPS nu poate să susțină sarcina critică.
- Sa conțină bypass mecanic de mentenanță integrat. Acesta va permite izolarea totală a sistemului UPS în timpul activităților de testare sau mentenanță, asigurând siguranța personalului, timp în care sarcina este susținută de rețeaua externă de alimentare bypass.
- Sa utilizeze baterii VRLA (Valve Regulated Lead Acid), fără mentenanță.
- Modulul de baterii trebuie să fie astfel realizat încât să permită înlocuirea de către utilizator, fără a fi necesară oprirea sistemului. Fiecare modul de baterii trebuie să permită monitorizarea tensiuni și temperaturii pentru a fi utilizate de sistemul de diagnosticare al bateriilor și de circuitul de încărcare cu compensare funcție de temperatură
- Încărcarea bateriilor nu va depăși 10% din puterea de ieșire a sistemului UPS în condiții de încărcare 100% cu sarcina la ieșirea acestuia.
- Circuitul de încărcare baterii va conține un circuit de compensare funcție de temperatura bateriilor, pentru a optimiza durata de viață a bateriilor.

- Sa conțină un sistem de management al bateriilor care să monitorizeze continuu starea fiecărui modul de baterii și care să transmită notificări în situația defectării sau deteriorare a capacității modulului.

- Sa conțină un sistem de protecție a bateriilor cu circuite de monitorizare și control care să limiteze nivelul de descărcare a bateriilor.

- Sistemul UPS să fie controlat de două module de control, redundante, care să poată fi înlocuite, în caz de defectare, fără a fi necesară oprirea sistemului UPS. Fiecare modul de control trebuie să aibă căi de comunicații separate, izolate optic, la modulele de putere și comutare statică și vor fi alimentate din surse de alimentare redundante.

- Sa aibă panou frontal, accesibil din față, care să permită afișarea parametrilor sistemului UPS și a componentelor sale, a parametrilor electrici de ieșire și intrare, evenimentele și alarmele cu data și ora producerii. Panoul va avea butoane prin care să se poată selecta parametrii sau evenimentele care doresc a fi vizualizate precum și posibilitatea de a efectua programarea sau controlul unor funcții ale sistemului UPS.

- Sistemul de distribuție modular, integrat, trebuie să asigure conectarea a până la 24 de circuite monofazice sau 6 circuite trifazice, sau combinații de circuite monofazice și trifazice, cu protecții de 16 și 32 A, cu cabluri de distribuție terminate cu conectori IEC 309. Parametrii și starea circuitele electrice de distribuție trebuie să poată fi monitorizate individual de către sistem, iar parametrii să poată fi afișați pe panoul frontal și transmiși la un sistem de monitorizare și administrare a infrastructurii centrului de date. Distribuția electrică se va realiza pe deasupra rack-urilor, iar lungimea cablurilor electrice va fi minimă, pentru a se minimiza pierderile și degajările termice.

- Sistemul UPS trebuie să permită extinderea distribuției modulare cu circuite electrice monofazice sau trifazice suplimentare, dacă va fi necesar în viitor. Extinderea trebuie să poată fi făcută prin instalarea unui sistem de distribuție modular suplimentar, independent sau montabil în rack standard. Sistemul de distribuție modular suplimentar trebuie să fie conectat la sistemul de monitorizare și administrare a infrastructurii.

- Sistemul UPS trebuie să aibă integrată o interfață de rețea Ethernet Web/SNMP care să permită integrarea într-un sistem de management a infrastructurii fizice de suport a Centrului de date și care să permită monitorizarea și administrarea sistemului UPS, inclusiv sistemul de distribuție electrică modulară, în mediu de rețea TCP/ IP.

- Sistemul UPS va semnaliza cel puțin următoarele defecte și alarme:
    - Încărcare baterii defectă
    - Baterie defectă
    - Temperatură mare baterii
    - Tensiune mare baterii
    - Monitorizare baterii defectă
    - Baterii descărcate
    - Inițiere shutdown
    - Defecțiune comunicare internă sistem UPS
    - Defecțiune hardware UPS - sarcina trecută pe bypass
    - Supraîncărcare - sarcina trecută pe bypass
    - Tensiunea sau frecvența sursei de bypass în afara parametrilor - sarcina nu poate fi trecută pe bypass
    - Defecțiune modul de control UPS
    - Suprasarcina
    - Defecțiune modul de putere
    - Alarmă redundantă
    - Pierdere redundantă
    - Defecțiune bypass static
    - Alarmă bypass de mentenanță
    - Alarme module distribuție: tensiune, curent sau putere în afara parametrilor.

Ofertantul va asigura și soluția de alimentare a rack-urilor de echipamente, de la sistemul de distribuție modular al sistemului UPS și va furniza și barele de distribuție (PDU - Power Distribution Unit) din rack-uri, capabile să susțină minimum 3,5 KW. Fiecare bară de distribuție va fi conectată Ia câte un circuit electric de distribuție distinct și va avea minimum 2 prize IEC 320-Cl9 și minimum 18 prize IEC 320-Cl3. Fiecare bară de alimentare va fi monitorizată prin cardul SNMP și va include și posibilitatea instalării unui senzor de temperatura și umiditate. Sistemul va permite adăugarea de noi circuite de alimentare duale pentru rack-uri, sau înlocuirea cu circuite electrice de puteri mai mari (11 KW sau 22 KW) pentru a se asigura creșterea densității de putere în rack-urile în care se vor instala echipamente noi sau se vor înlocui cele existente. Adăugarea sau înlocuirea de circuite electrice de distribuție trebuie să se poată efectua fără oprirea sistemului UPS. Garanţia pentru echipamente instalate va fi de minimum 36 luni de la data punerii în funcţiune.

6.3.6.3 Sistemul de răcire pentru Centrul de date

Sistemul de răcire ofertat pentru Centrul de date trebuie să fie eficient din punct de vedere energetic și să aibă funcționare eficientă într-o plajă largă de variație a încărcări termice ale echipamentelor instalate în rack-uri. Se dorește atingerea unui factor PUE (Power Usage Effectiveness) sub 1,6. În acest scop, toate componentele sistemului de răcire, inclusiv proiectarea sistemului de răcire, vor trebui să contribuie Ia atingerea acestui deziderat, prin integrarea în soluție de module de "free cooling" pentru agentul de răcire. Echipamentele de răcire din sală trebuie să aibă consum energetic minim și să fie adaptabile, funcție de încărcarea termică dinamică a echipamentelor IT și comunicații, prin controlul puterii ventilatoarelor pentru asigurarea debitului de aer rece, minimizarea lungimii căilor fluxurilor de aer și minimizarea sau eliminarea amestecului fluxurilor de aer rece și cald.

Soluția de climatizare trebuie să asigure răcirea rack-urilor de echipamente cu mari densități de putere din sala Centrului de date, inclusiv pentru rack-uri cu densități de putere de 10-20 KW/rack. Se dorește o soluție cu răcire zonală, cu izolarea unui culoar de aer (cald sau rece), pentru a se minimiza amestecul aerului cald cu cel rece și a se crește eficiența energetică a întregului sistem de răcire. Echipamentele de răcire vor utiliza ca agent de răcire amestec de apa/ glycol și trebuie să asigure răcirea sălii din Centrul de date inclusiv în intervalul de timp de la căderea tensiunii și preluarea alimentarii componentelor sistemului de răcire de către grupul generator de rezervă și reluarea producției de agent de răcire.

Toate echipamentele oferite vor fi din gama profesională, dedicate soluțiilor de răcire pentru Centre de date și vor permite integrarea într-un sistem de administrare și monitorizare, care va permite monitorizarea eficienței energetice a infrastructurii Centrului de date.

6.3.6.3.1 Dimensionarea Sistemului de răcire a Centrului de date

Sistemul de răcire va fi dimensionat pentru încărcare inițială de 80 KW scalabil o capacitate finală de 100 KW pentru sarcina IT și comunicații. Va fi luată în considerare o marjă de eroare de 10-15%. La dimensionarea sistemului de răcire vor fi luate în considerare și echipamentele infrastructurii de suport care generează încărcare termică în Centrul de date, respectiv răcirea echipamentelor infrastructurii de suport care trebuie să funcționeze continuu, chiar și în intervalul de la căderea tensiunii de rețea și pornirea și preluarea sarcinii de către sistemul electric de rezerva (grupul generator Diesel standby).

6.3.6.3.2 Echipamente de producere apă răcită (chillere)

Echipamentele de producere apă răcită au rolul de a furniza apa răcită necesară unităților interioare, în parametrii necesari. Ele trebuie să poată fi integrate intr-un sistem de răcire modular și scalabil, pentru a asigura capacitatea de răcire pentru încărcarea termică inițială și să permită în viitor upgrade pentru susținerea încărcării termice finale. Pentru asigurarea funcționării continue se dorește asigurarea în viitor a redundanței N+1 (un echipament va fi în standby pentru a prelua funcționalitatea în caz de defectare a altui echipament din sistem). Echipamentele vor fi din clasa de mare eficiență energetică și vor putea funcționa, în intervalele cu temperaturi scăzute, în “free cooling”.

Se va instala un sistem redundant ce va permite atât asigurarea redundanței, cât și creșterea capacității de răcire în funcție de creșterea capacității Centrului de date și a necesarului de răcire, iar în final să se poată ajunge Ia cel mult 3 echipamente în configurație redundanța 2+1.

Sistemul de producere apă răcită (chiller) ofertat trebuie să respecte specificațiile tehnice de mai jos, considerate minimale:

- Să fie din categoria echipamentelor profesionale de răcire a apei pentru Centre de date, proiectat astfel încât să combine cele mai bune performanțe în condiții eficiente, cu un impact scăzut asupra mediului.
- Să conțină un modul "free cooling" care să asigure consum minim de energie electrica în perioadele cu temperatură scăzută, fără a se utiliza compresoarele.

- Chiller-ul cu "free cooling'' trebuie să aibă trei moduri de funcționare pentru asigurarea eficienței maxime și reducerea consumului de energie electrică, funcție de temperatura exterioară și de încărcarea termică a sistemului:
    - mecanic (funcționează numai compresoarele) - întregul debit de lichid de răcire trece direct prin evaporator, fiind răcit de compresoare;
    - mecanic și "free cooling" - întregul debit de lichid de răcire trece în primă fază prin dry-cooler și apoi prin evaporator unde este răcit la temperatura dorită de către compresoare· (compresoarele funcționează parțial), când temperatura exterioară nu este suficient de scăzută pentru a asigura răcirea completa a sarcinii termice în "free cooling'';
    - "free cooling" (compresoarele nu mai funcționează)- întregul debit de lichid de răcire trece prin dry-cooler unde este răcit la temperatura setată.
- Toate funcțiile chiller-ului cu "free cooling'' trebuie să fie administrate și monitorizate de un controller cu microprocesor. Controlul vitezei ventilatorului, pornirea compresoarelor și repartizarea capacității de răcire trebuie să fie astfel administrate încât să se economisească la maxim energia electrică consumată.
- Echipamentul trebuie să poată funcționa cu apă sau cu un amestec apă-etilen glycol în diferite proporții, astfel încât să se asigure funcționarea sigură și la capacitatea de răcire proiectată în limite de variație a temperaturii exterioare între -25°C și +45°C.
- Sistemul de tip „Chiller” trebuie să aibă capacitatea de răcire de minimum 115 KW, la temperatura exterioară de +35°C, amestec apa/glycol 35%, T_{apa} = 7/12°C și minimum 40 KW în funcționare în mod "free cooling", la temperatură exterioară de 0°C.
- Sistemul de tip „Chiller” trebuie să fie echipat cu două compresoare de tip hermetic Scroll cu coeficient de performanță ridicat, nivel de zgomot scăzut, protecție termică internă
- Sistemul de tip „Chiller” trebuie să fie echipat cu presostate duble pentru protecția compresoarelor la suprapresiune sau subpresiune.
- Sistemul trebuie să fie livrat cu un controller care să permită monitorizarea tuturor parametrilor de funcționare sau a alarmelor de funcționare. De asemenea, trebuie să permită interconectarea a două sau mai multe echipamente asigurând funcționarea acestora în cascadă, în funcție de capacitatea de răcire necesară la un moment dat, cât și

funcționarea acestora prin rotație cu echipamentul de rezervă pentru a se realiza uzura uniformă a fiecărui echipament. Controllerul va asigura funcționarea/pornirea secvențiala decalată pentru a nu porni două echipamente în același timp (pentru a se evita curenții de pornire mari în același timp) și va asigura și pornirea automată a lor (autorestart) după oprirea lor la fluctuații de tensiune sau Ia căderi de tensiune, în aceleași condiții (cascadare, rotație, pornire secvențiala decalată).

- Sistemul trebuie să aibă două circuite frigorifice independente, pentru a asigura atât o funcționare eficientă din punct de vedere energetic la încărcare parțială, cât și creșterea redundanței și a fiabilității echipamentului.
- Sistemul trebuie să funcționeze cu freon ecologic.
- Sistemul de tip „Chiller" trebuie să funcționeze cu zgomot redus, fără a depăși nivelul de zgomot de 47 dB(A) măsurat la 10 metri de echipament.
- Sistemul trebuie să permită monitorizarea și să transmită parametrii de stare, alarmele sau atenționările cel puțin pentru:
    - în operare sau standby;
    - valori temperaturi apă tur și retur;
    - mod funcționare mecanic sau "free cooling";
    - număr compresoare în funcționare;
    - stare și alarme alimentare electrică;
    - stare și alarme controller;
    - stare și alarme compresoare
    - stare și alarme ventilatoare
    - stare și alarme circuite hidraulice.
- Amprenta la sol a unui echipament, inclusiv spațiul necesar de mentenață și operare nu va depăși 3.8 x 1.2 metri, iar greutatea în operare va fi de maximum 1800 kg.

Ofertantul va asigura proiectarea și implementarea soluției complete pentru echipamentele de producere de apă răcită, cu toate accesoriile și componentele necesare conectării lor în circuitul hidraulic și în sistemul de administrare și monitorizare a infrastructurii de suport a Centrului de date. Circuitul hidraulic va fi proiectat și realizat pentru puterea maximă IT a Centrului de date, astfel încât să se poată adăuga când este necesar chiller-e adiționale pentru asigurarea redundanței și creșterea capacității de răcire și va fi izolat termic pe întreaga sa lungime.

Pompele de recirculare a agentului frigorific din circuitul hidraulic vor fi alimentate de către sistemul UPS pentru a se asigura funcționarea neîntreruptă a sistemului de răcire.

Echipamentul de distribuție apă răcită trebuie să asigure distribuția centralizată și sigură a apei răcite sau a amestecului apa-glycol către echipamentele de răcire din sala Centrului de date, asigurând astfel modularitatea și scalabilitatea soluției de răcire.

Echipamentul de distribuție agent de răcire ofertat trebuie să aibă specificațiile tehnice de mai jos, considerate minimale:

- Să poată fi amplasat în sala de calculatoare sau într-un spațiu adiacent, cu valvele de izolare și de reglaj ușor accesibile. În cazul în care va fi instalat în sala de calculatoare, adâncimea nu va fi mai mare de 75 cm și lățimea va fi de maximum 110 cm, din cauza constrângerii spațiului disponibil.

- Să aibă posibilitatea de a conecta țevile de tur și retur ale circuitului frigorific de la chillere pe sus sau pe jos (sub pardoseala supraînălțată).

- Să poată asigura distribuția agentului de răcire spre echipamentele de răcire din sală prin țevi flexibile, izolate termic, instalate sub pardoseala supraînălțată.

- Să aibă posibilitatea de conectare a până la 12 echipamente de răcire, fiecare circuit tur și retur să poată fi izolat și balansat individual pentru a se asigura operarea optimă, mentenanța echipamentelor de răcire sau adăugarea de noi echipamente de răcire fără a fi necesară oprirea sistemului.

Va permite conectarea circuitelor hidraulice (tur și retur) către echipamentele de răcire cu țevi flexibile PEX-AL-PEX **(Cross-linked polyethylene**) de 1 țol, și un debit minim per circuit distribuție 1,2 l/s**.** Trebuie să poată funcționa cu apă sau amestec apă-glycol.

Echipamentul va fi livrat cu toate accesoriile necesare pentru conectarea la circuitul hidraulic al echipamentelor de producere apă răcita, precum și cu toate componentele circuitelor hidraulice

de distribuție pentru echipamentele de răcire ofertate pentru soluția de răcire a Centrului de date pentru încărcarea proiectată inițială, inclusiv elementele de fixare și izolare a acestor circuite.

6.3.6.3.3 Echipamente profesionale de răcire în rând pentru sala Centrului de date

Echipamentele de răcire pentru rack-urile de servere și echipamente de stocare date vor fi instalate în rândurile de rack-uri. Aceasta amplasare a echipamentelor de răcire profesionale pentru centre de date a fost luată în considerare din următoarele motive:

- Spațiul salii de calculatoare nu permite instalarea de echipamente profesionale de răcire profesionale perimetrale, cu livrarea aerului rece prin grile în pardoseala supraînălțată situate în fata rack-urilor, fără a avea limitări asupra debitelor fluxurilor de aer și asigurării condițiilor de răcire pentru densități mari de putere în rack-uri;

- Echipamentele de răcire în rând minimizează lungimea fluxurilor de aer, prin furnizarea aerului rece în față și recuperarea aerului cald din spatele rack-urilor de echipamente, în acest fel puterea necesară pentru ventilatoare pentru circulația volumului de aer fiind diminuată crescând eficiența energetică a sistemului de răcire;

- Permite mai ușor adoptarea de soluții pentru izolarea fluxurilor de aer cald sau rece în interiorul sălii de calculatoare, maximizând eficiența energetică globală a sistemului de răcire.

Echipamentele de răcire profesionale în rând ofertate trebuie să respecte specificațiile tehnice de mai jos, considerate minimale:

- Alimentare electrică 200-240V, 50/60 Hz.

- Capacitate de răcire minimum 18 KW, în condiții de temperatură de intrare a aerului pe serpentina de 29°C, umiditate relativa de 32%, temperatura intrare apă răcită de 7.2 °C și Delta T de 5.5 °C.

- Să permită conectarea echipamentului Ia sistemul UPS pentru a se asigura ventilația și răcirea continuu, chiar și în fereastra de timp de la căderea tensiunii de la rețeaua urbană și transferul alimentării electrice pe sistemul electric de rezervă pentru eliminarea pericolului creșterii excesive a temperaturii datorită densității mari de putere a echipamentelor din sala de calculatoare.

- Refularea aerului rece să se facă frontal, orizontal, pe toată înălțimea echipamentului.

- Colectarea aerului cald trebuie să se facă în partea din spate a echipamentului de răcire, pe toată înălțimea echipamentului.

- Ventilatoare să fie cu viteza variabilă, cu posibilitatea modulării vitezei în limita de 30-100%. Ventilatoarele vor fi cu soft start pentru a minimiza curenții de pornire care ar putea crea condiții de suprasarcină sistemului UPS pe care vor fi conectate echipamentele. Echipamentele trebuie să poată funcționa chiar în condițiile defectării unui ventilator, iar ventilatorul defect trebuie să poată fi înlocuit fără a fi necesară oprirea echipamentului de răcire.

- Fiecare echipament de răcire trebuie să poată furniza un debit minim de 75 m3/min, iar la defectarea unui ventilator trebuie să nu se diminueze debitul de aer al echipamentului cu mai mult de 15%.

- Echipamentul de răcire va fi prevăzut cu o valvă controlată de microprocesor care va asigura reglarea cantității de apă răcită care circulă prin serpentina pentru menținerea condițiilor optime de răcire.

- Echipamentul de răcire va funcționa cu apă sau amestec de apa/ glycol, va putea fi conectat la echipamentul de distribuție cu țevi de 1 țol (tur și retur) și va admite în mod obligatoriu conectarea pe jos a țevilor circuitului hidraulic.

- Echipamentele de răcire vor fi livrate standard cu câte un senzor de temperatura care să poată fi instalat pe rack-urile adiacente pentru a oferi informațiile privind temperatura la intrarea în rack, parametru care să fie utilizat pentru controlul funcționării echipamentului de răcire.

- Echipamentele vor fi prevăzute cu pompă și circuit de evacuare a condensului capabil să pompeze apa rezultată în afara spațiului sălii de calculatoare. Funcționarea incorectă a circuitului de evacuare condens va fi semnalată prin transmiterea unei alarme.

- Echipamentele vor avea instalate câte un detector de lichide, conectat la controller și va transmite alarme în cazul detecției scurgerii de agent de răcire pe pardoseala.

- Echipamentele vor avea două surse de alimentare și vor putea să fie alimentate pe două circuite electrice distincte, cu cordoane electrice cu conectori IEC 309, pentru a se putea asigura continuarea răcirii în cazul defectării unei surse de alimentare sau întreruperii unei căi de alimentare cu energie electrică.

- Echipamentele vor avea un panou frontal, gestionat de un controller cu microprocesor, cu ecran LCD și taste care vor permite monitorizarea și configurarea echipamentului pe baza unui meniu ale cărui funcții vor include rapoarte de stare și de setări ale parametrilor operaționali și care să permită navigarea prin meniuri, selectarea obiectelor și introducerea informațiilor alfanumerice. În plus, panoul frontal trebuie să aibă LED-uri care să indice starea de operare a echipamentului, existentă alarmelor sau atenționărilor și să atenționeze utilizatorul dacă au apărut noi alarme critice. Orice alarmă critică trebuie să fie avertizată și sonor. De asemenea, controllerul va oferi informații asupra timpului de utilizare pentru componentele majore ale echipamentului.

- Alarmele și evenimentele trebuie să fie memorate și însoțite de data și ora producerii evenimentelor precum și condițiile de operare ale echipamentului în momentul producerii evenimentului. Echipamentul va transmite cel puțin următoarele alarme:

    - eroare de comunicație internă a echipamentului
    - pierdere comunicație în grup
    - defect răcire
    - defectare senzori temperatura
    - temperatura fluid tur sau retur în afara parametrilor setați
    - senzori defecți
    - filtru aer colmatat
    - pompa condens defectă
    - detecție scurgeri lichid
    - defectare ventilator
    - defectare sursa alimentare
    - parametrii aer ieșire/intrare în afara celor setați.

Echipamentele de răcire vor avea interfața de rețea Ethernet care să permită administrarea, monitorizarea și notificarea evenimentelor într-o rețea prin TCP/IP și care să permită integrarea în sistemul de management a infrastructurii fizice de suport a Centrului de date.

Echipamentele de răcire trebuie să aibă aceeași înălțime și adâncime ca și rack-urile de servere furnizate, pentru a permite alinierea în față, spate și înălțime și pentru a se putea implementa o soluție de închidere și izolare a culoarului de aer (cald sau rece) pentru realizarea unei soluții care să permită instalarea de echipamente cu densități mari de putere. Ele vor fi astfel distribuite pentru a se asigura atât fluxul de aer cat și capacitatea de răcire necesare asigurării condițiilor optime de funcționare a echipamentelor susținute, cât și a redundanței N+ 1. În situația defectării sau opririi unui echipament, celelalte echipamente trebuie să susțină răcirea corespunzătoare a tuturor rack-urilor de echipamente.

Aerul proaspăt necesar pentru ventilarea încăperilor cu echipamente IT va fi furnizat de o centrală de tratare aer amplasată în camera de 136m2 de la parterul clădirii.

Centrala de tratare aer va avea în componență următoarele module: modul filtrare aer cu filtru aer clasa F7 și prefiltru clasa G4, modul recuperator de căldură aer-aer rotativ, modul încălzire aer având baterie de încălzire alimentată cu agent termic +600C/400C, modul răcire având baterie de răcire alimentată cu apă răcita +7/+120C, module ventilare având ventilatoare centrifugale cu palete curbate înapoi. Reglajul de temperatură se va face cu vana cu 3 căi și servomotor de tip divergență (reglajul debitului de apă la temperatură constantă) pentru circuitul de apă răcita și cu vana cu 2 căi și pompă de recirculare agent termic pentru circuitul de încălzire.

Debitul de va fi de 5.000m3/h. Sarcina termica totala necesara pentru încălzire va fi de Qi=72kW, sarcina bateriei de încălzire Qbi=28kW, capacitatea totala a recuperatorului de căldura Qrec=44kW. Sarcina totala de răcire va fi Qr=35kW.

Ventilatoarele centralei de tratare aer vor avea turații reduse (n<1.450rot/min) și vor fi încadrate din punct de vedere al consumului specific de energie in clasele SFP1÷SFP3 (PSFP<1250W/m3/s).

Distribuția aerului se va face cu canale de ventilare confecționate din tabla zincata, având secțiune rectangulara sau circulara, asigurând o buna accesibilitate pentru întreținere și curățare. In cadrul sistemului de ventilare, pe racordurile la încăperi, se vor monta dispozitive manuale de reglaj debit de aer (clapete reglaj debit aer).

Canalele principale de ventilare se vor monta pe coridor, pentru distribuția orizontala din subsol și respectiv in ghene închise pentru distribuția pe verticala (intre subsol și parter). Canalele de ventilare vor fi izolate termic cu saltele de vata minerala semirigida protejata cu folie de aluminiu, având grosimea izolației de min. 20mm pentru canalele montate la interior și min. 50mm pentru cele montate pe admisia\evacuarea de aer exterior. Canalele de aer montate la interior in spatii și

poziții in care acestea pot fi supuse la acțiuni mecanice ce pot conduce la deteriorarea izolației termice, se vor proteja la exterior cu tabla de aluminiu.

Introducerea aerului in încăperi se va face cu grile montate in perete sau anemostate montate in tavan. Acestea vor avea plenum de racordare izolat termic și acustic, dispozitive mobile de dirijare a jetului de aer. Nivelul de zgomot in dispozitivele de refulare aer nu va depăși 40dB(A).

Evacuarea aerului din încăperi se va face cu grile montate in perete sau guri de aspirație cu secțiune circulara montate in tavan. Acestea vor avea după caz plenum de racordare, dispozitive de reglaj a debitului de aer. Nivelul de zgomot in dispozitivele de aspirație aer nu va depăși 40dB(A).

Evacuarea fumului și gazelor de stingere după un eventual incendiu se va face cu un ventilator de evacuare aer de tip axial pentru montaj pe canal de aer cu secțiune circulara. Acesta va fi montat in paralel cu ventilatorul de evacuare aer al centralei de tratare aer. Pentru evacuarea fumului se vor utiliza aceleași canale de aer cu cele pentru ventilarea in regim normal. Trecerea de la regimul de ventilare normal la regimul de desfumare se va face cu comanda manuala, după stingerea incendiului și oprirea sistemului de deversare gaze de stingere. Comanda manuala va acționa sistemul de control al pornirii ventilatorului și respectiv motoarele de acționare a celor doua clapete de închidere montate pe aspirația celor doua ventilatoare. Aerul de compensare va fi introdus de centrala de tratare aer.

Echipamentele trebuie să fie livrate cu opțiunile necesare realizării canalelor de cablu pentru distribuția circuitele electrice de alimentare și a cablării de date, sistem de susținere deasupra rack-urilor și care să se integreze cu cel al rack-urilor de echipamente.

Vor fi livrate și instalate echipamentele de răcire, cu toate accesoriile necesare pentru conectarea în circuitul hidraulic, la sistemul de administrare și monitorizare a infrastructurii Centrului de date și accesoriile necesare realizării sistemului de susținere cabluri electrice și sistem cablare structurată pe deasupra rândurilor de rack-uri. Numărul lor trebuie să asigure soluția de răcire a Centrului de date pentru încărcarea inițială proiectată, inclusiv să asigure redundanța N+ 1 pentru echipamente.

6.3.6.4 Sistemul de management centralizat a infrastructurii Centrului de date

Sistemul de management centralizat trebuie să poată monitoriza parametrii de funcționare pentru echipamentele propuse în soluția pentru Centrul de date (UPS, distribuție electrică modulară, unități de răcire, sistem de monitorizare a temperaturii și umidității la nivel de rack).

Sistemul de management centralizat redundant ofertat trebuie să respecte specificațiile tehnice de mai jos, considerate minimale.

- Sistemul de management va fi livrat cu server montabil în rack, cu accesoriile de instalare în rack, pe care va rula aplicația de management centralizat. Sistemul de management va asigura monitorizarea centralizată prin utilizarea unei console grafice a alarmele și stările generale ale parametrilor echipamentelor de infrastructura a Centrului de date.

- Va efectua monitorizarea și va asigura notificarea în timp real a evenimentelor care apar la echipamentele infrastructurii Centrului de date asigurând eficienta în luarea deciziilor, reducerea timpilor de reparare și maximizarea disponibilității.

- Va asigura suport pentru echipamente de infrastructura de la producători diferiți.

- Interfața utilizator trebuie să permită filtrarea evenimentelor critice, atenționări sau normale.

- Va detecta automat echipamentele care pot fi monitorizate și va permite, pentru cele care au această facilitate, configurarea în grup pentru pragurile de alarmă.

- Va permite acces la informațiile curente și istorice și va permite efectuarea de analize asupra tendințelor pentru a se detecta din timp posibile situații critice. Informațiile vor fi stocate într-o bază de date centralizată a aplicației, de unde va fi posibilă sortarea după tip eveniment, dată, tip echipament și sau grup de echipamente.

- Să aibă posibilitatea integrării cu aplicații de administrare a operării, schimbărilor, capacității, eficienței energetice.

- Sa permită acces Web, prin comunicații criptate, administratorilor pentru a putea monitoriza 24 de ore din 24 starea echipamentelor infrastructurii de suport a centrului de date.

- Sistemul de management centralizat va fi livrat cu toate accesoriile necesare pentru instalare și operare în rack în sala de calculatoare a Centrului de date.

6.3.6.5 Sistemul integrat de securitate al Centrului de date

Sistemul integrat de securitate va fi proiectat cu respectarea tuturor prevederilor legale aplicabile domeniului de utilizare. Cerințele tehnice și funcționale sunt minimale.

Sistemul de securitate integrat va fi format din următoarele subsisteme:

6.3.6.5.1 Sistem de control acces

Sistemul de control acces va răspunde următoarelor cerințe minimale:

- Să permită integrarea cu celelalte sisteme de securitate, cu management din interfață unică
- Să conțină 4 filtre de control acces dublu sens, cu funcție anti-passback
- Centrala de control acces trebuie sa respecte următoarele: Alimentare 12Vcc, Intrare prezenţă reţea , Intrare baterie descărcată, Cititoare de cartele de proximitate sau similar, Intrări contact magnetic: 2, Butoane cerere ieșire: 2, Ieşiri libere de potenţial : 2 : contacte NC și NO, Port RS485 pentru comunicaţie cu interfeţele de control acces (max. 16), Port RS 485/RS232/USB pentru comunicaţie cu soft programare. Fiecare ușa trebuie sa poată funcționa autonom min.4 ore.
- Sistemul trebuie sa permită interfațarea cu sistemul de detecție anti incendiu și antiefracție și sa fie dotat cu butoane locale de urgenta.
- Să permită integrarea și managementul useri-lor cu Active Directory sau echivalent LDAP v3
- Sistemul trebuie să fie modular și să permită extensia ulterioară fără a afecta funcționarea sistemului inițial
- Să fie dotat cu electromagneți 500kgf pentru uși, cu montaj aplicat, butoane de urgență și monitorizare a stării ușilor.
- Programare software a ușilor care sunt pe calea de evacuare și care se vor deschide în caz de urgență.

6.3.6.5.2 Sistem de supraveghere video IP

Sistemul va cuprinde 8 camere IP, tip DOME, rezoluție 1080p, iluminare IR la minim 30metri (la 50 IRE), sensibilitate color 0.1 lux (50 IRE), lentila varifocala autoiris min.3-9mm, control electronic zoom, control electronic focalizare, compresie H.264, streaming JPG, funcție de analiză video, incalcare perimetru, traversare linie imaginara, obiecte părăsite, obiecte mișcate, viteza transfer 10/100/1000Mbps, temperatura de funcționare -20˚C ~ +50˚C, umiditate funcționare 20% ~ 95%, construcție rezistenta la vandalism, grad protecție IK10.

De asemenea, se va furniza un echipament de tip NVR (Network Video Recorder), care va asigura înregistrarea și păstrarea înregistrărilor pe o perioadă de minim 30 de zile.

Acesta trebuie sa gestioneze min. 8 camere IP la rezoluție maxima 1080P, sa asigura simultan modul setare, înregistrare date, vizualizare live, vizualizare playback, date remote-live și remote-playback. Sistemul va fi integrat cu sistemul de control acces și cu celelalte sisteme de securitate, cu management dintr-o interfață unică. Sistemul va dispune de un spațiu de stocare propriu de min. 4TB, extensibil la minim 10TB, compresie MJPEG, MPEG4, H.264.

Sistemul va fi inclus in structura unuia dintre rackurile de comunicații.

6.3.6.5.3 Sistem de alarmare la efracție

Se va furniza un sistem cu următoarea configurație minimală:

- Centrală cu 8 zone, extensibilă la minim 32 zone, Număr max. de evenimente de efracţie memorate min.: 3000 , Număr max. de evenimente de pontaj memorate: minim 3000 , Număr max de partiţii : 32, Coduri utilizator: min.120
- 8 detectori PIR în dublă tehnologie, PIR+MW, montaj pe perete,raza de acoperire detecție min. 15m la 90 grade, cu imunitate electromagnetica, anti masking
- 12 detectori de șoc, detector de soc digital programabil, pulse count 1-8, raza acțiune 1,5m ptr. beton; 2,5 m ptr. perete de caramida; 3 m ptr. metal; 3,5 ptr. lemn.
- 4 contacte magnetice de uz industrial, metalice cu cablul protejat în buclă metalică.
- Sistemul va fi integrat cu restul sistemelor de securitate, cu management dintr-o interfață unică

6.3.6.5.4 Sistem de stingere cu NOVEC

Implementarea unui sistem de detecție, semnalizare și comanda stingere incendiu are ca scop detectarea și semnalizarea unui început de incendiu în cel mai scurt timp, încă din faza incipienta, precum și stingerea incendiului, fără a afecta integritatea aparaturii electronice, sistem bazat pe tehnologia de deversare a unui agent de stingere incendiu stocat in butelii amplasate in fiecare camera sau centralizat într-o camera tehnica dedicata.

Ofertantul va prevedea o instalație automata de detecție, semnalizare și comanda stingere incendiu in camerele serverelor. Aceasta va funcționa cu agenți de stingere curați, ecologici.

Soluția tehnica pentru protejarea camerelor de servere împotriva incendiului se va baza pe utilizarea unui agent de stingere gazos, de tipul FK-5-1-12, având următoarele caracteristici fizico-chimice:

- Substanța cu denumirea chimica dodecafluor-2-metilpentan-3-1, având formula chimica F3CF2C(O)CF(CF3)2 este folosita ca substanța de stingere a incendiilor sub indicativul FK-5-1-12.
- La temperatura mediului ambiant de 20°C, substanța FK-5-1-12 este un lichid clar, fără culoare (incolor) și fără miros (inodor).
- Substanța FK-5-1-12 va fi stocata în butelii (cilindri) din otel, fiind presurizata cu azot la presiunea de 25 bar (abs) la temperatura de 20°C (presiune joasa), respectiv la presiunea de 42 bar(abs) la temperatura de 20° C (presiune înalta).

Sistemul astfel ofertat va asigura detecție la început de incendiu ultrarapidă prin aspirație, atât în rack-uri cât și sub pardoseala.

Sistemul de detecţie, semnalizare și comanda stingere incendiu va fi de tip adresabil, trebuind să asigure o supraveghere totală a spaţiilor şi a instalaţiilor din incintele protejate, inclusiv sub pardoseala.

Sistemul de detecție, semnalizare și comanda stingere la incendiu trebuie să cuprindă:

- Centrala adresabila de stingere incendiu, certificata pentru sisteme de stingere cu gaze
- Panou operare de la distanță
- Detectori adresabili optici de fum și temperatura, cu imunitate electromagnetica
- Detectori de fum prin aspirație
- Dispozitive de avertizare acustică (sirene) şi optică (flash-uri)
- Butoane manuale de declanșare stingere incendiu
- Butoane manuale întârziere stingere
- Dispozitive de detecție a umezelii provocate de condens sau scurgeri accidentale de fluide

Sistemul de stocare și distribuţie a agentului de stingere trebuie să cuprindă:
- Baterie de butelii cu agent de stingere ;
- Dispozitive automate pentru acţionarea automată a valvei buteliei în vederea eliberării agentului de stingere comandate de centrala de stingere;
- Dispozitiv manual-mecanice pentru acţionarea valvei buteliei în vederea eliberării agentului de stingere;
- Dispozitive de monitorizare presiune cilindri
- Reţea de distribuţie agent de stingere pentru agent stingere;
- Duze pentru descărcarea gazului.

Se vor utiliza cabluri electrice rezistente la foc min.E 30, free halogen.

Conductele de transport agent de stingere vor fi realizate din țeavă de otel galvanizată, iar fitingurile vor fi filetate, din fonta galvanizata.

Pentru condiționare la acționarea electrovanelor de evacuare a gazelor, sistemul trebuie să prevadă un sistem de evacuare a gazelor arse din incinta protejata, coroborat cu sistemul de ventilație.

Soluția trebuie să includă un sistem de eliminare a gazelor arse, coroborat cu cerințele sistemului de ventilație și climatizare ofertat.

Vor fi respectate următoarele standarde și norme in vigoare:

- EN54-2 Echipament de control și de semnalizare
- EN54-3 Dispozitive sonore de alarmare la foc
- EN54-4 Echipament de alimentare electrica
- EN54-5 Detectoare de căldură – Detectoare punctuale
- EN54-7 Detectoare de fum – Detectoare punctuale ce funcționează pe principiul difuziei luminii sau de ionizare
- EN54-11 Declanșatoare manuale de alarma
- SR EN 15004 sisteme de stingere incendiu ce utilizează agenți gazosi – proprietăți fizice
- P118/2 -2013 - „Normativ privind securitatea la incendiu a construcțiilor, Partea a II-a —
- Instalații de stingere”,
- I18/02 - Normativ pentru proiectarea și executarea instalațiilor de semnalizare a incendiilor și sistemelor de alarmare împotriva efracției din clădirile civile, de producție și depozitare;
- I7/2011 - Normativ pentru proiectarea și execuția instalațiilor cu tensiuni pana la 1000 Vca și i 500 Vcc;
- Directiva 99/36/EC – Directiva Europeana pentru recipiente sub presiune

7 LIVRABILELE PROIECTULUI

7.1 Infrastructură hardware şi de comunicaţii

În cadrul proiectului se vor furniza următoarele echipamente și componente:

Cod	Echipamente Hardware și de comunicații	U.M.	Cantitate (bucăți)
HW1.	Server tip1	buc.	144
HW2.	Șasiu pentru server-e de tip 1	buc.	36
HW3.	Server tip2	buc.	4

HW4.	Resurse stocare date HDD	buc.	2
HW5.	Sistem de stocare a datelor pe SSD	buc.	1
HW6.	Unitate back-up pe bandă	buc.	1
HW7.	Dulap metalic (rack) pentru echipamente de tip server	buc.	4
HW8.	Stații de lucru pentru administrare	buc.	15
HW9.	Echipamente multifuncționale de mare capacitate	buc.	3
HW10.	Sistem de comunicații – complet format din minim:	buc.	1
	Switch core L2/L3		2
	Server pentru managementul și virtualizarea serviciilor de rețea		2
	Switch layer 2 10/100/1000 management		8
	Load Balancer		2
	Firewall		2
	Router WAN		2
	Switch agregare acces		2
	Switch acces servere		12

Detalii cu privire la specificațiile acestor echipamente se regăsesc în cadrul Capitolului 5 al Caietului de Sarcini.

Lista livrabilelor este obligatorie, dar minimală. Fiecare ofertant poate propune completarea acesteia cu alte componente pe care le consideră necesare în vederea implementării arhitecturii pe care o propune, astfel încât să se realizeze un sistem complet funcțional, conform cerințelor acestui Caiet de Sarcini.

Se vor furniza toate soluțiile și accesoriile necesare pentru integrarea şi operaționalizarea acestor echipamente în cadrul sistemului informatic existent la nivelul ICI, inclusiv toate cablurile și accesoriile necesare pentru alimentarea echipamentelor și pentru interconectarea lor. De asemenea, se vor furniza toate accesoriile necesare în vederea instalării noilor echipamente.

7.2 Infrastructură software

În cadrul proiectului se vor furniza cel puțin următoarele elemente de infrastructură software:

Cod	Infrastructură Software	U.M.	Cantitate (bucăți)/observații
SWI1.	Pachet de software pentru virtualizarea resurselor hardware și managementul resurselor virtualizate, care va include minim:	buc.	1
	Sisteme de operare		Trebuie să fie licențiate pentru întreaga capacitate de procesare ofertată și conform cerințelor minime ale caietului de sarcini.
	Managementul resurselor virtualizate		Soluția trebuie să fie licențiată pentru întreaga capacitate de procesare ofertată și conform cerințelor minime.

	Sistem pentru gestiunea bazelor de date		Soluția trebuie să fie licențiată pentru minim doua servere fizice de tip 1 în configurație activ-activ pentru întreaga capacitate de procesare a serverelor și conform cerințelor minime.
	Platforma pentru managementul utilizatorilor și a accesului la sistem		Soluția trebuie să fie licențiată pentru minim doua servere fizice de tip 1 în configurație activ-activ pentru întreaga capacitate de procesare a serverelor și conform cerințelor minime.
SWI4.	Pachet de software pentru platforma de interoperabilitate	buc.	1 / (Soluția trebuie să fie licențiată pentru minim doua servere fizice de tip 1 în configurație activ-activ pentru întreaga capacitate de procesare a serverelor și conform cerințelor minime.)

Cantitățile indicate se referă la unități conceptuale și nu la modelul real de licențiere, care poate fi diferit pentru fiecare modul software în parte și de la producător la producător. Cantitatea solicitată va fi interpretată în contextul descrierii din coloana din stânga.

Detalii cu privire la specificațiile acestor elemente de infrastructură software se regăsesc în cadrul Capitolului 5 al Caietului de sarcini.

Lista livrabilelor este obligatorie, dar minimală. Fiecare ofertant poate propune completarea acesteia cu alte componente pe care le consideră necesare în vederea implementării arhitecturii

pe care o propune, astfel încât să se realizeze un sistem complet funcțional, conform cerințelor acestui Caiet de Sarcini.

Toate echipamentele furnizate în cadrul proiectului vor fi însoțite de toate driverele necesare, astfel încât să se realizeze recunoașterea corectă a tuturor componentelor echipamentelor, precum și utilizarea completă a tuturor resurselor instalate ale echipamentelor. De asemenea, tot software-ul încorporat (“embeded”) se va actualiza la ultima versiune disponibilă a producătorului.

Pentru tot software-ul licențiat se vor prezenta denumirile comerciale (ale fabricantului) pentru produsele și licențele ofertate și se va descrie detaliat modalitatea de licențiere, în concordanță cu configurația hardware ofertată.

7.3 **Aplicații specializate**

În cadrul proiectului se vor furniza următoarele aplicații software specializate:

Cod	Infrastructură Software	Cantitate
SWI5.	Serviciul „Date Deschise” (Sistem software integrat, bazat pe produse software standard plus software dezvoltat, destinat preluării datelor de interes public și publicării acestora)	1 buc.

SWI6.	Serviciul „Biblioteca virtuală” (Sistem software integrat, bazat pe produse software standard plus software dezvoltat/configurat, destinat preluării documentelor digitale de interes public și publicării acestora)	1 buc.

7.4 Echipamente destinate amenajării centrului de date

În cadrul proiectului se vor furniza cel puțin următoarele echipamente pentru amenajarea centrului de date:

Cod	Echipament	U.M.	Cantitate
CD 1	Materiale pentru podea tehnologică și tavan fals	pachet	1
CD 2	Materiale pentru cablarea electrică și de date	pachet	1
CD 3	Sistem de răcire pentru camerele server-elor	buc.	1
CD 4	Sistem UPS	buc.	1
CD 5	Generator de energie electrică	buc.	2
CD 6	Sistem de detectare, prevenire și stingere a incendiilor	buc.	1
CD 7	Sistem de control al accesului în centrul de date și monitorizare perimetrală	buc.	1

8 ACCEPTANȚA LIVRABILELOR ŞI A SISTEMULUI INTEGRAT

La livrare, produsele vor fi însoţite de declaraţia de conformitate/calitate din partea producătorului, de certificatul de garanţie şi/sau de alte documente necesare identificării acestora.

Ofertantul va livra echipamentele, va realiza instalarea şi configurarea acestora, precum și instalarea şi configurarea sistemelor de operare, a software-ului de bază și a pachetelor de aplicaţii.

Termenele de livrare şi recepţie a echipamentelor vor respecta perioadele/termenele prezentate în calendarul proiectului prezentat de ofertant și acceptat de beneficiar (diagrama Gantt).

Recepţia întregului sistem va fi efectuată de către reprezentanţii beneficiarului și se va face după instalarea, configurarea şi verificarea funcţionării tuturor componentelor sistemului la parametrii minimali solicitaţi în Caietul de Sarcini.

8.1 Recepţia cantitativă şi calitativă a livrabilelor

Recepţia cantitativă, respectiv recepţia calitativă a produselor hardware, software şi a serviciilor livrate se va face la locul în care urmează a fi instalate toate acestea, în prezenţa comisiei de recepţie a autorităţii contractante şi a personalului de specialitate pus la dispoziţie de furnizor, conform tabelului de mai jos:

Livrabil	**Descriere sumară**	**U.M.**	**Cantitate**
Dulap metalic (rack) pentru echipamente de tip server	Dimensiune 19”, 42U, incluzând accesorii (switch KVM, consolă KVM)	buc.	4,00

Șasiu pentru server-e de tip 1	Rack-abil, dimensiune 2U, poate găzdui până la 4 server-e de tip I	buc.	36,00
Server-e tip 1 (aplicații)	Se încadrează în șasiu Găzduiește aplicații cu necesar scăzut/moderat de putere de calcul	buc.	144,00
Server-e tip II (baze de date)	Rack-abil Găzduiește aplicații cu necesar ridicat de putere de calcul	buc.	4,00
Sistem de stocare a datelor pe HDD	Bazat pe discuri clasice (HDD) Stochează datele în volume mari	buc.	2,00
Sistem de stocare a datelor pe SSD	Bazat pe discuri de tip SSD Stochează datele care necesită performanță ridicată la acces	buc.	1,00
Sistem de backup al datelor pe benzi	Bazat pe tehnologie LTO Capabil să asigure o copie de siguranță a datelor și sistemelor din platforma Cloud	buc.	1,00
Stații de lucru pentru administrare	Destinate administratorilor platformei	buc.	15,00
Echipamente multifuncționale de mare capacitate	Destinate administratorilor platformei	buc.	3,00
Instalare și configurare server-e, echipamente de stocare a datelor	Echipamentele sunt puse pe poziția finală, sunt configurate, sunt realizate conexiunile dintre server-e și echipamentele de stocare	buc.	1,00
Materiale pentru podea tehnologică și tavan fals	Materiale care compun podeaua tehnologică și tavanul fals	pachet	1,00
Materiale pentru cablarea electrică și de date	Cabluri, canale de cabluri, etc.	pachet	1,00
Sistem de răcire pentru camerele server-elor	Asigură un climat controlat în camerele server-elor	buc.	1,00
Sistem UPS	Asigură alimentarea cu energie a echipamentelor din centrul de date, pe termen limitat	buc.	1,00
Generator de energie electrică	Generează energia electrică necesară funcționării echipamentelor în cazul întreruperii alimentării de la rețeaua de distribuție a energiei electrice	buc.	2,00
Sistem de detectare, prevenire și stingere a incendiilor	Senzori de fum, sistem de stingere a incendiilor specific centrelor de date	buc.	1,00
Sistem de control al accesului în centrul de date și	Bazat pe cartele de proximitate și senzori care controlează deschiderea ușilor	buc.	1,00

monitorizare perimetrală			
Realizare podea tehnologică și tavan fals	Realizarea cadrului metalic necesar, montarea panourilor modulare	buc.	1,00
Cablare structurată de date și alimentare cu energie electrica	Realizarea canalelor de cablu, pozarea cablurilor	buc.	1,00
Implementarea sistemului de asigurare a climatului controlat	Realizarea conductelor de aer rece / cald	buc.	1,00
Asigurarea continuității alimentării cu energie electrică	Realizarea circuitului prin care sistemul UPS și generatorul electric preiau alimentarea echipamentelor din centrul de date în cazul întreruperii alimentării de la rețeaua de distribuție	buc.	1,00
Implementarea sistemului de detectare, prevenire și stingere a incendiilor	Montarea senzorilor de fum, a conductelor de agent de stingere a incendiilor	buc.	1,00
Implementarea sistemului de securitate (control al accesului, monitorizare perimetrala)	Montarea senzorilor de carduri de proximitate, montarea mecanismelor de blocare a ușilor de acces către centrul de date	buc.	1,00
Pachet de software pentru virtualizarea resurselor hardware și managementul resurselor virtualizate	Pachet software format din platforma de virtualizare (hipervizor) și software-ul de management al resurselor virtualizate	buc.	1,00
Pachet de software pentru platforma de interoperabilitate	Pachet software destinat implementării unei arhitecturi de tip SOA	buc.	1,00
Serviciul „Date Deschise”	Sistem software integrat, bazat pe produse software standard plus software dezvoltat, destinat preluării datelor de interes public și publicării acestora	buc.	1,00
Serviciul „Biblioteca virtuală”	Sistem software integrat, bazat pe produse software standard plus software dezvoltat/configurat, destinat preluării documentelor digitale de interes public și publicării acestora	buc.	1,00
Analiza cerințelor platformei de Cloud Computing	Sunt analizate cerințele detaliate cu privire la implementarea platformei de Cloud	buc.	1,00

	Computing		
Identificarea cerinţelor de interfaţare cu alte sisteme și produse existente	Sunt analizate modelele de date, protocoalele de interfațare cu alte sisteme TIC existente	buc.	1,00
Proiectarea platformei de Cloud Computing	Se realizează prototipuri, este proiectată în detaliu platforma de Cloud Computing	buc.	1,00
Instalare și configurare pachet software pentru virtualizarea resurselor hardware și managementul resurselor virtualizate	Este instalat și configurat pachetul software pentru virtualizarea resurselor hardware și managementul resurselor virtualizate	buc.	1,00
Testarea infrastructurii de Cloud Computing	Este testată infrastructura de Cloud Computing	buc.	1,00
Implementarea platformei de interoperabilitate	Platforma de interoperabilitate este configurată, sunt definite transformări de date, formate de mesaje, etc.	buc.	1,00
Migrarea serviciilor ICI pe platforma de Cloud Computing	Sunt preluate în platforma de Cloud Computing o serie de servicii existente în cadrul ICI, cum ar fi Biblioteca Națională de Programe, serviciul „domenii.ro” etc.	buc.	1,00
Sistem comunicații	Include echipamentele de comunicații (firewall, router-e, switch-uri)	buc.	1,00
Servicii de consultanţă în domeniul managementului de proiect	Sunt asigurate servicii de consultanță în managementul proiectului (planificarea/coordonarea/monitorizarea progresului proiectului, gestionarea situațiilor excepționale, etc.), în managementul financiar al proiectului (colectarea datelor necesare cererilor de rambursare, formularea cererilor de rambursare, etc.)	contract	1,00

NOTĂ: Livrabilele se pot grupa, în acest caz se va întocmi un singur Proces Verbal de Recepție.

8.2 Recepția finală

Recepția finală a sistemului se va realiza la expirarea perioadei de garanție, ocazie cu care se va semna un proces verbal de acceptanță finală de către ICI.

9 CERINȚE PRIVIND GARANŢIA ŞI MENTENANȚA SISTEMULUI

Asistenta tehnică și suport

Garanția pentru toate echipamente ofertate va fi de minimum 36 luni de la data punerii în funcțiune.

Garanția pentru sistemul integrat ofertat va fi de minimum 36 luni de la data punerii în funcțiune.

Se vor furniza actualizări (patch-uri și actualizări de securitate disponibile de la producător) ale produselor software de tip COTS (aplicații standard) ofertate pe o perioadă de minim 36 de luni de la furnizarea acestora.

Serviciile de intervenție la defect în perioada de garanție

Acest serviciu are ca scop diagnosticarea defectelor și anomaliilor hardware și software ale echipamentelor furnizate și remedierea acestora. Remedierea se face prin depanare sau înlocuire de echipamente sau subansamble ale acestora (pentru defectele hardware) sau prin actualizări de microcod sau aplicare de soluții software recomandate de către producător (în cazul defectelor software). Remedierea defectelor se va face cu păstrarea, eventual creșterea, în nici un caz diminuarea caracteristicilor tehnice ale echipamentului original.

Timpul de remediere al defecțiunilor hardware necritice (care pot fi gestionate prin realocări de echipamente sau care nu duc la pierderea unui serviciu IT) va fi de maximum 14 zile și reprezintă durata de timp măsurată din momentul comunicării și confirmării unei probleme până în momentul rezolvării.

10 ELABORAREA OFERTEI

În elaborarea ofertei, Ofertanții trebuie să ia în considerare următoarele cerințe:

- Documentele aferente propunerii tehnice trebuie prezentate în format electronic (fişiere compatibile .doc sau echivalent, editabile și căutabile, toate legăturile dinamice din document trebuie să fie active – site-uri, cuprins, referințe etc.). Documentele ofertei tehnice trebuie redactate într-o manieră organizată, astfel încât, în procesul de evaluare a ofertelor, să permită identificarea facilă a corespondenţei informaţiilor cuprinse în ofertă cu cerințele caietului de sarcini.

- Atât oferta tehnică cât și cea financiară trebuie realizate astfel încât să fie respectate prevederile stabilite în cadrul fișei de date a achizițiilor incluse în documentația de atribuire.

- Ofertanții trebuie să prezinte enumerarea și explicarea riscurilor și ipotezelor privind execuția proiectului.

- Ofertanții trebuie să realizeze identificarea unor soluții de preîntâmpinare a riscurilor și de restrângere a efectelor acestora.

- Ofertanții trebuie să prezinte răspunsuri punctuale la toate cerințele caietului de sarcini și să detalieze în cadrul ofertei tehnice modalitatea şi mijloacele concrete prin care serviciile oferite îndeplinesc aceste cerinţe.

- Ofertanții trebuie să prezinte pe larg soluția propusă pentru proiect, în vederea atingerii obiectivelor acestuia și a rezultatelor așteptate.

- Ofertanții trebuie să prezinte arhitectura logică a sistemului propus. Se vor evidenția toate componentele arhitecturii software, realizându-se şi o mapare cu produsele software ofertate (pentru fiecare element al arhitecturii logice se vor prezenta produsele software cu care se va implementa componenta respectivă).

- Ofertanții trebuie să prezinte arhitectura tehnică a sistemului, cu identificarea tuturor componentelor hardware ale soluţiei și a produselor care vor fi instalate pe fiecare echipament în parte.

- Ofertanții trebuie să prezinte arhitectura de integrare a sistemului propus, atât între componentele soluţiei oferite cât și între acestea şi sisteme informatice externe, conform Caietului de Sarcini.

- Ofertanții trebuie să prezinte o corelare punctuală a ofertei cu secțiunea 8 a caietului de sarcini. Răspunsurile vor fi numerotate. Sunt aşteptate răspunsuri concrete care să demonstreze înţelegerea cerinţei și modalitatea propusă pentru atingerea ei (de ex. descriere a funcţionalităţii, capturi de ecrane, referințe cu numărul paginii/capitolului către documentația producătorului, link cu referință către site-ul producătorului etc.). Nu se așteaptă o simplă declarație de confirmare a conformității, ci o demonstrare a modului concret în care soluția ofertată răspunde cerințelor. Simpla declarare a respectării cerinţelor sau copierea cerințelor fără personalizarea răspunsului în funcție de soluția ofertată nu se va considera că este o dovadă a modalităţii în care acest lucru se va realiza, iar oferta tehnică va fi respinsă.

- Ofertanții trebuie să prezinte în detaliu, în raport cu specificul acestuia și cu metodologia propusa, modalitatea în care proiectul va fi organizat, incluzând cel puţin următoarele elemente: Reprezentantul său în cadrul Comitetului de Conducere al Proiectului, Manager de Proiect, Şefi de Echipă, Experții tehnici și alte roluri importante din cadrul echipei tehnice de proiect, Echipa de Suport administrativ.

- Ofertanții trebuie să prezinte organizarea și responsabilitățile fiecărei părți implicate în proiect, inclusiv propunerile pentru organizarea Beneficiarului/Utilizatorilor.

- Ofertanții trebuie să-și asume în întregime efectuarea activităților care concura la atingerea rezultatelor, ținând seama de resursele umane limitate ale Beneficiarului/Utilizatorilor.

- În cazul în care ofertantul reprezintă o asociere, ofertantul trebuie să descrie modalitatea în care fiecare membru al asocierii intervine în proiect, distribuirea și interacțiunea sarcinilor și responsabilităților.

- Oferta trebuie să includă o organigrama a echipei de proiect oferite. Se vor descrie responsabilitățile detaliate ale fiecăruia dintre experții ofertați.

- Ofertantul va prezenta planificarea activităților propuse, în interdependenţa acestora – un grafic Gantt. Acesta va respecta toate cerinţele explicite ale caietului de sarcini.

- Ofertantul va detalia care sunt resursele (experții cheie și non cheie numiți generic prin competentele lor) pe care le va aloca pentru fiecare etapă și activitate a proiectului.

- Ofertantul va prezenta o descriere detaliată a abordării pentru implementarea proiectului, prin detalierea fiecăreia dintre activităţile incluse în graficul Gantt pe care îl va prezenta. Pentru fiecare activitate se vor prezenta durata, experții implicați, efortul estimat din partea resurselor (măsurat în zile-om la 8 ore/zi) rezultatul aşteptat şi eventualele dependenţe de activităţi/resurse ale ICI. Se vor identifica livrabilele principale ale serviciilor de implementare prestate, precum și acceptanţele parţiale.

- Se va prezenta un tabel centralizator al tuturor livrabilelor proiectului (livrabile de management și livrabile tehnice). Livrabilele tehnice sunt cele care ajuta la atingerea obiectivelor concrete ale proiectului (produse, servicii, documentaţie etc.). Se va avea în vedere documentația prevăzută de metodologia de implementare propusă. Livrabilele de management sunt acele livrabile prevăzute de metodologia de project management propusă (planuri, ședințe, rapoarte etc.).

- Documentele de susținere ale ofertei tehnice vor trebui să includă minim: specificații tehnice ale produselor ofertate, declarațiile furnizorilor cu privire la faptul că echipamentele ofertate fac parte din producția lor curentă, documente explicative ale mecanismelor și condițiilor de licențiere pentru toate produsele software de tip “COTS” ofertate.

- Nu vor fi luate în considerare componente ale ofertei tehnice cum ar fi: pliante, diverse materiale promoționale ale firmelor producătoare sau furnizoare de echipamente sau servicii, prezentări, broşuri, etc. care nu au legătură directă cu obiectul, structura și cerințele din prezentul Caiet de Sarcini.

- Neprezentarea în cadrul ofertei a tuturor informațiilor solicitate în cadrul acestei secțiuni a Caietului de sarcini va face imposibilă evaluarea conformității ofertelor și se va considera o încălcare a cerințelor explicite ale Autorității Contractante privind modalitatea de prezentare a ofertei.

11 DISPOZIŢII FINALE

a.i.1. Va fi respins orice ofertant care nu demonstrează prin oferta sa faptul că îndeplineşte cerinţele minimale prezentate în caietului de sarcini. Prin demonstrare nu se înțelege simpla reafirmare a cerințelor caietului de sarcini – o astfel de abordare simplistă a ofertanților va duce la respingerea ofertei. Autoritatea contractantă așteaptă ca ofertele să demonstreze concret modul în care fiecare cerință va fi implementată, inclusiv prin folosirea capturilor de ecran relevante din aplicațiile ofertate.

a.i.2. Omiterea vreunei informaţii cerute în documentele procedurii sau prezentarea unei oferte necorespunzătoare faţă de documentele procedurii poate duce la respingerea ofertei.

a.i.3. Ofertantul are obligaţia să examineze instrucţiunile, formularele, termenii și specificaţiile din documentele procedurii, iar în cazul în care are nevoie de lămuriri asupra documentelor prezentate, să le solicite în scris achizitorului.

a.i.4. Ofertantul suportă toate cheltuielile asociate elaborării și prezentării ofertei sale, nefiind îndreptățit să solicite rambursare acestora indiferent de rezultatul obţinut în urma adjudecării contractului.

a.i.5. Duratele fazelor, datele de început și sfârșit ale activităților menționate graficul de implementare și planul detaliat de implementare vor putea fi actualizate de către Ofertant la semnarea contractului în conformitate cu data efectivă de începere a contractului.

a.i.6. Specificațiile tehnice definite in cadrul prezentului caiet de sarcini corespund necesităților și exigențelor ICI. Având în vedere specificul acestui proiect, autoritatea a descris operatorilor economici interesați necesarul de livrabile și servicii la nivel de detaliu suficient, permițând astfel identificarea cu ușurință a obiectului acestei achiziții publice. Toate specificațiile, serviciile și cerințele menționate și solicitate in cadrul acestui caiet de sarcini sunt însoțite de mențiunea „sau echivalent”.

a.i.7. Oferta va fi redactată în limba română.