**AUTORITATEA CONTRACTANTA**

**Caiet de sarcini**

**pentru**

**implementarea unui “Sistem Informatic pentru îmbunătățirea capacității de publicare a actelor operatorilor economici, de colaborare intre angajati si de asigurare a securitatii si monitorizarii sistemului informatic integrat ce susține procesele de furnizare a serviciilor publice aflate in responsabilitatea Oficiului Naţional al Registrului Comerţului”**

**72200000-7 Servicii de programare si de consultanta software (Rev.2)**

**30211300-4 Platforme informatice**

**48000000-8 Pachete software si sisteme informatice**

**72240000-9 Servicii de analiza si de programare de sisteme**

**72262000-9 Servicii de dezvoltare software (Rev.2)**

**72590000-7 Servicii informatice profesionale**

**48900000-7 Diverse pachete software si sisteme informatice**

**51612000-5 Servicii de instalare de echipament de procesare a informațiilor (Rev.2)**

**80533100-0 Servicii de formare in informatica**

**48820000-2 Servere**

**32420000-3 Echipament de rețea (Rev.2)**

**32570000-9 Echipament de comunicații**

Cuprins

[1 Date generale 5](#_Toc532977562)

[1.1 Structura organizatorică 5](#_Toc532977563)

[1.2 Locații implementare proiect 5](#_Toc532977564)

[1.3 Legislaţia privind organizarea şi funcţionarea instituţiei 5](#_Toc532977565)

[1.4 Descrierea instituţiei 6](#_Toc532977566)

[2 Obiectivul achiziţiei 11](#_Toc532977567)

[2.1 Obiectivul general 11](#_Toc532977568)

[2.2 Scopul proiectului 12](#_Toc532977569)

[2.3 Situaţia actuală (Sisteme existente) 13](#_Toc532977570)

[3 Descrierea noului sistem informatic 43](#_Toc532977571)

[3.1 Rezultate așteptate 43](#_Toc532977572)

[3.2 Utilizatorii noului sistem informatic 47](#_Toc532977573)

[4 Cerințe privind soluția tehnică 53](#_Toc532977574)

[4.1 Cerințe generale 53](#_Toc532977575)

[4.2 Cerințe funcționale 57](#_Toc532977576)

[4.3 Arhitectura generala a sistemului 66](#_Toc532977577)

[4.4 Descrierea nivelului tehnic al sistemului 81](#_Toc532977578)

[4.5 Cerințe de livrare și implementare 203](#_Toc532977579)

[4.6 Organizarea şi coordonarea proiectului 204](#_Toc532977580)

[4.7 Riscuri identificate 222](#_Toc532977581)

[4.8 Cerințe specifice 226](#_Toc532977582)

[4.9 Evaluarea performantei Contractantului 227](#_Toc532977583)

[5 Cerinte experti cheie 227](#_Toc532977584)

[5.1 Structura echipei de proiect 227](#_Toc532977585)

[5.2 Responsabilitatile expertilor cheie 229](#_Toc532977586)

[5.3 Cerinte minime obligatorii ale expertilor cheie 233](#_Toc532977587)

[6 Modalitatea de întocmire a ofertei 238](#_Toc532977588)

[7 Criterii de atribuire 240](#_Toc532977589)

[7.1 Descrierea modalitatii de punctare a factorului de evaluare “Pretul ofertei” 241](#_Toc532977590)

[7.2 Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnică – Capabilitati solutie tehnica” 241](#_Toc532977591)

[7.3 Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnica - Experiența profesionala a personalului” 243](#_Toc532977592)

[7.4 Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului” 245](#_Toc532977593)

[8 Cerinte pentru sesiunea demonstrativa 246](#_Toc532977594)

[9 Drepturi de proprietate intelectuală 249](#_Toc532977595)

[10 Modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului. 249](#_Toc532977596)

[11 Modalitatea de plată 250](#_Toc532977597)

[12 Informatii finale 251](#_Toc532977598)

[Anexa 1 - Lista locaţiilor semnificative la nivelul proiectului – ONRC, ORCT București şi ale ORCT Brașov 253](#_Toc532977599)

[Anexa 2 – Indicatori de performanta pentru realizarea activitatilor din contract 254](#_Toc532977600)

Cuprins figuri:

[Figură 1 Arhitectura hardware ONRC (mediu de productie) 25](#_Toc532977601)

[Figură 2 Distributia aplicatiilor si bazelor de date pe servere 26](#_Toc532977602)

[Figură 3 Arhitectura fizica ORCT Bucuresti 32](#_Toc532977603)

[Figură 4 Arhitectura fizica ORCT Medii si Mici 35](#_Toc532977604)

[Figură 5 Utilizatorii interni ai sistemului 48](#_Toc532977605)

[Figură 7 Utilizatori externi ai sistemului 52](#_Toc532977606)

[Figură 8 Descrierea generală a arhitecturii a BERC 58](#_Toc532977607)

[Figură 9 Schema generală flux de publicare Buletinul Electronic al Registrului Comertului 59](#_Toc532977608)

[Figură 10 Arhitectura generala a sistemului 67](#_Toc532977609)

[Figură 11 Arhitectura logica subsistem BERC 71](#_Toc532977610)

[Figură 12 Arhitectura logica Subsistem Colaborare 72](#_Toc532977611)

[Figură 13 Arhitectura logica propusa subsistem BERC 73](#_Toc532977612)

[Figură 14 Schema de baza a subsistemului tehnic de procesare, stocare si integrare a datelor 77](#_Toc532977613)

[Figură 15 Schema de baza a subsistemului tehnic de monitorizare generala a datelor 78](#_Toc532977614)

[Figură 16 Schema de baza a subsistemului tehnic de securitate si audit 79](#_Toc532977615)

[Figură 17 Niveluri arhitecturale 81](#_Toc532977616)

### Abrevieri și denumiri

| **Termen** | **Explicaţie** |
| --- | --- |
| AC | Autoritatea contractantă |
| AMPOC | Autoritatea de Management pentru Programul Operațional Competivitate |
| ACP | Autoritate de Certificare şi Plată |
| BPI | Buletinul Procedurilor de Insolvenţă |
| EC | Comisia Europeană |
| G2B | Government to Business |
| G2C | Government to Citizen |
| G2G | Government to Government |
| MCSI | Ministerul Comunicaţiilor şi Societății Informaționale |
| MFP | Ministerul Finanţelor Publice |
| MFE | Ministerul Fondurilor Europene |
| ONRC | Oficiul Naţional al Registrului Comerţului |
| OIPSI | Organism Intermediar pentru Promovarea Societăţii Informaţionale |
| ORCT | Oficiul Registrului Comerţului de pe lângă Tribunale |
| RCCC | Registrul Comerţului Central Computerizat al Oficiului Național al Registrului Comerțului |
| RC | Registrul Comerţului |
| BPI | Buletinul Procedurilor de Insolvenţă |
| RL | Registrul Litigiilor |
| SAE | Sistem de Arhiva Electronică |
| SOA | Service Oriented Architecture |
| SE | Sistemul Existent (sistemul informatic existent al ONRC) |
| BPEL | Business Process Execution Language – limbaj de definire a proceselor de afacere |
| UE | Uniunea Europeană |
| SNADR | Strategia Națională pentru Agenda Digitală România 2020 |
| TIC | Tehnologia Informației și Comunicații |

# Date generale

Prezentul caiet de sarcini conține cerințele generale ale Oficiului Naţional al Registrului Comerţului (ONRC) în vederea atribuirii contractului având ca obiect achiziționarea unui sistem informatic, compus din produse hardware, software și servicii de dezvoltare software, in vederea atingerii obiectivelor sale strategice, prevazute in legislatia aplicabila si in strategiile sectoriale.

## Structura organizatorică

Oficiul Naţional al Registrului Comerţului (ONRC) este o instituție publică cu personalitate juridică, organizată în subordinea Ministerului Justiției, finanțată integral de la bugetul de stat prin bugetul Ministerului Justiției.

În subordinea ONRC sunt organizate 42 oficii teritoriale, fără personalitate juridică, care funcționează pe lângă tribunale.

## Locații implementare proiect

Proiectul va fi implementat la nivel naţional, în 2 centre de date, și anume:

- la unul din sedile din Bucuresti ale Oficiului Naţional al Registrului Comerţului (ONRC/ORCT București), considerat site principal;

- la sediul ORCT Brasov, considerat site secundar.

şi implică toate cele 42 oficii ale registrului comerţului teritoriale (ORCT) precum şi sediile birourilor teritoriale care funcţionează pe lângă ORCT.

Adresele locaţiilor menţionate sunt prezentate în **Anexa 1**.

În afara birourilor teritoriale existente, se pot deschide şi alte birouri teritoriale în oraşele mari din diferite judeţe, unde numărul persoanelor supuse obligaţiei de înregistare în registrul comerţului este relativ mare.

## Legislaţia privind organizarea şi funcţionarea instituţiei

Funcţionarea şi organizarea **Registrului Comerțului** și **Buletinul Procedurilor de Insolvenţă** sunt reglementate de următorul cadru juridic:

* + la nivel național: [www.onrc.ro/index.php/ro/legislatie/legislatie-nationala](http://www.onrc.ro/index.php/ro/legislatie/legislatie-nationala)
  + la nivel european: [www.onrc.ro/index.php/ro/legislatie/legislatie-europeana](http://www.onrc.ro/index.php/ro/legislatie/legislatie-europeana)

**Registrul litigiilor**

În afara actelor normative menţionate anterior, Codul de procedură civilă, Codul Civil, Codul de Procedura Penala, codul Penal, Codul Muncii.

## Descrierea instituţiei

**Viziunea şi misiunea ONRC**

Viziunea ONRC este de a contribui la dezvoltarea mediului de afaceri din România, prin oferirea de servicii publice de calitate, flexibile şi orientate către nevoile specifice ale solicitanţilor.

Misiunea principală a Oficiului Naţional al Registrului Comerţului (ONRC) constă în prestarea serviciului public de ţinere a registrului comerţului şi de efectuare a publicităţii legale a actelor şi faptelor întreprinzătorilor, precum şi efectuarea procedurii de citare şi publicitate a procedurilor de insolvenţă.

**Valori ale ONRC**

1. **Orientarea către solicitanţii de servicii publice** – ONRC este o instituţie publică total dedicată solicitanţilor de servicii, adaptându-se la particularităţile activităţilor comerciale ale fiecăruia, astfel încât înregistrarea datelor întreprinzătorilor să fie făcută cu acurateţe;
2. **Accesibilitatea serviciilor** – ONRC caută continuu noi mijloace pentru a face serviciile “să vină mai aproape de solicitant” şi pentru a spori promptitudinea prestaţiei sale;
3. **Transparenţă**– transparenţa operaţiunilor în raport cu mediile de business şi guvernamentale este un deziderat constant al ONRC.

**Factorii cheie ai dezvoltării ONRC**

1. **Digitalizarea serviciilor destinate mediului de afaceri (G2B) pe baza identităţii electronice**, condiţie a autentificării on-line a utilizatorilor externi;
2. **Creșterea accesibilităţii serviciilor,** prin dezvoltarea serviciilor destinate mediului de afaceri (G2B) online, ca alternativă la serviciile de ghişeu;
3. **Integrarea cu aplicaţii de e-Payment în arhitectura de sistem a** ONRC în vederea facilitării plăţilor on-line;
4. **Implementarea practicilor europene cu privire la serviciile publice**;
5. **Respectarea prevederilor legislative cu privire la înregistrarea întreprinzătorilor şi editarea Buletinului Procedurilor de Insolvenţă**;
6. **Creşterea calităţii serviciilor,** în întâmpinarea nevoii crescânde a mediului de afaceri pentru servicii mai accesibile;
7. **Asigurarea securităţii** în condiţiile creşterii continue a disponibilităţii datelor pentru asigurarea confidenţialităţii şi continuităţii serviciilor on-line;
8. **Asigurarea interoperabilităţii interinstituţională** (juridic, organizațional, semantic, tehnic);
9. **Instruirea prealabilă a resurselor umane** pentru a îmbunătăţi interacţiunea operatorilor umani cu noile servicii;
10. **Creşterea eficienţei interne a ONRC,** prin implementarea unei infrastructuri IT moderne care să suporte serviciile destinate mediului de afaceri (G2B) şi serviciile destinate altor instituții guvernamentale (G2G) precum şi prin implementarea/automatizarea unor procese IT necesare exploatării eficiente a acestei infrastructuri.

**Strategia ONRC**

1. **În planul serviciilor destinate mediului de afaceri (G2B):**

* Atragerea de noi solicitanţi de servicii, prin prestaţii prompte, personalizate şi promovarea unor tarife accesibile;
* **Accesibilitate în furnizarea serviciilor**, inclusiv prin asigurarea disponibilităţii on-line a acestora;
* Dezvoltarea de servicii “user centric” (servicii cu valoare adăugată);
* Protejarea datelor transmise de solicitanţi.

1. **În planul serviciilor cu alte instituţii guvernamentale (G2G):**

* Identificarea permanentă de noi oportunităţi de **colaborare cu instituţii publice centrale şi judeţene** pentru promovarea intereselor comune (furnizarea de servicii cu valoare adăugată, elaborarea de propuneri legislative şi norme metodologice, etc.);
* Creşterea permanentă a numărului de protocoale de colaborare de schimb de date.

1. **În plan intra-instituţional:**
   1. *La nivel managerial*:
   * Creşterea posibilităţilor de **control şi monitorizare internă**;
   * **Evaluarea periodică a fluxurilor de lucru** şi de transmitere a informaţiilor precum şi identificarea oportunităţilor pentru optimizarea acestora.
   1. *În plan tehnologic:*
   * Evaluarea şi retehnologizarea permanentă a infrastructurii IT&C de suport, în scopul **derulării eficiente atât a serviciilor publice, cât şi a activităţilor interne**;
   * Asigurarea securităţii datelor preluate/procesate/ transmise;
   * **Creşterea interoperabilităţii interinstituţionale** la nivel de back-office/ front-office.
   1. *În domeniul resurselor umane*:
   * Managementul eficient al posturilor;
   * Fidelizarea angajaţilor, prin politici adecvate şi atractive;
   * Posibilităţi sporite de perfecţionare profesională, prin asigurarea accesului la programe de instruire ;
   * **Optimizarea comunicării intra-instituţionale** pe orizontală (atât în cadrul ONRC, cât şi ORCT), precum şi pe verticală (ONRC-ORCT).
   1. *În plan economico-financiar*:
   * Gestiunea eficientă a resurselor materiale şi financiare:
     + optimizarea proceselor de angajare, lichidare, ordonanţare şi plată a cheltuielilor;
     + planificarea anuală a bugetului şi investiţiilor pe baza analizelor de execuţie şi a prognozelor;
     + corelarea proceselor de achiziţii publice cu nevoile reale;
     + gestionarea corespunzătoare a patrimoniului.
   * Identificarea de noi pârghii pentru minimizarea costurilor

Atribuţiile ONRC sunt reglementate, în principal, de Legea nr. 26/1990 privind registrul comerţului, republicată, cu modificările şi completările ulterioare, precum şi de Regulamentul de organizare şi funcţionare a Oficiului Naţional al Registrului Comerţului şi a oficiilor registrului comerţului, aprobat prin Ordinul ministrului justiției nr. 1.082/C/2014, cu completările și modificările ulterioare.

Astfel, în conformitate cu prevederile cap. 1 din Regulamentul de organizare şi funcţionare a Oficiului Naţional al Registrului Comerţului şi a oficiilor registrului comerţului de pe lângă tribunale, ONRC este organizat pe 2 niveluri:

**• nivel național,** reprezentat de Oficiul National al Registrului Comerțului ce funcționează în subordinea Ministerului Justiției şi

**• nivel local,** reprezentat de cele 42 de Oficii ale registrului comerțului funcționează pe lângă tribunale (ORCT) sunt organizate în fiecare reședință de județ, în subordinea ONRC fără personalitate juridică

ONRC are atribuțiile care îi revin potrivit dispozițiilor Legii nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare, ale Legii nr. 31/1990 privind societățile, republicată, cu modificările și completările ulterioare, ale Legii nr. 359/2004 privind simplificarea formalităților la înregistrarea în registrul comerțului a persoanelor fizice, asociațiilor familiale și persoanelor juridice, înregistrarea fiscală a acestora, precum și la autorizarea funcționării persoanelor juridice, cu modificările și completările ulterioare, ale Ordonanței de urgență a Guvernului nr. 44/2008 aprobată, cu modificări și completări, prin Legea nr. 182/2016 privind desfășurarea activităților economice de către persoanele fizice autorizate, întreprinderile individuale și întreprinderile familiale, cu modificările și completările ulterioare, ale Legii nr. 85/2014 privind procedurile de prevenire a insolvenței și de insolvență, cu modificările și completările ulterioare, ale Legii nr. 151/2015 privind procedura insolvenţei persoanelor fizice, ale Ordinului Ministrului Justiției nr. 2.594/C/2008 pentru aprobarea Normelor metodologice privind modul de ținere a registrelor comerțului, de efectuare a înregistrărilor și de eliberare a informațiilor, precum și cele stabilite prin alte acte normative cu incidență în domeniul său de activitate.

Principalele funcții ale Oficiului National al Registrului Comerțului și ale oficiilor registrului comerțului de pe lângă tribunale, în conformitate cu dispozițiile Legii nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare, și ale Regulamentului de organizare şi funcţionare a Oficiului Naţional al Registrului Comerţului şi a oficiilor registrului comerţului de pe lângă tribunale, aprobat Ordin al M.J. nr. 1082/C/2014 cu modificarile și completările ulterioare, sunt:

**• funcţia de ţinere a registrului comerţului;**

**• funcţia de eliberare de înscrisuri şi de informare;**

**• funcţia de arhivare a înscrisurilor în baza cărora se efectuează înregistrările în registrul comerţului;**

**• funcţia de asistenţă pentru persoanele fizice şi juridice supuse înregistrării în registrul comerţului;**

**• funcţia de editare şi publicare a Buletinului procedurilor de insolvenţă.**

Cât privește **funcţia de ţinere a registrului comerţului** exercitată de oficiile registrului comerţului de pe lângă tribunale aceasta se poate detalia astfel:

- **înregistrarea tuturor persoanelor juridice supuse obligaţiei de înregistrare, a sucursalelor înființate de acestea, precum şi a persoanelor fizice autorizate, întreprinderilor individuale şi întreprinderilor familiale** care desfăşoară activităţi economice, cu sediul social/sediul profesional pe raza teritorială a tribunalului;

- **evidenţa datelor din documentele de înregistrare ale persoanelor supuse înregistrării, precum şi arhiva oficială a documentelor cu caracter constitutiv sau modificator ale acestora****, cea de publicitate legală****;**

- **transmiterea datelor în vederea înregistrării fiscale a contribuabililor şi obţinerii codului unic de înregistrare de la Ministerul Finanţelor Publice**, precum **şi a informaţiilor din cazierul fiscal**, în condiţiile legii;

- **eliberarea certificatului de înregistrare** și **a certificatului de înscriere de menţiuni**, după caz, precum și a **certificatelor constatatoare** emise în baza declaraţiilor-tip pe propria răspundere, conform Legii nr. 359/2004, cu modificările şi completările ulterioare, **şi transmiterea acestor declarații către autorităţile publice competente;**

- **transmiterea** **cererilor de înregistrare a documentului care atestă dreptul de folosinţă asupra spaţiului cu destinaţie de sediu social şi de eliberare a certificatului pentru spaţiul cu destinaţie de sediu social alături de actele doveditoare ale dreptului de folosinţă către administraţiile finanţelor publice,** în vederea emiterii certificatelor pentru spaţiul cu destinaţie de sediu social şi a adeverinţelor privind înregistrarea documentului care atestă dreptul de folosinţă asupra spaţiului cu destinaţie de sediu social.

Cât privește **serviciile publice oferite** de ONRC, acestea pot fi grupate, în principal, astfel:

* **asistență acordată persoanelor interesate pentru înregistrarea în registrul comerțului;**
* **înregistrarea în registrul comerțului, furnizarea de informații din registrul comerțului și eliberarea de copii;**
* **publicare și furnizare BPI, furnizarea de informații din BPI, de certificate constatatoare, de rapoarte istorice și eliberarea de copii.**

# Obiectivul achiziţiei

## Obiectivul general

Obiectivul general al proiectului este îmbunătățirea capacitatii administrative a ONRC prin asigurarea suportului informatic pentru procesul de publicare legală a actelor operatorilor economici, prin asigurarea unui cadru colaborativ intre angajați și prin întărirea securității și disponibilității sistemelor informatice ce sustin procesele de furnizare a serviciilor publice din responsabilitatea ONRC.

Beneficiile urmarite prin implementarea proiectului sunt următoarele:

* simplificarea şi reducerea barierelor administrative şi a birocratizării excesive, aferente proceselor şi reglementărilor, din perspectiva cetăţenilor şi a angajaţilor mediului de afaceri;
* reducerea timpului de procesare a datelor in vederea furnizarii serviciilor, cu o reducere corespunzătoare a costurilor;
* suport tehnologic sigur şi scalabil;
* asigurarea securitatii datelor şi controlul accesului la toate resursele sistemului;
* asigurarea disponibilităţii ridicate (24 x 7) a serviciilor;
* administrarea şi operarea la costuri reduse a infrastructurii şi componentelor soluţiei.

Pentru atingerea obiectivului general mai sus menționat ONRC iși propune extinderea Sistemului Informatic Integrat (SII) cu următoarele subsisteme informatice:

1. Subsistemul informatic „Buletinului Electronic al Registrului Comerțului” (SSIBERC) ce va permite extinderea si consolidarea sistemului de publicitate legala a actelor. Acest subsistem va fi utilizat de cel putin 500 de angajati ai ONRC iar serviciile online vor fi accesibile publicului larg, mediului de afaceri si autoritatilor publice prin intermediul portalului ONRC si a unei aplicatii mobile dezvoltate pentru platformele cele mai populare (cel putin Android si iOS);
2. Subsistemul informatic de tip “Colaborativ” (SSICO) ce va fi implementat în vederea sprijinirii angajaților ONRC în abordarea problemelor, pe activitați, în vederea unificarii activitaților necesare efectuarii de sarcini zilnice si periodice, gestionarii proceselor interne si a raspunsurilor catre mediul de afaceri si administrația publica;
3. Subsisteme informatice de monitorizare a performanțelor si asigurarea securitatii Sistemului Informatic Integrat al ONRC;

## Scopul proiectului

Achiziția de produse hardware, software și servicii de dezvoltare software în vederea implementarii sistemului informatic ce va asigura imbunatatirea capacitatii de publicare a actelor operatorilor economici, de colaborare intre angajati si de asigurare a securitatii si monitorizarii sistemului informatic integrat al ONRC.

Astfel, prin implementarea proiectului „**Imbunătățirea capacității de publicare a actelor operatorilor economici, de colaborare intre angajati si de asigurare a securitatii si monitorizarii sistemului informatic integrat ce susține procesele de furnizare a serviciilor publice aflate in responsabilitatea Oficiului Naţional al Registrului Comerţului**”, scopul ONRC este de:

* Reducere a timpului de efectuare a publicitatii legale;
* Desfasurare a activitatii în mod unitar la nivelul ONRC si a celor 42 de oficii teritoriale ale registrului comertului de pe lânga tribunale;
* Imbunatatire a capacitatilor institutiei de a furniza consecvent servicii care sa satisfaca cerintele solicitantilor (persoane juridice, persoane fizice, instituţii publice) coroborat cu reglementarile în vigoare prin crearea unui cadru colaborativ bazat pe tehnologii de ultima generatie;
* Îmbunatatire continua a calitatii si a disponibilitatii serviciilor furnizate;
* Crestere a credibilitatii si transparentei institutiei;
* Crestere a eficientei si eficacitatii interne;
* Aliniere la standardele europene.
* Se urmareste deschiderea de noi orizonturi privind modalitatile de furnizare a serviciilor publice si optimizarea proceselor decizionale si a fluxurilor de lucru în cadrul ONRC, în concordanta cu principiile debirocratizarii, maximizarii transparentei si integritatii, cresterii calitatii serviciilor furnizate.

Proiectul este finantat prin Programul Operational Capacitate Administrativa 2014-2020, Axa prioritara 2 - Administratie publica si sistem judiciar accesibile si transparente, cod 119317, cod SIPOCA 456.

## Situaţia actuală (Sisteme existente)

Începând cu data de 06 februarie 2012, ONRC utilizează la nivel naţional, atât la sediul central, cat si la sediile celor 42 de oficii ale registrului comerţului de pe lângă tribunale (ORCT) organizate în subordinea ONRC, inclusiv sediile birourilor teritoriale care funcţionează pe lângă ORCT, un nou sistem informatic integrat, pentru asigurarea de servicii on line destinate comunităţii de afaceri prin intermediul unui portal dedicat.

Sistemul informatic integrat ONRC este rezultatul proiectului *“Servicii on-line (de e-Guvernare) oferite de ONRC pentru comunitatea de afaceri prin intermediul unui portal dedicat”*, derulat in perioada 2009 - 2012, scopul fiind acela de a crea beneficii atât pentru utilizatori (cetăţeni şi mediul de afaceri), cât şi pentru administraţia publică.

**Beneficiarii direcţi** ai proiectului sunt reprezentaţi de următoarele categorii:

* Solicitanţii de servicii publice:
  + persoane juridice - servicii destinate mediului de afaceri - “Government to Business” (G2B);
  + persoane fizice - servicii destinate persoanelor fizice - “Government to Citizen” (G2C)
  + instituţii publice - servicii destinate institutţilor guvernamentale - “Government to Government” (G2G)
* Instituţiile publice colaboratoare, cu care ONRC dezvoltă relaţii de tip G2G

**Beneficiarii indirecţi** ai proiectului sunt următorii:

* Administraţia publică, datorită eficientizării furnizării serviciilor publice şi contribuţiei proiectului la reducerea birocraţiei;
* Angajaţii companiilor, datorită eliminării timpului alocat deplasării la sediile ONRC precum şi reducerii costurilor aferente utilizării serviciilor instituţiei.

Oferta de servicii a ONRC în raport cu segmentele mai sus menţionate este după cum urmează:

**Servicii destinate mediului de afaceri (G2B)**

* Înregistrarea tuturor persoanelor juridice supuse obligaţiei de înregistrare, a persoanelor fizice autorizate şi asociaţiiilor familiale, care desfaşoară activităţi economice
* Înscrierea de menţiuni pentru toate persoanele juridice, persoane fizice autorizate şi asociaţii familiale, care au fost supuse înregistrării
* Eliberarea de certificate constatatoare, extrase de registru şi alte înscrisuri pentru comercianţi
* Editarea Buletinului Procedurilor de Insolvenţă în care se publică citaţiile, convocările şi notificările actelor de procedură efectuate de instanţele judecătoreşti, practicienii în insolvență și alte persoane interesate
* Furnizarea de statistici cu privire la comercianţi
* Punerea la dispoziţie de informaţii legale despre firme din registrul central al comerţului
* Asigurarea liberului acces la informaţii de interes public.

**Servicii destinate instituţiilor guvernamentale (G2G)**

* Colaborarea cu autorităţile şi instituţiile publice responsabile pentru elaborarea, actualizarea şi utilizarea unor nomenclatoare unitare pe plan naţional
* Colaborarea cu autorităţile şi instituţiile publice implicate în constituirea şi autorizarea funcţionării comercianţilor, pentru simplificarea procedurilor specifice
* Obţinerea şi asigurarea evidenţei acordurilor privind folosirea denumirii firmei
* Editarea Buletinului Procedurilor de Insolvenţă în care se publică citaţiile, convocările şi notificările actelor de procedură efectuate de instanţele judecătoreşti, practicienii în insolvență și alte persoane interesate
* Punerea la dispoziţie de informatţi legale despre firme din registrul central al comerţului
* Furnizarea de statistici cu privire la comercianţi
* Asigurarea liberului acces la informaţii de interes public.

**Servicii destinate persoanelor fizice (G2C)**

* Punerea la dispoziţie de informaţii legale despre firme din registrul central al comerţului
* Furnizarea de statistici cu privire la comercianţi
* Asigurarea liberului acces la informaţiile de interes public.

Prin intermediul portalului de servicii online se asigură următoarele servicii:

**Secţiunea G2B şi G2C:**

* **Servicii on-line specifice Registrul Comerţului**
* Informarea iniţială on-line a solicitanţilor despre categoriile de informaţii/ servicii furnizate de ONRC;
* Asistenţa acordată solicitanţilor prin intermediul portalului;
* Formulare accesibile on-line;
* Atenţionarea profesioniștilor privind situaţia firmei;
* Furnizarea de informaţii on-line cu privire la stadiul dosarului;
* Publicarea lunară a publicaţiilor statistice de sinteză;
* Publicitatea pe internet a informaţiilor / documentelor prevăzute de lege;
* RECOM on-line - furnizarea de informaţii la zi din bazele de date privind profesioniștii înregistraţi la Registrul Comerţului – cu un grad de complexitate ridicat prin introducerea plăţii on-line;
* Verificarea şi rezervarea on-line a disponibilităţii firmei;
* Verificarea şi rezervarea disponibilităţii emblemei;
* Verificarea unicităţii sediului social şi asociatului;
* Completarea on-line şi offline şi transmiterea electronică a tuturor cererilor / formularelor (înmatriculări, menţiuni, cereri de informaţii şi documente etc.) utilizate în activitatea registrului comerţului, inclusiv a documentelor doveditoare, necesare pentru susţinerea cererilor, documente şi informaţii ce vor fi încărcate în baze de date specifice, utilizând tehnologii hardware şi software moderne şi performante – cu un grad de complexitate ridicat prin introducerea plăţii on-line;
* Furnizarea de statistici on-line personalizate, pe baza datelor înregistrate în registrul comerţului central computerizat - RCCC (informaţii la zi şi din istoric);
* Furnizarea de informaţii privind istoricul firmei, depus prin portal „furnizare informatii la zi, privind istoricul firmei, statistici”, inclusiv plăţi on-line;
* Eliberarea de copii semnate electronic cu certificat digital calificat din arhiva electronică de documente constituită din dosarele comercianţilor – cu plata on-line;
* Plăţi on-line;
* Atenţionarea profesioniștilor, prin mijloace electronice, asupra unor acte normative cu incidenţă în relaţia cu registrul comerţului;
* Actualizarea datelor de contact firmă (telefon, fax, e-mail, web-site).
* **Servicii on-line specifice Buletinului Procedurilor de Insolvenţă (BPI)**
* Transmiterea electronică automată din sistemul judiciar şi din alte sisteme (ex. practicieni în insolvenţă) în baza BPI, în format electronic, cu semnătură electronică, a actelor de procedură gestionate în cadrul publicării BPI şi informaţiilor din baze de date;
* Completarea şi transmiterea on-line, cu semnătură electronica, a formularelor, a actelor de procedură şi a informaţiilor pentru publicare în BPI, inclusiv plata on-line;
* Asistenţă BPI acordată solicitanţilor la completarea şi transmiterea on-line a actelor de procedură şi formularelor BPI;
* Transmiterea electronică automată din bazele BPI în sistemul judiciar şi în alte sisteme (ex. practicieni în insolvenţă), în format electronic, cu semnătură electronică, a dovezilor de publicare şi informaţiilor aferente;
* Acces on-line la informaţiile BPI gratuite prin extinderea categoriilor şi criteriilor de selectare disponibile utilizatorilor;
* Înştiinţarea profesioniștilor, prin mijloace electronice, asupra unor acte normative cu incidenţă în relaţia cu BPI (newsletter pe adresa de e-mail, mesaj pe cont personal);
* Furnizare on-line a publicaţiei BPI prin extinderea criteriilor de selectare disponibile utilizatorilor, inclusiv plata on-line;
* Completarea şi transmiterea on-line, cu semnătură electronică, a comenzilor pentru abonament BPI şi a cererilor de furnizare informaţii, inclusiv plata on-line;
* Furnizarea on-line de informaţii din bazele de date ale BPI;
* Publicarea lunară a situaţiilor statistice de sinteză din BPI.

**Secţiunea G2G**

* + **Servicii specifice Registrul Comerţului**
* Gestiunea denumirii de firma pentru care este nevoie de acordul Secretariatul General al Guvernului;
* Transmiterea electronică a actelor spre publicare în Monitorul Oficial;
* Transmiterea electronică a datelor şi declaraţiilor tip pe proprie răspundere către ministerele avizatoare;
* Transmiterea electronică automată de date către Institutul Naţional de Statistică, Garda Financiară etc. (16 instituţii)
* Transmiterea electronică de informaţii către Ministerul Finanţelor Publice - DGTI (date şi documente) necesare înregistrării în registrul comerţului (CUI şi informaţii din cazierul fiscal);
* Transmiterea electronică de informaţii şi înştiinţări către Administraţiile Financiare.
  + **Servicii specifice BPI**
* Transmiterea electronică automată din sistemul judiciar şi din alte sisteme (ex. practicieni în insolvenţă) în baza BPI, în format electronic, cu semnătură electronică, a actelor de procedură gestionate în cadrul publicării BPI şi informaţiilor baze de date;
* Completarea şi transmiterea on-line, cu semnătură electronica, a formularelor, a actelor de procedură şi a informaţiilor pentru publicare în BPI, inclusiv plata on-line;
* Asistenţă BPI acordată solicitanţilor la completarea şi transmiterea on-line a actelor de procedură şi formularelor BPI;
* Transmiterea electronică automată din bazele BPI în sistemul judiciar şi în alte sisteme (ex. practicieni în insolvenţă), în format electronic, cu semnătură electronică, a dovezilor de publicare şi informaţiilor aferente;
* Acces on-line la informaţiile BPI gratuite prin extinderea categoriilor şi criteriilor de selectare disponibile utilizatorilor;
* Furnizarea on-line a publicaţiei BPI prin extinderea criteriilor de selectare disponibile utilizatorilor, inclusiv plata on-line;
* Completarea şi transmiterea on-line, cu semnătură electronică, a comenzilor pentru abonament BPI şi a cererilor de furnizare informaţii, inclusiv plata on-line;
* Furnizarea on-line de informaţii din bazele de date ale BPI;
* Publicarea lunară a situaţiilor statistice de sinteză din BPI.

Obiectivele specifice ale proiectului de implementare au fost:

* Facilitarea accesului utilizatorilor (cetăţeni, mediul de afaceri şi administraţia publică) şi creşterea celerităţii în furnizarea serviciilor prin punerea la dispoziţia acestora a serviciilor publice prin mijloace electronice, on-line, oferind un număr de 34 servicii publice on-line prin intermediul unui portal dedicat, dintre care 24 servicii publice on-line nou create în cadrul proiectului implementat;
* Creşterea numărului de utilizatori ai serviciilor publice on-line oferite de ONRC, estimându-se un ritm anual de creştere de 5% a numărului de utilizatori în perioada ulterioara implementării proiectului, atingându-se un procent de 25% în al cincilea an;
* Eficientizarea fluxului de informaţii în relaţiile cu instituţiile avizatoare şi cele guvernamentale cu care ONRC are încheiate protocoale de colaborare - 16 instituţii publice vor beneficia de reducerea timpului necesar obţinerii informaţiilor din registrul central al comertului conform acordurilor inter-instituţionale încheiate;
* Creşterea gradului de instruire a personalului ONRC în vederea utilizării noii infrastructuri TIC implementate, prin instruirea unui număr de 100 persoane, atât la nivel central cât şi local;
* Implementarea unui serviciu de plăţi on-line (e-payment) pentru gestionarea completă a serviciilor electronice comerciale oferite de ONRC, asigurându-se cel mai înalt nivel de complexitate al noului sistem informatic.;
* Implementarea unei infrastructuri IT&C moderne, care să deservească în mod optim derularea activităţilor specifice ONRC (ex.: creşterea performantelor şi securităţii sistemului, monitorizarea sistemului informatic, etc.), vizându-se dotarea cu infrastructura IT&C moderna a celor 43 de locaţii în care ONRC oferă servicii publice.

Activitatea instituţiei este aproape complet informatizată și este susținută 24x7 prin intermediul sistemului informatic integrat (SII) al ONRC, instituția fiind dotată cu echipamentele, produsele software şi serviciile informatice aferente necesare desfăşurării activităţii.

**Sistemul informatic al ONRC are, în principal, următoarele caracteristici:**

* este suportul de baza al întregii activități desfășurate la nivel local și central al ONRC;
* este unitar – folosește aceeași metodologie, aceleași proceduri de lucru, nomenclatoare, structuri de date şi programe la toate oficiile registrului comertului teritoriale;
* furnizează direct, din datele înregistrate în registrul computerizat, actele eliberate solicitanţilor privind soluţionarea cererilor;
* asigură accesul partajat şi controlat la baza de date atât pentru introducerea datelor cât şi pentru furnizarea rapoartelor;
* este dotat cu sisteme de protecţie fiind permis accesul numai persoanelor autorizate din cadrul sistemului registrului.

Sistemul informatic integrat (SII) al ONRC este un sistem cu o viziune și abordare integrată, distribuit teritorial şi ierarhizat pe 2 nivele:

* **nivel central** care asigură în timp real:
  + centralizarea datelor înregistrate;
  + publicarea informațiilor conform prevederilor legale;
  + depunerea/eliberarea documentelor on-line prin intermediul portalului de servicii online;
  + interconectarea cu alte sisteme informatice la nivel național/local (G2G);
  + administrarea la nivel teritorial;
* **nivel teritorial** care gestionează întregul proces de înregistrare a profesioniștilor – inclusiv comunicaţia cu alte instituţii pe plan local, în vederea efectuării înregistrărilor, eliberarea de certificate constatatoare şi furnizarea de informaţii.

**Sistemul informatic integrat al ONRC conţine următoarele componente:**

* **Componenta Registrul Comerţului**, distribuită teritorial şi ierarhizată pe 2 nivele:
* **nivelul central**, care asigură centralizarea, corelarea şi administrarea informaţiilor de la nivel teritorial, în timp real;
* **nivelul teritorial**, care gestionează întregul proces de înregistrare a comercianţilor – inclusiv comunicaţia cu alte instituţii pe plan local, în vederea efectuării înregistrărilor, eliberarea de certificate constatatoare şi furnizarea de informaţii.
* **Baza de date** a registrului comerţului, la nivel local şi la nivel central, se structurează în 2 componente:
* baza de date cu informaţiile la zi ale persoanelor fizice şi juridice înregistrate în registrul comerţului, supusă frecvent interogărilor şi prelucrărilor statistice;
* baza de date de arhivă conţinând istoricul firmei cu datele iniţiale de la înmatriculare şi toate menţiunile ulterioare, supusă interogărilor şi prelucrărilor statistice.
* **Componenta Registrul Litigiilor**, care este un sistem centralizat, utilizat la nivel naţional de ONRC şi ORCT-uri.
* **Componenta Buletinul Procedurilor de Insolvenţă**, care este un sistem centralizat, utilizat la nivel naţional de ONRC şi ORCT-uri.

Pe lângă componentele descrise, la nivel central există şi următoarele sub-sisteme:

1. **Sistemul de arhivare electronică (SAE) a documentelor**, cuprinzând imaginea în format electronic (.PDF) a cererilor de înregistrare şi a documentelor care au stat la baza înregistrărilor care sunt scanate şi indexate la nivel local şi apoi transmise la nivel central; acest sistem este supus interogărilor utilizatorilor din ORCT
2. **Bazele de date financiar contabile şi pentru managementul resurselor umane** sunt formate din două componente:

* componenta "resurse umane şi calcul salarii" se constituie numai la nivel central şi este formată din înregistrări în tabele FOXPRO care sunt supuse prelucrărilor şi interogărilor, generându-se documente, declaraţii către autorităţi şi către ordonatorul principal de credite, precum şi diverse statistici în format DOC şi XLS. Componenta "resurse umane" are o subcomponenta ce include foaia colectivă de prezenţă care se generează local şi se transmite la sediul central;
* componenta "financiar contabilă" se constituie din subcomponente la nivel local unde se realizează înregistrarea încasărilor şi facturarea clienţilor în baza notelor de calcul, evidenţa materialelor, obiectelor de inventar şi mijloacelor fixe, înregistrarea diverselor documente şi a plăţilor între subunităţi, şi se generează balanţa de verificare. Baza de date este transmisă la sediul central unde se verifică datele înregistrate, se centralizează balanţele de verificare şi se generează documente, declaraţii către autorităţi şi către ordonatorul principal de credite, se fac plăţi pentru furnizori, precum şi pregătirea de statistici în format DOC şi XLS.

Sistemul este dezvoltat pe tehnologii Oracle şi Java. Aplicaţiile care fac parte din Sistemul Informatic Integrat al ONRC (SII) sunt următoarele:

* Registratura Locaţie (REG)
* Registrul Litigiilor (RL)
* Registrul Comerţului (RC)
* Buletinul Procedurilor de Insolvenţă (BPI)
* Portalul Serviciilor Online al instituţiei ONRC (include servicii online RC şi BPI)
* Nomenclatoare (centrale – RC+RL, BPI şi locale)
* Antecalcul (TAX)
* Publicare date pentru alte instituţii (prin intermediul portalului)
* Sistem de securitate internă (central şi local) şi externă (Aplicația Centralizată de Management Utilizatori - ACMU)
* Raportare Analitică

**Aria de acoperire geografică şi funcțională a sistemului informatic al ONRC**

Locatiile, sistemele si aplicatiile care fac parte din Sistemul Informatic Integrat sunt următoarele:

* Locatii:
* Sediul central al ONRC Bucuresti
* Sediile ORCT din tara si din Bucuresti (42 locatii)
* Birourile teritoriale ale ORCT
* Aplicatii SII:
* Registratura Locatie (RG)
* Registrul Litigiilor (RL)
* Registrul Comertului (RC)
* Buletinul Procedurilor de Insolventa (BPI)
* Portalul Serviciilor Online al institutiei ONRC
* Nomenclatoare (RC+RL, BPI)
* Antecalcul
* Publicare date catre alte institutii
* Sistem de securitate interna (central si local) si externa (Aplicatia Centralizata de Management Utilizatori - ACMU)
* Raportare Analitica
* Alte aplicatii istorice (implementate anterior proiectului e-Guvernare):
* Casierie – aplicatie ce ruleaza la nivel central si local (FOXPro)
* CAPTIVA – aplicatie de arhivare ce ruleaza la nivel local si central (EMC Captiva)
* SAE (Sistemul de Arhivare Electronica) – aplicatie ce ruleaza la nivel central (WebSphere AS, DB2 Content Manager, Java, UDB DB2)
* Clienti/ facturi – aplicatie din suita ERP ce ruleaza la nivel central si local (FOXPro) si care administreaza din punct de vedere contabil clientii ONRC generand facturi si monitorizand stadiul acestor facturi.
* Aplicatii externe:
* Obtinere CUI – MFP
* Obtinere cazier fiscal – MFP
* Monitorul Oficial
* ECRIS - MJ
* SEN - „Platformă pentru integrarea serviciilor de e-guvernare în Sistemul Electronic Naţional” din cadrul Ministerului Comunicaţiilor şi Societăţii Informaţionale reprezentate de PCU şi OneStopShop
* Autoritati certificate digitale calificare

**Infrastructura hardware**

În fiecare ORCT funcţionează reţele locale proprii, cablare structurată voce-date, în general.

Principalele echipamente din dotarea fiecărui ORCT:

**LAN**

* două servere de baze de date cu sisteme de operare Linux (RedHat, Fedora etc.), Samba, NFS, etc.;
* un server de comunicaţii (Internet) cu sistem de operare Linux (RedHat, Fedora etc.) pe care sunt instalate: server de mail, proxy, server HTTP etc.;
* un server/o staţie de lucru dedicat/dedicată cu sistem de operare Windows Server/Windows XP pentru sistemul de arhivare electronică a documentelor;
* staţii de lucru cu sistem de operare Windows XP Professional şi Windows Vista Ultimate, Windows 7, Windows 8.x, Windows 10 Professional;
* echipamente de reţea (dulapuri de conexiuni, switch-uri);
* echipamente de comunicaţie (routere CISCO);
* alte echipamente: imprimante, scanere, inscripţionatoare DVD, switch-uri KVM, copiatoare etc.

**DMZ**

* Infrastructura SII

La sediul ORCT este implementată o arhitectura bazată pe un firewall (un cluster cu 2 noduri), care împarte reţeaua în trei zone:

* + zona demilitarizată (DMZ) – în care sunt amplasate echipamentele SII;
  + reţeaua internă care cuprinde serverele interne (file servere şi baze de date), staţii de lucru, imprimante, scanere, echipamente active de reţea (switch-uri) – care nu sunt accesibile din exterior sau din ORCT, ci numai din reţeaua internă, având adrese IP din clase private;
  + zona reţelei virtuale private (VPN) a sistemului registrului comerţului.

La sediul central al ONRC există o reţea locală proprie, cablare structurată voce-date, cat. 6.

Principalele echipamente din dotarea ONRC sunt următoarele:

**LAN si DMZ**

* + servere de reţea locală şi baze de date cu sisteme de operare Linux (RedHat) şi SGBD FoxPro şi Oracle;
  + servere care asigură servicii Internet şi Intranet (servere de mail, DNS, web etc.) cu sisteme de operare Linux (Red Hat);
  + servere dedicate pentru aplicaţii/soluţii;
  + servere de baze de date;
  + servere pentru sistemul de arhivare electronică a documentelor;
  + servere pentru Buletinul Procedurilor de Insolvenţă;
  + echipamente de reţea: dulapuri de conexiuni, switch-uri;
  + echipamente de comunicaţie (routere CISCO);
  + staţii de lucru cu sistem de operare Windows XP Professional şi Windows Vista Ultimate, Windows 7, Windows 8.x, Windows 10 Professional;
  + alte echipamente: imprimante, scanere, inscripţionatoare DVD, switch-uri KVM, copiatoare etc.

**DMZ-uri SII**

* + Infrastructura SII.

La sediul central este implementată o arhitectura bazată pe un firewall (un cluster cu 2 noduri), care împarte reţeaua ONRC în mai multe zone:

* + zona demilitarizată (DMZ) – în care sunt amplasate echipamentele (în principal servere) care trebuie să fie accesibile din exterior şi din ORCT (din Internet şi Intranet);
  + DMZ-uri infrastructura SII;
  + reţeaua internă care cuprinde serverele interne (file servere şi baze de date), staţii de lucru, imprimante, scanere, echipamente active de reţea (switch-uri) – care nu sunt accesibile din exterior sau din ORCT, ci numai din reţeaua internă, având adrese IP din clase private;
  + zona reţelei virtuale private (VPN) a sistemului registrului comerţului;
  + zona reţelei virtuale private (Extranet VPN) cu instituțiile publice;

**Infrastructura de comunicaţii**

În sistemul registrului comerţului sunt instalate două tipuri de comunicaţii:

* în cadrul sistemului registrului comerţului: între ONRC şi ORCT precum şi cele între birourile teritoriale şi biroul ORCT de care aparţin şi ONRC;
* comunicaţii Internet – cu alte instituţii şi clienţi.

**Comunicaţiile în cadrul sistemului registrului comerţului** sunt necesare, în principal, pentru:

* transmisia permanentă de informaţii şi documente de la ORCT către ONRC, inclusiv a informaţiilor necesare obţinerii codului unic de înregistrare (CUI) şi a cazierului fiscal de la Ministerul Finanţelor Publice (MFP);
* difuzarea de documente, adrese, aplicaţii, manuale etc., în special prin tehnologia web (intranet);
* acces la sistemul informatic integrat (SII);
* acces la sistemul de arhivare electronică a documentelor (SAE);
* intervenţii tehnice si configurări realizate de la distanţă de către Serviciul AIC, DTI din cadrul ONRC, pe echipamentele din cadrul ORCT;

**Comunicaţiile Internet** sunt necesare, în principal, pentru:

* acces la site-ul [www.onrc.ro](http://www.onrc.ro/), la serviciile SII oferite prin [portal.onrc.ro](http://www.onrc.ro/), la site-ul Buletinului procedurilor de insolvenţă [www.buletinulinsolventei.ro](http://www.buletinulinsolventei.ro/), [www.bpi.ro](http://www.bpi.ro/);
* schimb de informaţii şi documente cu alte instituţii;
* comunicarea cu furnizorii şi prestatorii de servicii;
* realizarea update-urilor la sisteme de operare, produse software, drivere, semnături la produsele antivirus, produse legislative, etc;
* acces la informaţii necesare în activitatea instituţiei;
* comunicarea cu clienţii serviciilor ONRC;

Comunicaţiile în cadrul sistemului registrului comerţului sunt realizate prin reţeaua virtuală privata (VPN) a registrului comerţului implementată, în baza H.G. nr. 1213/2005, prin Serviciul de Telecomunicaţii Speciale. Toate comunicaţiile sunt criptate (prin protocolul IPSec) utilizând modulul de criptare din router-ele CISCO instalate în toate locaţiile.

Pentru BPI şi înregistrarea hotărârilor judecătoreşti în registrul comerţului, altele decât cele în materia insolvenţei, trebuie activată reţeaua de comunicaţii VPN – ONRC/ORCT – instanţe judecătoreşti, Ministerul Justiţiei, alte structuri din sistemul judiciar, prin STS.

Fiecare locaţie are 2 conexiuni VPN :

* o conexiune principală, în majoritatea locaţiilor pe fibră optică;
* o conexiune de backup pe diferite medii de comunicaţie.

La aceasta reţea virtuală privată sunt conectate şi birourile teritoriale ale ORCT.

**Comunicaţiile Internet**

Sunt asigurate de diferiţi furnizori de servicii Internet, selectaţi prin licitaţii publice:

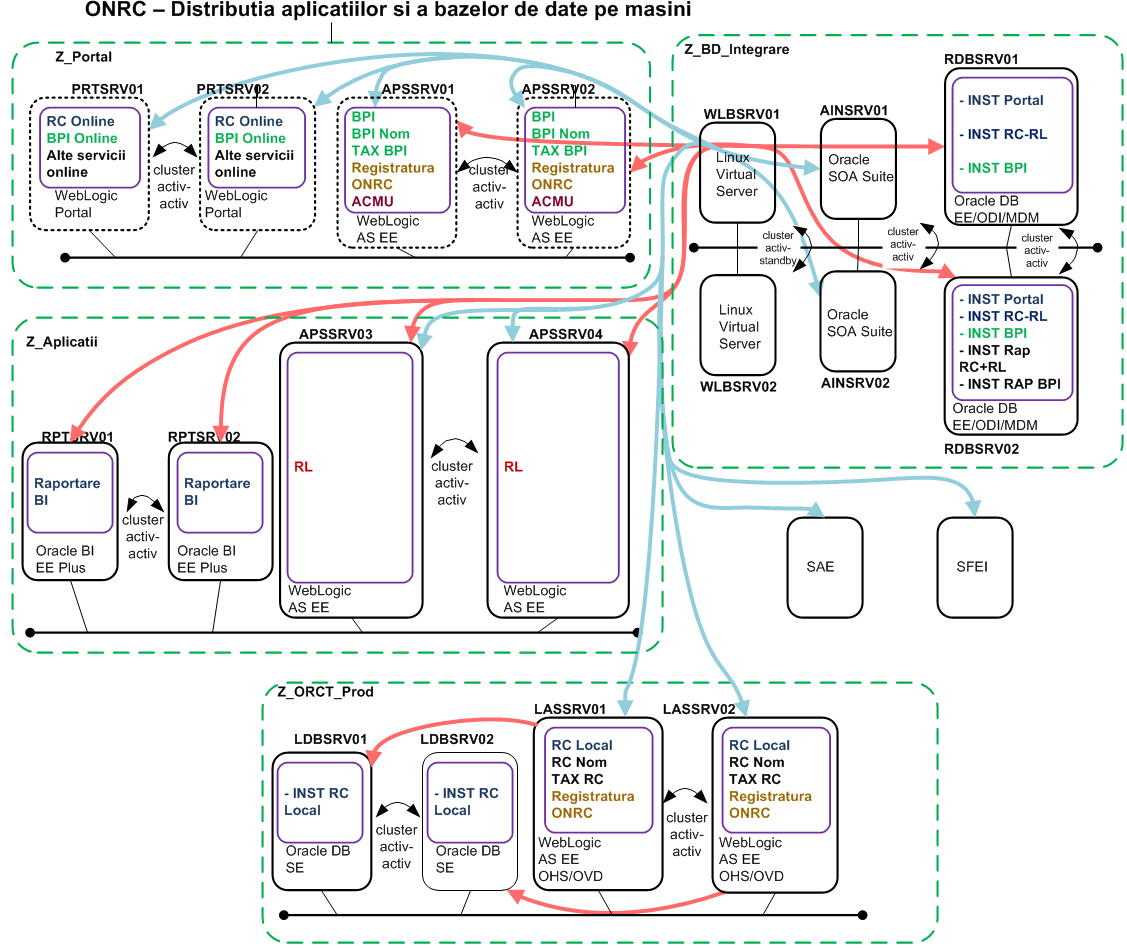
* ONRC are două conexiuni permanente pe fibră optică (principală şi de backup);
* ORCT Bucureşti are o conexiune permanentă;
* celelalte ORCT au conexiuni permanente pe medii fizice diferite (fibră optică, linie telefonică închiriată) cu rate de transfer optime activităţii.

Birourile teritoriale nu au conexiuni Internet proprii, utilizând comunicaţiile Internet de la sediul ORCT de care aparţin.

Diagrama urmatoare prezinta sistemele plasate in locatia ONRC, mediul de productie:



Figură 1 Arhitectura hardware ONRC (mediu de productie)



Figură 2 Distributia aplicatiilor si bazelor de date pe servere

| **Zona** | **Denumire,** | **Rol** | **Platforma hardware** | **Sistem de operare** | **Software** |
| --- | --- | --- | --- | --- | --- |
| Z\_DMZ1 | ELBSRV01 | Load Balancer acces din internet si extranet - utilizatori si sisteme. Nod activ. | Intel  4core  6GB | Linux | Linux Virtual Server |
| Z\_DMZ1 | ELBSRV02 | Load Balancer acces din intenet si extranet utilizatori si sisteme. Nod stand-by. | Intel  4core  6GB | Linux | Linux Virtual Server |
| Z\_DMZ1 | ESCSRV01 | HTTP Server si verificare acces pentru utilizatori din Internet | p570  4core  16GB | AIX | Oracle HTTP Server  Oracle WebGate |
| Z\_DMZ1 | ESCSRV02 | HTTP Server si verificare acces pentru utilizatori | p570  4core  16GB | AIX | Oracle HTTP Server  Oracle WebGate |
| Z\_DMZ2 | ILBSRV01 | Load Balancer acces utilizatori din Intranet. Nod activ. | Intel  4core  6GB | Linux | Linux Virtual Server |
| Z\_DMZ2 | ILBSRV02 | Load Balancer acces utilizatori din Intranet. Nod stand-by. | Intel  4core  6GB | Linux | Linux Virtual Server |
| Z\_DMZ2 | ISCSRV01 | HTTP Server si verificare acces pentru utilizatori din Intranet. | p570  4core  16GB | AIX | Oracle HTTP Server Oracle WebGate |
| Z\_DMZ2 | ISCSRV02 | HTTP Server si verificare acces pentru utilizatori din Intranet. | p570  4core  16GB | AIX | Oracle HTTP Server  Oracle WebGate |
| Z\_PORTAL | PRTSRV01 | Server aplicatie portal pentru utilizatori Internet. | partitie logica p570  4core  16GB | AIX | Oracle WebLogic Portal |
| Z\_PORTAL | PRTSRV02 | Server aplicatie portal pentru utilizatori Internet. | partitie logica p570  4core  16GB | AIX | Oracle WebLogic Portal |
| Z\_ PORTAL | WSCSRV01 | Server de test aplicatii interne pentru servicii portal. | p570  4core  16GB | AIX | Oracle WebLogic Server Enterprise Edition |
| Z\_PORTAL | WSCSRV02 | Server de test aplicatii interne pentru servicii portal. | p570  4core  16GB | AIX | Oracle WebLogic Server Enterprise Edition |
| Z\_Aplicatii | RPTSRV01 | Server de raportare pentru aplicatiile interne | Intel  4core  16GB | Linux | Oracle Business Intelligence Enterprise Edition Plus |
| Z\_Aplicatii | RPTSRV02 | Server de raportare pentru aplicatiile interne | Intel  4core  16GB | Linux | Oracle Business Intelligence Enterprise Edition Plus |
| Z\_ Aplicatii | APSSRV01 | Server aplicatii interne pentru servicii portal BPI si Taxe. | partitie logica p570  4core  16GB | AIX | Oracle WebLogic Server Enterprise Edition |
| Z\_ Aplicatii | APSSRV02 | Server aplicatii interne pentru servicii portal BPI si Taxe. | partitie logica p570  4core  16GB | AIX | Oracle WebLogic Server Enterprise Edition |
| Z\_Aplicatii | APSSRV03 | Server aplicatii interne pentru utilizatorii interni. Aplicatiile centrale de Registratura, RC si RL. | p570  8core  32GB | AIX | Oracle WebLogic Server Enterprise Edition |
| Z\_Aplicatii | APSSRV04 | Server aplicatii interne pentru utilizatorii interni. Aplicatiile centrale de Registratura, RC si RL. | p570  8core  32GB | AIX | Oracle WebLogic Server Enterprise Edition |
| Z\_Aplicatii | storage | Server de stocare de 4.5TB. | N/A | Linux | N/A |
| Z\_DB\_Integrare | RDBSRV03 | Server de baze de date ce va prelua parte din datele din productie. | Intel  4core  6GB | Linux | Oracle Database Enterprise Edition  Oracle Real Application Clusters |
| Z\_DB\_Integrare | RDBSRV04 | Server de baze de date ce va prelua parte din datele din productie. | Intel  4core  6GB | Linux | Oracle Database Enterprise Edition  Oracle Real Application Clusters |
| Z\_DB\_Integrare | AINSRV01 | Server servicii web si procese. | p570  4core  16GB | AIX | Oracle Service Bus  Oracle BPEL Process Manager  Oracle Business Activity Monitoring |
| Z\_DB\_Integrare | AINSRV02 | Server servicii web si procese. | p570  4core  16GB | AIX | Oracle Service Bus  Oracle BPEL Process Manager  Oracle Business Activity Monitoring |
| Z\_DB\_Integrare | RDBSRV01 | Server baza de date centrala si integrare la nivel de date.  Instanta SIIHQ1  VIRT.IP: | p570  8core  64GB | AIX | Oracle Database Enterprise Edition  Oracle Real Application Clusters  Oracle Partitioning  Orace Advanced Security  Oracle Data Integration Suite  Oracle Master Data Management |
| Z\_DB\_Integrare | RDBSRV02 | Server baza de date centrala si integrare la nivel de date.  Instanta SIIHQ2.  VIRT.IP: | p570  8core  64GB | AIX | Oracle Database Enterprise Edition  Oracle Real Application Clusters  Oracle Partitioning  Orace Advanced Security  Oracle Data Integration Suite  Oracle Master Data Management |
| Z\_DB\_Integrare | RDBSRVQ | Server de baze de date utilizat pentru Ad-Hoc querys pe baza de date centrala. | Intel  4core  6GB | AIX | Oracle Database Enterprise Edition |
| Z\_Securitate | ACCSRV01 | Server politici de acces la resurse. Server primar. | Intel  4core  16GB | Linux | Oracle Access Manager Access Server  Oracle Identity Server |
| Z\_Securitate | ACCSRV02 | Server politici de acces la resurse. Server secundar. | Intel  4core  16GB | Linux | Oracle Access Manager Access Server  Oracle Identity Server |
| Z\_Securitate | IDMSRV01 | Server director si management identitati. Server primar. | p570  4core  16GB | AIX | Oracle Virtual Directory  Oracle Internet Directory  Oracle Directory  Integration Platform |
| Z\_Securitate | IDMSRV02 | Server director si management identitati. Server secundar. | p570  4core  16GB | AIX | Oracle Virtual Directory  Oracle Internet Directory  Oracle Directory Integration Platform |
| Z\_Management | MGTSRV01 | Server management sisteme | Intel  4core  16GB | Linux | Oracle Enterprise Manager Grid Control  IBM Tivoli Storage Manager |
| Z\_Management | CDRSRV01 | Server pentru controlul datelor replicate | Intel  4core  16GB | Linux | Oracle Data Integrator Operator |
| Z\_PKI | PKISRV01 | Server solutie PKI | Intel  4core  6GB | Windows 2008 Enterprise Edition | Window 2008 Server Enterprise Certification Authority cu rolurile de Agent de inrolare  Certification Authority cu functia de Agent de Recuperare a Cheilor (Key Recovery Agent).  (Enrollment Agent) |
| Z\_PKI | PKISRV02 | Server solutie PKI | Intel  4core  6GB | Windows 2008 Enterprise  Edition | Windows 2008 Server Enterprise  Certification Authority cu functia de Agent de Recuperare a Cheilor (Key Recovery Agent). |
| Z\_PKI | PKISRV03 | Server solutie PKI | Intel  4core  6GB | Windows 2008 Enterprise Edition | Window 2008 Server Enterprise Certification Authority cu functia de OCSP Server |
| - | STGSRV01 | Server stocare externa | IBM DS5100  10 TB | N/A | N/A |
| - | LIBSRV01 | Biblioteca de benzi | IBM TS3310 | N/A | N/A |

Diagrama urmatoare prezinta sistemele plasate in Bucuresti, mediul de productie:



Figură 3 Arhitectura fizica ORCT Bucuresti

| **Zona** | **Denumire,**  **IP** | **Rol** | **Platforma hardware** | **Sistem de operare** | **Software** |
| --- | --- | --- | --- | --- | --- |
| Z\_ORCTB\_Prod | BDBSRV01 | Server baza de date si integrare la nivel de date. In cluster cu BDBSRV02. | p570  8core  64GB | AIX | Oracle Database Enterprise Edition  Oracle Real Application Clusters  Oracle Partitioning  Orace Advanced Security |
| Z\_ORCTB\_Prod | BDBSRV02 | Server baza de date si integrare la nivel de date. In cluster cu BDBSRV02. | p570  8core  64GB | AIX | Oracle Database Enterprise Edition  Oracle Real Application Clusters  Oracle Partitioning  Orace Advanced Security |
| Z\_ORCTB\_Prod | BASSRV01 | Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG).  In cluster cu serverele BASSRV02, BASSRV03, BASSRV04. | p570  8core  16GB | AIX | Oracle WebLogic Server Enterprise Edition  Oracle HTTP Server  Oracle Virtual Directory |
| Z\_ORCTB\_Prod | BASSRV02 | Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluster cu serverele BASSRV01, BASSRV03, BASSRV04. | p570  8core  16GB | AIX | Oracle WebLogic Server Enterprise Edition  Oracle HTTP Server  Oracle Virtual Directory |
| Z\_ORCTB\_Prod | BASSRV03 | Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluter cu cu serverele BASSRV01, BASSRV02, BASSRV04. | p570  8core  16GB | AIX | Oracle WebLogic Server Enterprise Edition  Oracle HTTP Server  Oracle Virtual Directory |
| Z\_ORCTB\_Prod | BASSRV04 | Server de aplicatie pentru aplicatiile locale (RC, RL, Antecalcul, REG). In cluster cu cu serverele BASSRV01, BASSRV02, BASSRV03. | p570  8core  16GB | AIX | Oracle WebLogic Server Enterprise Edition  Oracle HTTP Server  Oracle Virtual Directory |
| Z\_ORCTB\_Prod | WLBSRV01 | Load Balancer acces servicii web. Nod activ. In cluster cu WLBSRV02. | Intel  4core  6GB | Linux | Linux Virtual Server |
| Z\_ORCTB\_Prod | WLBSRV02 | Load Balancer acces servicii web. Nod stand-by. In cluster cu WLBSRV01. | Intel  4core  6GB | Linux | Linux Virtual Server |
| Z\_ORCTB\_Prod | BBKPSRV01 | Server de backup centralizat pentru infrastructura din ORCT Bucuresti. | Intel  4core  6GB | Linux | IBM Tivoli Storage Manager |
| Z\_ORCTB\_Prod | BSTSRV01 | Server de stocare externa | IBM DS5100  10 TB | N/A | N/A |
| Z\_ORCTB\_Prod | BLISRV01 | Biblioteca de benzi | IBM TS3310 | N/A | N/A |



Figură 4 Arhitectura fizica ORCT Medii si Mici

| **Zona** | **Denumire,**  **IP** | **Rol** | **Platforma hardware** | **Sistem de operare** | **Software** |
| --- | --- | --- | --- | --- | --- |
| Z\_ORCT\_Prod | SDBSRV01 | Server baza de date si integrare la nivel de date. | Intel  4core  24GB | Linux | Oracle Database Enterprise Edition  Oracle Real Application Clusters  Oracle Partitioning  Orace Advanced Security |
| Z\_ORCT\_Prod | SDBSRV02 | Server baza de date si integrare la nivel de date. | Intel  4core  24GB | Linux | Oracle Database Enterprise Edition  Oracle Real Application Clusters  Oracle Partitioning  Orace Advanced Security |
| Z\_ORCT\_Prod | SASSRV01 | Server de aplicatie pentru aplicatiile locale (REG, RC si Taxe) | Intel  4core  24GB | Linux | Oracle WebLogic Server Enterprise Edition  Oracle HTTP Server  Oracle Virtual Directory |
| Z\_ORCT\_Prod | SASSRV02 | Server de aplicatie pentru aplicatiile locale (REG, RC si Taxe) | Intel  4core  24GB | Linux | Oracle WebLogic Server Enterprise Edition  Oracle HTTP Server  Oracle Virtual Directory |
| Z\_ORCT\_Prod | SSTSRV01 | Server de stocare externa | IBM DS5020  0.9 TB | N/A | N/A |

**Infrastructura Software**

**Aplicatii existente**

În sistemul informatic sunt utilizate mai multe categorii de produse software.

La nivelul ORCT:

* sisteme de operare:
  + pe servere: Linux (RedHat, Fedora etc.) ;
  + pe staţii de lucru – Windows XP Professional, Windows Vista, Windows 7, Windows 8.x, Windows 10 Professional;
* pachete software antivirus pe fiecare staţie de lucru şi pe serverul de mail;
* pachete de tip Office: MS Office, Open Office;
* EMC Captiva – pentru sistemul de arhivare electronică a documentelor;
* alte pachete software pe staţii de lucru: Adobe Acrobat Standard (pentru semnare electronică a documentelor pdf), Total Commander, Win Rar, Corel Draw etc.

La nivelul ONRC:

* sisteme de operare:
  + pe servere: IBM AIX cu HACMP, Linux (RedHat, Fedora etc.) cu Samba, NFS, etc.; Windows 2000 Server, Windows 2003 Server;
  + pe staţiile de lucru: Windows XP Professional, Windows Vista, Windows 7, Windows 8.x, Windows 10 Professional;
* servere de baze de date (sisteme de gestiune de baze de date): Oracle Database 11g, Oracle RAC, IBM DB2, IBM DB2 Content Manager (ultimele două pe serverele de la sistemul de arhivare electronică a documentelor;
* servere web: apache, IBM HTTP server;
* servere de aplicaţii: Oracle Application Server 11g, WAS Network Deployment,
* software pentru back-up sisteme;
* software pentru dezvoltare aplicaţii: Oracle Developer Suite;
* produse Quest pentru monitorizare și replicare baze de date Oracle;
* servere ce asigură diverse servicii Internet: email, web, dns, nfs etc.;
* pachete software antivirus pe fiecare staţie de lucru şi pe serverul de mail;
* pachete de tip Office : MS Office, Open Office;
* servere pentru sistemul de arhivare electronică a documentelor: Captiva 5.x;
* alte pachete software pentru dezvoltare aplicaţii, procesare documente: Adobe Acrobat Standard (pentru semnare electronică a documentelor pdf), Macromedia, Adobe Acrobat Professional, produse Macromedia etc.

Aplicaţiile care fac parte din Sistemul Informatic Integrat al ONRC (SII) sunt enumerate mai jos, impreuna cu infrastructura tehnologică utilizată:

* **Registratura Locatie (RG)**
* Nivelul de persistenta
* RDBMS: Oracle 11g (RAC)
* Nivelul aplicatie
* Hibernate 3
* Hibernate annotations
* Spring 3.0.5
* JBPM 4.4
* Jasper Reports
* Nivelul de prezentare
* Wicket 1.4.6
* WEBDAV
* HTML/CSS
* Weblogic Portal 11g
* Nivelul de integrare date si procese
* Oracle Streams
* Apache CXF WS
* Oracle ESB
* Middle Tier
* Weblogic Server 11g
* **Registrul Litigiilor (RL)**
* Nivelul de persistenta
* RDBMS: Oracle 11g (RAC)
* Nivelul aplicatie
* Hibernate 3
* Hibernate annotations
* Spring 3.0.5
* JBPM 4.4
* Jasper Reports 4.0.1
* Nivelul de prezentare
* Oracle ADF
* HTML/CSS
* Weblogic Portal 11g
* Nivelul de integrare date si procese
* Oracle Streams
* Apache CXF WS
* Oracle ESB
* Middle Tier
* Weblogic Server 11g
* **Registrul Comertului (RC)**
  + Nivelul de persistenta
  + RDBMS: Oracle 11g (RAC)
  + Nivelul aplicatie
  + IBATIS
  + Spring 3.0.5
  + BIRT Reports
  + Nivelul de prezentare
  + HTML/CSS
  + Oracle ADF
  + Weblogic Portal 11g
  + Nivelul de integrare date si procese
  + Oracle Streams
  + JAX -WS
  + Oracle ESB
  + Middle Tier
  + Weblogic Server 11g
* **Buletinul Procedurilor de Insolventa (BPI)**
  + Nivelul de persistenta
  + RDBMS: Oracle 11g (RAC)
  + Nivelul aplicatie
  + Hibernate 3
  + Hibernate annotations
  + Spring 3.0.5
  + JBPM 4.4
  + Jasper Reports
  + Nivelul de prezentare
  + Wicket 1.4.6
  + WEBDAV
  + HTML/CSS
  + Weblogic Portal 11g
  + Nivelul de integrare date si procese
  + Oracle Streams
  + Apache CXF WS
  + Oracle ESB
  + Middle Tier
  + Weblogic Server 11g
* **Portalul Serviciilor Online al institutiei ONRC**
  + Nivelul de persistenta
  + RDBMS: Oracle 11g (RAC)
  + Nivelul aplicatie
  + Hibernate 3
  + Hibernate annotations
  + Spring 3.0.5
  + JBPM 4.4
  + Jasper Reports
  + Nivelul de prezentare
  + Specificatia Portlet 286 (implementarea Weblogic)
  + Wicket 1.4.6
  + WEBDAV
  + HTML/CSS
  + Nivelul de integrare ata si procese
  + Oracle Streams
  + Apache CXF WS
  + Oracle ESB
  + Middle Tier
  + Weblogic Portal 11g
* **Antecalcul**
  + Nivelul de persistenta
  + RDBMS: Oracle 11g (RAC)
  + Nivelul aplicatie
  + Hibernate 3
  + Hibernate annotations
  + Spring 3.0.5
  + JBPM 4.4
  + Jasper Reports
  + Nivelul de prezentare
  + Wicket 1.4.6
  + WEBDAV
  + HTML/CSS
  + Weblogic Portal 11g
  + Nivelul de integrare date si procese
  + Oracle Streams
  + Apache CXF WS
  + Oracle ESB
  + Middle Tier
  + Weblogic Server 11g
* **Publicare date catre alte institutii**
  + Oracle ESB
  + Oracle 11g Database
* **Sistem de securitate interna (central si local) si externa (Aplicatia Centralizata de Management Utilizatori - ACMU)**
  + Oracle Identity Manager 11g
  + Oracle Access Manager 11g
  + Oracle Web Gate
* **Raportare Analitica**
  + Oracle Business Intelligence Suite Enterprise Edition 11g
* **Aplicatia de acces utilizatori**
  + Oracle ADF
  + Oracle Weblogic 11g
  + Oracle Database 11g
* **Replicare masiva de date** 
  + SharePlex for Oracle

Infrastructura tehnologică utilizată de catre SAE (Sistemul de Arhivare Electronica)

* + WebSphere AS
  + DB2 Content Manager
  + Java
  + UDB DB2

În **ONRC** sunt implementate politici IT referitor la următoarele domenii:

* + Securitatea informatiei si controlul accesului;
  + Disponibilitatea sistemelor ;
  + Proceduri de backup / restore;
  + Plan de continuitate;
  + Arhivarea datelor.

**Securitatea informatiei si controlul accesului**

Având în vedere faptul ca informaţiile registrului comerţului sunt informaţii publice, măsurile de asigurare a securităţii s-au concentrat, până în prezent, în special pe asigurarea funcţionării continue a sistemului informatic, de care depinde buna desfăşurare a activităţii instituţiei.

Securitatea sistemelor informatice la nivelul ONRC este asigurată astfel:

* la nivel fizic – prin reguli de acces fizic la resursele IT (staţii de lucru, imprimante, echipamente active de reţea, echipamente de comunicaţie, firewall);
* prin implementarea unei arhitecturi a sistemului informatic care să asigure protecţie maximă la accesele din afara reţelei.
* la nivelul ONRC, prin intermediul unui firewall central, care împarte reţeaua ONRC în zone demilitarizate (DMZ – DeMilitarized Zone), reţea internă, respectiv zona reţelelor virtuale private (VPN și Extranet VPN);
* la nivelul fiecărui ORCT, prin intermediul unui firewall, care împarte reţeaua ORCT în zonă demilitarizată (DMZ – DeMilitarized Zone), reţea internă, respectiv zona reţelei virtuale private (VPN);
* prin controlul accesului utilizatorilor la resursele IT:
* controlul accesului utilizatorilor la nivelul staţiilor de lucru
* controlul accesului la serverul DNS (în DMZ);
* controlul accesului la serverul Internet de mail;
* controlul accesului la serverele web – care găzduiesc site-ul web oficial al instituţiei – [www.onrc.ro](http://www.onrc.ro), intranet.onrc.ro, portal.onrc.ro, etc (în DMZ-uri);
* controlul accesului la serverele de baze de date interne;
* controlul accesului la imprimante;
* controlul accesului la echipamentele active de reţea (switch-uri) şi routere;
* controlul accesului la firewall-uri ;
* prin implementarea de reguli de acces la aplicaţii şi informaţii: regulile de acces la aplicaţii şi informaţii sunt stabilite pe baza atribuţiilor angajaţilor din fişele de post;
* prin programe specifice instalate pe echipamente (staţii de lucru, servere) ce asigură protecţia antivirus, antispyware;
* prin reguli de acces implementate la nivelul firewall-urilor şi router-elor, reguli ce asigură protecţia resurselor IT şi informaţii atât în faţa acceselor din afara reţelei cât şi din interior:
* reguli de acces implementate la nivelul router-ului ce asigură conexiunea Internet
* reguli de acces implementate la nivelul firewall-urilor instalate pe staţiile de lucru.
* prin monitorizarea permanentă a echipamentelor şi pachetelor software ce asigură securitatea sistemelor informatice:
* monitorizarea funcţionării firewall-urilor;
* monitorizarea funcţionării router-elor;
* monitorizarea funcţionării pachetului antivirus pe serverul de mail (mail.onrc.ro)
* monitorizarea serverului pentru update-uri la produsele antivirus de pe staţii de lucru.

**Disponibilitatea Sistemelor / High Availability**

Avind in vedere ca asigurarea funcţionarii continue a sistemului informatic este un obiectiv prioritar in strategia IT a ONRC, au fost implementate solutii pentru asigurarea funcţionării continue a echipamentelor critice dupa cum urmeaza:

* soluţii de tip cluster pentru servere
* echipamente de rezervă, configurate identic cu cele în funcţiune (exemplu : firewall central) ;
* echipamente de rezervă (în special switch-uri) ;

**Proceduri de Backup / Restore**

La nivelul bazelor de date politica de backup se realizeaza dupa cum urmeaza:

* Baze de date Oracle (utilizate de catre SII): salvarea bazelor de date Oracle se realizeaza periodic pe banda prin intermediul Tivoli Storage Manager şi pe dispozitive de tip SmartBackup cu acces rapid; procedura de backup / restore prevede atat full online si offline backup cat si salvari incrementale;
* Baze de date DB2 (utilizate de catre sistemul de arhivare electronica): salvarea bazelor de date DB2 se realizeaza periodic pe banda prin intermediul Tivoli Storage Manager; procedura de backup / restore prevede atat full offline backup cat si salvari incrementale.

La nivelul sistemului de operare politica de backup se realizeaza dupa cum urmeaza:

* Pentru serverele Intel exista platforme de rezerva care pot fi utilizate pentru a inlocui o eventuala masina defecta;
* Pentru platformele AIX se utilizeaza configuratii de inalta disponibilitate care permit comutarea rapida a incarcarii de pe un nod defect pe un nod functional.

# Descrierea noului sistem informatic

## Rezultate așteptate

Oficiul National al Registrului Comertului, aflat in subordinea Ministerului Justitiei, are in vedere derularea de proiecte care sa vizeze atingerea obiectivelor sale strategice, prevazute in legislatia aplicabila si in strategiile sectoriale. In ultimii ani, ONRC a urmarit in mod constant cresterea eficientei si transparentei serviciilor furnizate catre terti, in concordanta cu strategia de informatizare a sistemului judiciar si cu strategiile din domeniul e-guvernării.

**Buletinul Electronic al Registrului Comerţului**

Prin implementarea şi dezvoltarea subsistemului informatic Buletinul Electronic al Registrului Comerţului, sub forma unei platforme electronice se urmăreşte derularea cu celeritate şi producerea efectelor scontate a serviciului organizat de Oficiul Naţional al Registrului Comerţului în îndeplinirea obligaţiei de publicare pe pagina de Internet a instituţiei a actelor şi informaţiilor prevăzute în mod expres de lege în sarcina sa, precum şi a informaţilor privind menţiunile efectuate din oficiu în registrul comerţului, în baza hotărârilor judecătoreşti comunicate de instanţele judecătoreşti sau a altor înscrisuri emise de autorităţi şi instituţii publice.

Acest instrument electronic, Buletinul Electronic al Registrului Comerţului, va asigura şi baza materială necesară punerii în aplicare a viitoarelor prevederi normative privind simplificarea formalităţilor de asigurare a publicităţii actelor profesioniștilor.

Astfel, proiectul de lege privind registratorii comerciali şi activitatea de înregistrare în registrul comerţului, reglementează, pe lângă înfiinţarea profesiei de registrator comercial şi instituirea procedurii de soluţionare a cererilor de înregistrare în registrul comerţului şi extinderea categoriilor de acte, fapte şi menţiuni ale profesioniștilor şi ale celorlalte persoane juridice supuse obligaţiei de înregistrare în registrul comerţului, pentru care asigurarea publicităţii se va realiza de către Oficiul Naţional al Registrului Comerţului prin intermediul unei platforme electronice centrale, Buletinul Electronic al Registrului Comerţului.

La data de 14 ianuarie 2010 a intrat în vigoare O.U.G. nr.116/2009 pentru instituirea unor măsuri privind activitatea de înregistrare în registrul comerţului, astfel încât *(...)* ***competenţa de soluţionare a cererilor de înregistrare în registrul comerţului*** *şi, după caz, a altor cereri aflate în competenţa de soluţionare a judecătorului delegat* ***aparţine****, până la reglementarea activităţii de înregistrare în registrul comerţului efectuată de registratori comerciali* ***directorului oficiului registrului comerţului de pe lângă tribunal şi/sau persoanei sau persoanelor desemnate de către directorul general al Oficiului Naţional al Registrului Comerţului.***

Aşadar, având în vedere contextul social economic care impunea, pe de o parte, o decongestionare a activităţii judiciare prin luarea unor măsuri energice de remediere a supraîncărcării instanţelor şi, pe de altă parte, o fluidizare a procedurilor aferente activităţii comerciale, competenţa de soluţionare a cererilor de înregistrare în registrul comerţului şi, după caz, a altor cereri aflate în competenţa de soluţionare a judecătorului delegat a fost preluată, până la reglementarea activităţii de înregistrare în registrul comerţului, de registratori comerciali, directorul oficiului registrului comerţului de pe lângă tribunal şi/sau persoanei ori persoana desemnata de către directorul general al Oficiului Naţional al Registrului Comerţului.

O.U.G. nr.116/2009 a fost aprobată cu modificări şi completări prin Legea nr.84/2010, ulterior fiind modificată de O.U.G. 85/2010.

**Ministerul Justiţiei a elaborat un proiect de lege privind registratorii comerciali şi activitatea de înregistrare în registrul comerţului, prin care se propune ca activitatea de registru să se desfăşoare sub control administrativ.**

Pornind de la aceste legiferări, prin proiectul de lege mai sus amintit se reglementează:

* Procedura de înregistrare în registrul comeţului în baza controlului registratorului comercial sau, după caz, în baza hotărârii instanţei judecătoreşti;
* Profesia de registrator comercial;
* Extinderea categoriilor de acte ale persoanelor supuse obligaţiei de înregistrare înregistrul comerţului, pentru care Oficiul Naţional al Registrului Comerţului asigură efectuarea publicităţii prin Buletinul Electonic al Registrului Comerţului, organizat ca un instrument electronic;
* Modul de organizare și funcţionare a Oficiului Naţional al Registrului Comerţului şi a oficiilor registrului comerţului.

Extinderea categoriilor de acte şi informaţii supuse publicităţii prin Buletinul Electronic al Registrului Comerţului este în acord şi cu prevederile Directivei 2009/101 a Parlamentului European şi a Consiliului din 16 septembrie 2009, de coordonare, în vederea echivalării, a garanţiilor impuse societăţilor în statele membre, în înţelesul articolului 48 al doilea paragraf din tratat, pentru protejarea intereselor asociaţilor sau terţilor, care, la art. 3 alin. (5)–(6), conferă statelor membre dreptul de a asigura publicitatea actelor şi faptelor profesioniștilor şi prin intermediul portalului ONRC.

Subsistemul informatic “Buletinul Electronic al Registrului Comerţului” va asigura pe de-o parte colectarea online sau la ghiseu, procesarea si publicarea datelor si documentelor supuse publicitatii si pe de alta parte va asigura consultarea online prin intermediul portalului ONRC si a unei aplicatii mobile de catre publicul larg, mediul de afaceri si autoritatile publice a buletinelor electronice publicate.

**Subsistemul Informatic Colaborativ**

Un factor determinant in imbunatatirea proceselor interne si a capacitatii de furnizare a serviciilor publice il constituie crearea unui cadru colaborativ (cu precadere pe orizontala intre angajatii distribuiti teriorial care impartasesc aceeasi specialitate / pregatire / responsabilitati) care sa sustina si sa incurajeze partajarea de idei, opinii, abordari, solutii referitoare la problemele profesionale curente. Obiectivul principal al cadrului colaborativ va fi acela de sustinere a fluxurilor informationale si procedurilor formale existente in cadrul organizatiei si de facilitare a comunicarii in cadrul comunitatilor interne de specialisti in domeniile de interes ale ONRC (juridic, IT, etc).

Totodata, cadrul colaborativ va avea in vedere si sustinerea proceselor integratoare la nivelul institutiei cum ar fi: gestiunea proiectelor, gestiunea incidentelor software, gestiunea ciclului de viata al aplicatiilor software, etc.

In vederea stabilirii proceselor interne asupra carora cadrul colaborativ poate avea un impact semnificativ, se va derula o etapa de analiza a sistemului informational-decizional existent. Pe baza acestei analize vor fi identificate:

1. Comunitatile interne de specialisti (juridic, IT, etc) – a caror colaborare pe orizontala contribuie atat la perfectionarea lor cat si imbunatatirea calitatii serviciilor prestate
2. Departamentele care sunt implicate in activitati specifice derulate de regula prin intermediul proiectelor interne
3. Organizarea actuala a echipelor de IT pentru dezvoltarea, administrarea si intretinerea sistemelor informatice ale ONRC
4. Propuneri privind crearea cadrului colaborativ la nivelul institutiei avand in vedere elementele identificate la punctele 1-3

Rezultatele analizei sistemului informational-decizional existent vor fi utilizate in cadrul etapei de analiza pentru elaborarea specificatiilor tehnice ale subsistemului informatic de tip “Colaborativ” (SSICO).

Grupul tinta pentru implementarea SSICO il reprezinta angajatii ONRC ce participa in procesele identificate in etapa de analiza a sistemului informational-decizional existent. Activitatile/procesele avute cu prioritate in vedere de ONRC sunt cele in care pot fi implicati un numar cat mai mare de angajati, distribuiti la nivel teritorial, printre care enumeram urmatoarele – fara a ne limita doar la acestea:

* Elaborarea raspunsurilor la solicitari atipice ale operatorilor economici privind inregistrari in registrul comertului
* Elaborarea raspunsurilor la solicitari atipice ale persoanelor fizice/juridice privind inregistrari in BPI
* Managementul proiectelor interne ONRC (de ex. cu finantare externa)
* Dezvoltarea / Testarea / Imbunatatirea aplicatiilor software
* Elaborarea de cerinte functionale / documentatii in vederea achizitionarii de servicii / produse

**Subsisteme informatice de monitorizare a performanțelor si asigurarea securitatii SII al ONRC**

Din punctul de vedere al tehnologiilor de asigurare a securitatii si a disponibilitatii, Sistemul Informatic Integrat al ONRC nu a mai fost actualizat de ceva timp dupa lansarea acestuia in productie.

In contextul unei evolutii continue a amenintarilor cibernetice, a nevoii de diversificare a serviciilor oferite prin intermediul internetului si de asigurare a unei disponibilitati de nivel inalt pentru aceste servicii, ONRC isi propune ca prin implementarea acestui proiect sa intareasca Sistemul Informatic Integrat prin actualizarea/inlocuirea tehnologiilor folosite in prezent si prin instruirea corespunzatoare a personalului de specialitate penttru a face fata noilor provocari.

Tendinta actuala in crearea sistemelor informatice integrate incuba elementele de securitate – in special, si cele de monitorizare – in secundar, la toate nivelurile si inca din faza de conceptie a sistemului. Astfel, primele elemente le vom avea la nivelul preponderent hardware, care, conform nevoilor specifice generate de subsistemele de business, poate fi impartit la randul lui in trei zone relevante, respectiv procesarea datelor, stocarea datelor si interconectarea la nivelul retelei beneficiarului; propunerea de fata adreseaza aceste zone cu cate un subsistem dedicat.

In continuare, nevoile de securitate si monitorizare se concentreaza pe nivelul preponderent software, iar definirea zonelor adresate incearca nu doar sa raspunda cerintelor beneficiarului ci sa si maximizeze oportunitatile de dezvoltare ale acestuia in viitorul apropiat – atat din perspectiva sistemelor in sine si tendintelor tehnologice cat si la nivel organizational – preponderant dpdv impartire zonala.

Revenind la nivelul hardware, nevoilor de procesare li se raspunde cu o solutie moderna cu trei atribute de baza: putere, densitate si scalabilitate. Puterea este reprezentata de procesoare de ultima generatie, iar densitatea si scalabilitatea rezida din arhitectura modulara (sasiu + servere); ultimul reper fiind partea de interconectare privata – intre subsistemul de procesare si cel de stocare. De mentionat ca, la nivel de set – sasiu + servere blade, solutia trebuie sa prevada astfel de seturi pentru fiecare site.

In continuare, nevoilor de stocare li se raspunde cu o solutie completa de stocare ale carei atribute de baza trebuie sa fie disponibilitatea, flexibilitatea si scalabilitatea. Daca disponibilitatea e asigurata de arhitectura dual-controller in special, si flexibilitatea rezida din capabilitatile de multi-protocol si multiple tipuri de matrici RAID suportate, scalabilitatea rezulta din capabilitatile majore de extindere facila a spatiului de stocare.

Comunicarea intre cele doua subsisteme de mai sus este reprezentata distinct de subsistemul de interconectare privata, care asigura un acces uniform al nodurilor de procesare atat la zone de stocare cat si catre zona de retea; nivelul de performante al acestui subsistem nu va trebui sa ingradeasca sub nicio forma nivelurile de performanta in procesarea si respectiv stocarea datelor.

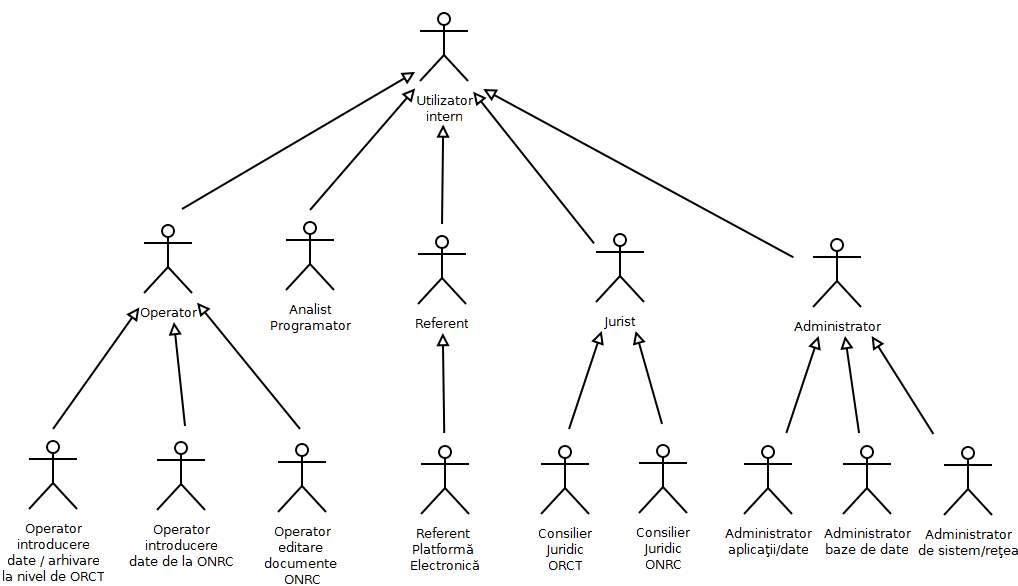
Din punctul de vedere al monitorizarii performantelor, relevant pentru proiect sunt trei zone distincte, respectiv dezvoltarea si exploatarea aplicatiilor, accesul la date si serviciile. Acoperirea primelor doua zone va aduce beneficiarului vizibilitatea si controlul necesar din punct de vedere al accesului la date si performentelor pe toata durata de viata al aplicatiilor dezvoltate, ultima zona contureaza o imagine de ansamblu la nivel general de retea si organizational, ingloband capabilitati de monitorizare a traficului si a experientei utilizatorului – sub-zona din ce in ce mai sensibila in contextual actual de orientare spre consumatorul de drept (cetateanul) al serviciilor publice.

Pentru zona de Securitate si audit, stringentele implica o complexitate sporita, iar aceasta complexitate nu e generata doar de dezvoltarea tehnologica in ansamblu, ci si de multitudinea aplicatiilor si tehnologiilor folosite intern de catre beneficiar. Astfel, zonele de adresat in cadrul proiectului sunt: testarea si remedierea securitatii aplicatiilor, distributia accesului si protectia serviciilor de aplicatie, protectia antimalware si a resurselor la nivel client, analiza reurselor utilizate si managementul datelor de audit.

## Utilizatorii noului sistem informatic

### Utilizatori interni (personal ONRC)

| **Nume User** |
| --- |
| Operator introducere date/arhivare la nivel de ORCT |
| Consilier Juridic ORCT |
| Operator introducere date de la ONRC, dupa caz |
| Consilier Juridic ONRC |
| Operator verificare/validare documente ONRC |
| Referent subsistem BERC |
| Administrator aplicaţii/date |
| Administrator baze de date |
| Administrator de sistem/reţea/comunicaţii/securitate |
| Specialist IT |
| Director Platformă electronică/Şef Serviciu Platformă electronică |

****

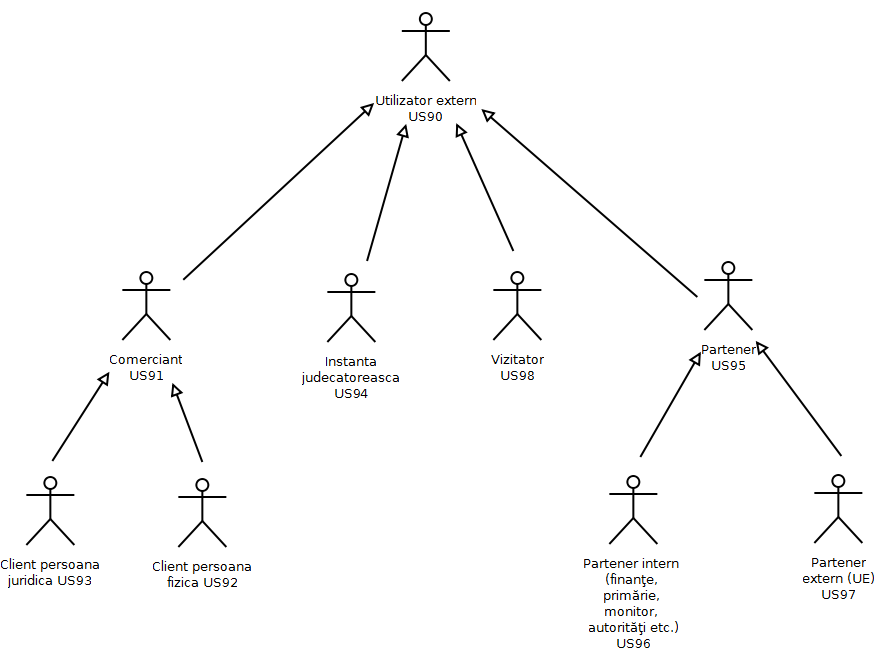
Figură 5 Utilizatorii interni ai sistemului

| **Nr. crt.** | **Cod utilizatori** | **Denumire** | **Descriere utilizatori** |
| --- | --- | --- | --- |
| 1 | US1 | Operator introducere date/arhivare la nivel de ORCT | * Preluare/prelucrare acte primite de la profesioniști; * generare si incarcare acte pentru a fi publicate; * trimitere acte la ONRC pentru a fi publicate în BERC; * arhivare acte în Sistemul de Arhivare Electronic. |
| 2 | US2 | Consiler Juridic ORCT | * verifică actele primite de la profesioniști; * verifică datele de identificare ale profesionistului. |
| 3 | US3 | Consilier Juridic ONRC | * verifică actele primite de la ORCT, dupa caz; * verifică datele de identificare ale profesionistului, dupa caz; * verifică corectitudinea numerelor de BERC înainte de publicarea lor în BERC. |
| 4 | US4 | Operator verificare date la ONRC | * verificarea datelor în aplicaţia BERC al registrului comerţului aferente actelor primite spre publicare. |
| 5 | US5 | Operator validare documente ONRC | * selectarea/validarea actelor în vederea realizării unui BERC; * redactarea actelor care necesită acest lucru, dupa caz; * rularea macro-urilor pentru realizarea buletinului; * redactarea BERC, dupa caz. |
| 6 | US6 | Referent BERC | * gestionarea corespondenţei cu clienţii; * gestionarea contractelor şi a cererilor de furnizare primite de la persoanele interesate; * întocmirea documentelor solicitate ca urmare a încheierii unui contract/protocol de furnizare; * livrarea informaţiilor şi documentelor pentru care există contract/protocol, clienţilor. |
| 7 | US7 | Administrator aplicaţii / date | Administratorul aplicaţii/date va avea următoarele atribuţiuni:   * instalare aplicaţii; * configurare aplicaţii; * administrare roluri/grupuri de utilizatori aplicaţii; * administrare securitate aplicaţii; * utilizare/configurare module de administrare a aplicaţiilor; * gestiunea datelor aplicaţiilor; * monitorizarea evenimentelor apărute în exploatarea aplicaţiilor; * analiza logurilor/jurnalelor de aplicaţii. |
| 8 | US8 | Administrator baze de date | * coordonează actualizarea şi asigura protecţia bazei de date utilizând mijloace puse la dispoziţie de software-ul existent; * administrează şi exploatează baza de date; * administrează transmiterea şi recepţia datelor către diverse baze de date, în temeiul legii sau a acordurilor de cooperare, la termenele şi în modalităţile convenite cu instituţiile care ţin şi gestionează bazele de date respective. |
| 9 | US9 | Administrator de sistem/reţea/ comunicaţii/ securitate | Administrator IT având următoarele atribuţii:   * instalarea sistemelor de calcul si/sau a reţelelor; * configurarea sistemelor de calcul si/sau a reţelelor; * gestiunea utilizatorilor sistemelor de calcul; * monitorizarea evenimentelor apărute în exploatarea sistemelor de calcul/reţelelor; * optimizarea sistemelor de calcul/reţelelor; * instalarea aplicaţiilor şi a sistemelor software de sistem. |
| 10 | US10 | Specialist IT | * elaborează şi participa la elaborarea de noi aplicaţii şi programe informatice, în scopul informatizării şi optimizării tuturor activităţilor desfăşurate; * instruieşte utilizatorii produselor informatice elaborate de Oficiul Naţional al Registrului Comerţului şi răspunde de utilizarea bazelor de date în condiţii corecte şi strict în limitele autorizate de acces. |
| 11 | US11 | Director BERC/Şef Serviciu BERC | Coordonează, avizează şi controlează activităţile specifice transmiterii şi publicării actelor în Buletinul Electronic al Registrului Comerţului;  Repartizează cererile de furnizare, comenzile şi contractele/protocoale de furnizare informaţii, precum şi orice adresa referitoare la furnizarea informaţiilor din BERC după înregistrarea acestora la registratura generala;  Coordonează, avizează şi controlează activităţile de elaborare instrucţiuni de lucru/norme metodologice, puncte de vedere si/ sau proiecte de acte normative, alte documente, specifice Platformei electronice, efectuare control asupra activităţii Platformei electronice, alte activităţi incidente. |

### Utilizatori externi (grupurile ţintă)

| **Cod User** | **Nume User** |
| --- | --- |
| US91 | Client persoană fizică |
| US92 | Client persoană juridică |
| US93 | Instanţa judecătorească sau asimilat |
| US94 | Partener intern (administraţie financiară, primărie, monitor, autorităţi etc.) |
| US95 | Partener extern (UE) |
| US96 | Vizitator |

| **Nr. crt** | **Cod utilizator** | | **Denumire** | **Descriere utilizatori** |
| --- | --- | --- | --- | --- |
|  | US91 | Profesionist | | Persoană înregistrată în Registrul Comerţului |
|  | US92 | Client persoana fizica | | Persoana fizică care intră în relaţie cu BERC a ONRC |
|  | US93 | Client persoana juridica | | Persoana juridică care intră în relaţie cu BERC a ONRC |
|  | US94 | Instanţa judecătorească saua similat | | Instanţa judecătorească sau asimilat care emite hotărâri/documente cu impact semnificativ în procesele operaţionale ONRC |
|  | US95 | Partener | | O entitate care schimbă informaţii cu BERC bazat pe o convenţie sau o înţelegere |
|  | US96 | Partener intern (administraţie financiară, primărie, monitor, autorităţi etc.) | | Autorităţi cu care ONRC are protocoale de colaborare |
|  | US97 | Partener extern (UE) | | Autorităţi externe cu care ONRC are protocoale de parteneriat în cadrul şi în afara UE |
|  | US98 | Vizitator | | Un utilizator cu drepturi limitate care accesează online sistemele ONRC |



Figură 6 Utilizatori externi ai sistemului

### Managementul utilizatorilor si accesul la sistem

Utilizatorii noului sistem si accesul la aplicațiile acestuia vor fi gestionați folosind solutia existenta pentru managementul accesului, implementata pe baza următoarelor produse: Oracle Internet Directory (server director cu rol de depozit de profiluri de utilizator) si Oracle Access Manager (server management acces).

Aplicațiile noului sistem se vor integra cu soluția de managementul accesului si utilizatorilor, in sensul ca vor utiliza profilurile de utilizatori deja existente in cadrul serverului director. Utilizatorii care au acces in noul sistem vor fi diferentiati prin adaugarea unui nou atribut in profilurile stocare in serverul director.

Mecanismele de acces implementate in prezent vor fi reutilizate pentru a securiza si aplicațiile noului sistem. In acest scop, aplicațiile noului sistem vor avea capacitatea de a se integra cu platforma de control acces, permitand autentificarea utilizatorilor de catre serverul de control acces. Autentificarea se va realiza pe baza de utilizator si parola sau pe baza de certificat digital.

Autorizarea utilizatorilor va fi realizata prin mecanismele puse la dispoziție de fiecare aplicație a noului sistem sau prin utilizarea facilitaților de autorizare ale serverului de management acces. Accesul la aplicatii va fi permis numai utilizatorilor autorizati in acest sens.

# Cerințe privind soluția tehnică

## Cerințe generale

Soluţiile ce vor fi implementate trebuie să ţină cont de următoarele recomandări de abordare a unui sistem informatic modern şi deschis:

* abordare unitară, etapizată, folosind metodologii şi tehnologii adecvate;
* sisteme pre-integrate - pe cât posibil de la acelaşi producător;
* arhitectura modulara şi deschisă, bazată pe standarde;
* sistem centralizat cu punct de administrare unic;
* arhitectura tip 'Internet'/'Intranet';

Toate informaţiile, cerinţele, funcţionalităţile prezentate în acest document nu sunt exhaustive. Intenţia acestui document este de a furniza o privire de ansamblu asupra proiectului şi nu poate fi înţeles ca fiind o descriere detaliată a cerinţelor proiectului. Cerinţele detaliate ale proiectului vor fi definite în fazele iniţiale de implementare a acestui proiect.

### Subsistemul Buletinul Electronic al Registrului Comerţului

Subsistemul informatic propus trebuie să fie modular, uşor extensibil şi să fie bazat pe următoarele module de soluţie:

* componenta portal care să permită definirea şi găzduirea tuturor interfeţelor cu utilizatorii externi;
* componenta de gestiune conţinut şi documente care să permită stocarea documentelor in format electronic, regăsirea acestora folosind criterii de selecţie bazate pe atribute si arhivarea documentelor electronice conform unor politici de retenţie personalizabile;
* componenta de gestiune a bazelor de date pentru stocarea sigură a datelor sub forma unei baze de date relaţionale (SGBDR) cu capabilităţi extinse de replicare şi backup;
* componenta server de aplicaţii care să ofere suport sigur şi scalabil de rulare pentru toate modulele proiectului (integrare, gestiune conţinut, portal, etc.);
* componenta de integrare aplicaţii bazată pe standarde deschise care să permită coexistenţa noului proiect cu aplicaţiile deja existente la ONRC;
* componenta de integrare a datelor care să asigure popularea / migrarea datelor utilizând sursele de date existente în ONRC şi să permită sincronizarea şi consolidarea datelor;

### Subsistemul Colaborativ

Subsistemul propus trebuie să fie modular, uşor extensibil şi să fie bazat pe următoarele componente functionale:

* + - O componenta de colaborare menita sa ajute echipele implicate in proiecte sa urmareasca toate activitațile necesare efectuarii de sarcini zilnice si periodice, incluzând dar nu limitat derularea proiectelor, gestionarea proceselor interne de aprobare, crearea documentelor si a fluxurilor de lucru modelate pe procesele de business
    - O componenta pentru managementul integrat al cerințelor de business, managementul cazurilor si scenariilor de test, managementul librariilor de teste manuale, automate, de funcționalitate, performanța, si securitate/integritate a aplicațiilor. Managementul defectelor identificate si menținerea transabilitații intre defecte, cazuri de testare si cerințe.
    - O componenta pentru creare si management al testarii automate software, care are la baza limbaje de scripting de ultima generatie (Javascript, C sharp, jscript/python, etc) cu support pentru Continuous integration/continuous delivery si cu posibilitatea de includere de librarii externe opensource in crearea testelor automate;
    - O componenta de testare a aplicațiilor, pentru masurarea comportamentului sistemului si a performanței componentelor aplicației sub sarcina cu suport pentru Continuous integration/continous delivery. Acesta ar permite simularea activitații utilizatorilor prin generarea de mesaje între componentele aplicației sau prin simularea interacțiunilor utillizatorului cu interfața de lucru in aplicație, prin intermediul scripturilor create manual sau în mod automat.

### Subsisteme de monitorizare a performanțelor si asigurarea securitatii SII al ONRC

Modulele avute in vedere pentru construirea subsistemului de monitorizare sunt:

* + - Soluții de monitorizare si diagnosticare end to end, incluzând monitorizarea instrumentelor hardware si software, a serviciilor informatice pentru identificare proactiva si reactiva a potențialelor probleme care pot duce la degradarea serviciilor oferite de catre ONRC catre beneficiari, fie ei direcți sau indirecți, precum si performanța, continuitatea si disponibilitatea fluxului de informații în relațiile cu instituțiile avizatoare si cele guvernamentale
    - Modul software pentru monitorizarea performanței tranzacțiilor serviciilor informatice în medii tradiționale, virtualizate sau în cloud, pentru izolarea rapida a problemelor de performanța prin diagnoza de tip „deep dive” care identifica unitațile de cod cu probleme de performanța cum ar fi metode ale obiectelor din cod sau statement-uri sql. Identifica si agrega tranzacții la nivel de utilizator, server, baza de date si back end.
    - Modul software pentru masurarea în mod proactiv a experienței utilizatorilor prin executarea într-un mod controlat, repetat de tranzacții din locatii multiple înainte sau dupa sistemele de protecție de tip firewall, pentru a identifica disponibilitatea si performanța sistemelor si a aplicațiilor.
    - Modul software de diagnosticare care monitorizeaza starea aplicației în mediile tradiționale, virtualizate sau cloud, funcționând în starile de pre-producție si producție pentru o rapida diagnosticare a blocajelor în performanța aplicațiilor si aduc o înbunatațire a calitații acestora.
    - Instrumente de monitorizare activitatea bazelor de date prin captarea traficului de rețea, generând loguri de audit.

Din perspectiva securitatii, modulele avute in vedere sunt:

* + - Componente integrate si performante de asigurare a fiabilitații si funcționalitații sistemelor si soluțiilor informatice implementate, precum si a securitații, prin implementarea de soluții de testare manuala si automata a instrumentelor software dezvoltate intern si/sau extern pentru asigurarea de înalta calitate, de testare de securitate pentru înlaturarea potențialelor vulnerabilitați chiar din stadiile incipiente ale dezvoltarii instrumentelor, de testare a performanțelor instrumentelor software pentru eficientizarea fluxului de informații, a managementul procesului de testare, etc;
    - Modul software cu capabilitați de suport si creare de analiza software cu capacitate de raportare detaliata pentru metrici de software cu privire la release-uri, cod sursa, bune practici de programare, si standarde de Securitate în programare, cu capabilitați de masurare a performanței echipei de dezvoltare (având în vedere cerințele legale si instituționale cu privire la securitatea sistemelor dar si la complexitatea soluțiilor informatice necesare si cresterea complexitații atacurilor informatice asupra instituțiilor publice
    - Instrumente de analiza a accesului utilizatorilor la aplicațiile web protejând aplicațiile si datele de atacurile cibernetice, cu capabilitați de învațare în mod dinamic a comportamentul "normal" al aplicațiilor, de actualizata în timp real pentru a oferi o protecție superioara.
    - Modul software pentru scanarea dinamica sau statica a codului sursa cu acoperire în cât mai multe tehnologii posibile pentru identificarea vulnerabilitaților de securitate si verificarea acestora. Este necesar sa faca si recomandari de remediere a vulnerabilitaților identificate în urma scanarii. Trebuie sa prezinte acuratețe mare în identificarea vulnerabilitaților si realizarea de recomandari de remediere si reducerea de tip “false-positive”. Trebuie sa prezinte capabilitați de actualizare constanta a bazei de date cu noi tipuri de vulnerabilitați si sa permita identificarea vulnerabilitaților de tip ”0 day”.
    - Soluție de securitate pentru detectarea si identificarea vulnerabilitaților din cadrul rețelei, monitorizarea activa de detectare a potențialelor brese de securitate.
    - Intrumente de tip firewall la nivel de aplicație, pentru protecția aplicațiilor web, precum si analiza dinamica de malware.
    - Instrumente pentru colectarea, agregarea si colectarea de evenimente de securitate, astfel încat sa se permita detecția de incidente care afecteaza buna desfasurare a serviciilor.
    - Instrumente de punere în aplicare si asigurare a securitații datelor, prin implementarea de politici care reglementeaza si restricționeaza modul în care utilizatori interni utilizeaza si transfera date cu caracter confidențial prin instrumente comune, cum ar fi e-mail, imprimare si unitați USB si/sau CD
    - Instrumente de detectare a atacurilor avansate si cu capabilitați de transformare a informațiilor despre atacuri în acțiuni de protecție imediate, cu capacitați adiționale de inspecție ce pot duce la o larga detectare si descoperire de potențiale atacuri
    - Instrumente de captura de date privind interacțiunile interne si/sau externe ale utilizatorilor în raport cu aplicațiile utilizate, de declansarea de alerte privind evenimentele suspecte în timp real, cu capabilitați în auditare si detectarea fraudelor.
    - Instrumente de detectare si remediere automata pentru potențiale atacuri de tip troian si malware, ransomware, cu capabilitați de creare si implementare de politici proprii, de corelare a indicatorilor proveniți din diverse surse.

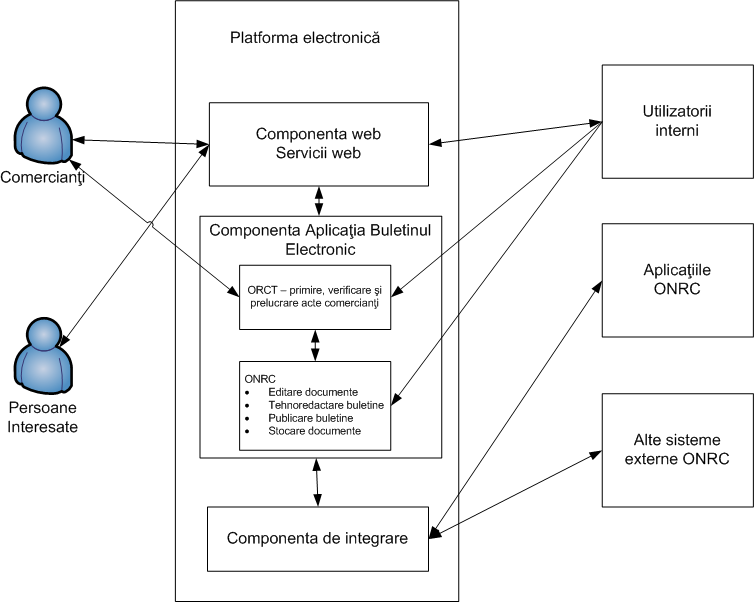
## Cerințe funcționale

### Subsistemul Buletinul Electronic al Registrului Comerţului

Din punct de vedere functional, subsistemul „Buletinul Electronic al Registrului Comertului” va contine urmatoarele module dezvoltate customizat pentru ONRC:

* + - Modul web integrat pentru Buletinul Registrului Comerțului, care se integreaza în/cu portalul existent pentru oferirea de servicii adiționale online pentru utilizatori cetațeni, mediul de afaceri si administrația publica;
    - Un modul software care sa permita cu usurința si profesional prelucrarea si publicarea de informații de interes, cu posibilitate de manipulare, editare si adaugare de conținut în timp real cu capacitate de colaborare marite cu restul funcțiunilor din cadrul organizației cu posibilitati de afisare automata a proceselor interne;
    - O aplicație inovativa pentru echipamente mobile si instrumente de dezvoltare aplicatii mobile pentru consolidarea sistemului registrului comerțului. ONRC isi propune sa furnizeze in premiera servicii de m-governance (soluții care sa permita accesul facil si sigur la informație de pe dispozitive mobile, care au o pondere din ce în ce mai importanta în modalitațile identificate de acces al portalului nostru) prin dezvoltarea si integrarea unei aplicații pentru modulul web pentru echipamente mobile pentru oferirea de servicii online, scopul fiind diversificarea si facilitarea metodelor de accesare a resurselor si serviciile ONRC, aducând beneficii pentru utilizatori cetațeni, mediul de afaceri si administrația publica

În continuare este prezentată diagramă arhitecturală de ansamblu ce descrie interacţiunea dintre entităţile implicate.



Figură 7 Descrierea generală a arhitecturii a BERC

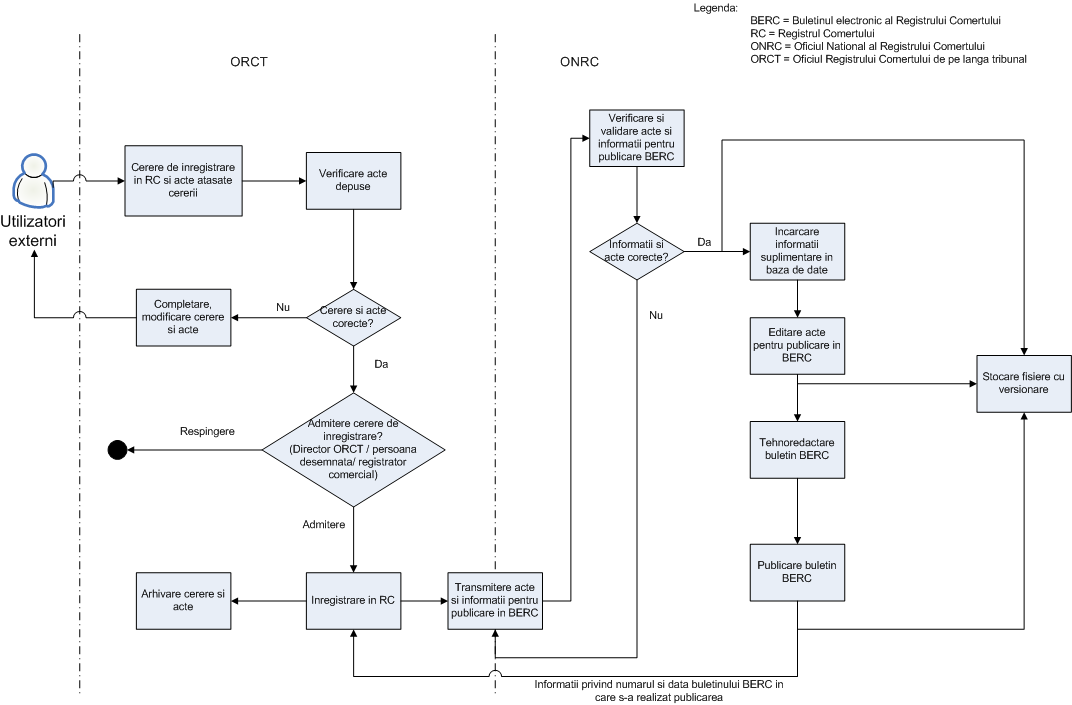
Din punct de vedere procedural, vor exista două nivele de organizare a procesarii datelor specifice BERC:

* nivelul local reprezentat de structurile teritoriale ale ONRC şi anume: ORCT (42 locaţii) şi birourile teritoriale ale ORCT; acestea vor prelua actele profesioniștilor şi vor proceda la verificarea şi pregătirea acestor acte, concomitent cu realizarea înregistrărilor şi menţiunilor în registrul comerţului;
* nivelul central reprezentat de ONRC – unde se vor centraliza toate actele profesioniștilor primite de la ORCT-uri, se vor verifica și valida pentru publicarea pe platforma centrală.

În Figură 9 este prezentată schema generală a fluxului de publicare în Buletinul Electronic al Registrului Comertului.

Pentru atingerea scopului implementarii acestui subsistem, realizarea publicităţii actelor persoanelor supuse obligaţiei de înregistrare în registrul comerţului prin publicarea electronică într-o manieră rapidă şi eficientă, este necesar să se ţină cont de următoarele aspecte:

* + Vor fi reutilizate la maximum, anumite subsisteme/aplicaţii informatice din cadrul sistemului informatic actual al ONRC prin tehnologii de tip SOA;
  + Se vor reutiliza elementele de bună practică şi experienţa acumulată în implementarea, dezvoltarea şi exploatarea Buletinului Procedurilor de Insolvenţă;
  + va permite integrarea sa în cadrul Portalului ONRC prin conceperea sa modulară şi prin folosirea serviciilor web şi de integrare;
  + Întreaga soluţie va permite susţinerea de servicii online prin furnizarea de informaţii orientate către clienţii persoane fizice sau juridice, publicului larg;
  + Componentele soluţiei, permit extinderea continuă a serviciilor online găzduite de platformă;
  + Întreaga soluţie obţinută să fie în concordanţă cu obiectivele generale şi specifice stabilite în cadrul proiectului.



Figură 8 Schema generală flux de publicare Buletinul Electronic al Registrului Comertului

Subsistemul pentru editarea şi publicarea Buletinului Electronic al Registrului Comerţului va conţine cel puţin următoarele componente funcţionale ce vor fi dezvoltate customizat in cadrul acestui proiect:

* + Consultare Online a Buletinului Electronic al Registrului Comertului (COBERC) ce contine 2 module
    - Modulul Portal – interfaţa web ce va permite accesul persoanelor interesate la Buletinul Electronic al Registrului Comerţului şi la informaţii din bazele de date aferente acestuia din cadrul portalului ONRC;
    - Modulul Mobil – aplicatie ce va permite accesul persoanelor interesate la Buletinul Electronic al Registrului Comerţului şi la informaţii din bazele de date aferente acestuia de pe dispozitive mobile;
  + Colectare si Elaborare Buletin Electronic al Registrul Comerţului (CEBERC) – interfata ce permite angajatilor ONRC sa gestioneze procesul de editare, elaborare si publicare a Buletinului Electronic al Registrului Comertului;
  + Integrare (CIBERC) cu aplicaţiile registrului comerţului în primul rând, dar şi cu alte sisteme interne şi externe ONRC;

În continuare vor fi prezentate cerinţele funcţionale ale fiecărei secţiuni a platformei electronice. De asemenea vor fi enumerate şi modul de interacţiune al platformei cu restul componentelor sistemului informatic integrat al Oficiului Naţional al Registrului Comerţului

##### Consultare Online a Buletinului Electronic al Registrului Comertului

Aceasta componenta reprezinta punctul de interacţiune central al subsistemului cu utilizatorii externi, si anume prin intermediul portalului si a aplicatiei mobile.

Componenta COBERC va fi instrumentul modern care va asigura legătura directă între instituţie şi publicul larg. Trebuie subliniat faptul că această componentă trebuie gândită şi concepută în aşa fel încât să permită integrarea facilă în cadrul portalului Oficiului Naţional al Registrului Comerţului.

De asemenea această componentă devine principalul instrument de furnizare a serviciilor on-line asociate realizării publicităţii actelor comercianţilor. Privit ca întreg, această componentă va răspunde următoarelor cerinţe funcţionale şi nefuncţionale grupate pe diverse categorii:

**Interfaţa grafică**

* interfaţa grafică va fi intuitivă, uşor de utilizat, iar navigarea, rapidă şi simplă;
* toate informaţiile vor fi prezentate implicit în limba română, însă soluţia trebuie să conţină toate elementele de internaţionalizare necesare astfel încât să permită extinderea prezentării şi la alte limbi de circulaţie internaţională;
* din punct de vedere tehnic / tehnologic această interfaţă va respecta standardele actuale în domeniu (css, xhtml etc.); respectarea acestor standarde permite extinderea/ modificarea uşoară a acestei interfeţe;
* nu va impune utilizarea unui anumit tip de browser de internet.

**Securitate**

* accesul la serviciile online va fi securizat, fără a exista posibilitatea de a fi accesate în absenţa autentificării prin metode clasice (nume utilizator, parola, certificate digitale).
* Sa implementeze mecanismele informatice pentru principiilor prevazute in cadrul GDPR
* Principiul legalitatii, corectitudinii și transparenței
* Principiul limitării scopului
* Principiul colectarii minimului de date pentru atingerea scopului pentru care s-a obtinut consimtamantul
* Principiul mentinerii datelor actualizate
* Principiul stocării datelor strict pe perioada pentru care s-a obtinut consimtamantul
* Principiu asigurarii securitatii adecvate datelor astfel incat acestea sa fie integre, confidentiale si disponibile
* Principiu responsabilitatii

**Arhitectura componentei**

* din punct de vedere arhitectural, întreaga soluţie, implicit şi componenta web, este construită pe o arhitectură deschisă; pot fi adăugate noi funcţionalităţii sau modificate funcţionalităţile existente;
* va permite accesul celorlalte componente ale soluţiei;
* informaţiile vor fi expuse către sisteme externe platformei, prin intermediul serviciilor web; accesul la aceste servicii web făcându-se controlat şi securizat.

**Administrare**

* administrarea portalului web va fi făcută de către administratorii întregului sistem;
* vor fi utilizate politici de securitate pentru administrarea: utilizatorilor, grupurilor/roluri, servicii.

**Secţiunea publică – COBERC- funcţionalităţi**

* acces la sectiunea publica a publicaţiei Buletinul Electronic al Registrului Comerţului şi informaţii din bazele de date aferente. Aceasta include sumarul buletinelor electronice publicate;
* prezentarea serviciilor platformei electronice;
* furnizarea de informaţii de interes public.

**Secţiunea privata – COBERC- funcţionalităţi**

* acces la publicaţii de tip Buletinul Electronic al Registrului Comerţului şi informaţii din bazele de date aferente;
* plata on-line pentru serviciile de furnizare a publicaţiei şi de informaţii;
* Formulare on-line (web-based) pentru transmiterea actelor persoanelor supuse obligaţiei de înregistrare în registrul comerţului spre publicare în Buletinul Electronic al Registrului Comerţului;
* Statistici şi rapoarte.

**Serviciile on-line oferite prin intermediul platformei electronice**

Prin intermediul platformei electronice vor fi oferite următoarele servicii on-line:

* Buletinul Electronic al Registrului Comerţului (în format PDF);
* Sumarul buletinelor electronice publicate;
* Actele şi documentele publicate pentru fiecare persoană supusă obligaţiei de înregistrare în registrul comerţului;
* Plata on-line pentru serviciile de furnizare a publicaţiei şi de informaţii;
* Statistici şi rapoarte.

##### Colectare si Elaborare Buletin Electronic al Registrul Comerţului (CEBERC)

Aşa cum s-a menţionat, componenta de consultare a platformei electronice va reprezenta principalul instrument de realizare a publicităţii legale pentru actele persoanelor supuse obligaţiei de înregistrare în registrul comerţului. Logica de business a platformei electronice va fi asigurată însă de componenta de CEBERC. Aceasta va fi răspunzătoare, în mod transparent pentru utilizatorii externi, de toate detaliile legate de primirea, verificarea şi gestionarea actelor persoanelor supuse obligaţiei de înregistrare în registrul comerţului, precum şi de tehnoredactarea buletinelor propriu zise.

Cerinţele la care va răspunde componenta CEBERC, sunt strâns legate de scopul platformei, de a publica actele persoanelor supuse obligaţiei de înregistrare în registrul comerţului prin intermediul componentei COBERC.

Aplicaţia va răspunde la următoarele cerinţe funcţionale:

1. trebuie să permită tehnoredactarea buletinelor electronice;
2. trebuie să permită selectarea unor documente şi a informaţiilor aferente acestora pentru a fi grupate în vederea realizării unui buletin pentru publicare;
3. trebuie să permită semnarea electonică a documentelor şi a buletinului electronic, utilizând certificate digitale calificate şi certificate digitale interne (emise prin intermediul sistemului PKI implementat la ONRC în cadrul proiectului „Servicii on-line (de e-guvernare) oferite de ONRC pentru comunitatea de afaceri prin intermediul unui portal dedicat”); aplicaţia va trebui să permită atât semnarea unui document cât şi a unui set de documente stocate în unul sau mai multe foldere;
4. trebuie să permită preluarea documentelor ce urmează a fi publicate în buletinul electronic precum şi a informaţiilor legate de un operator economic din aplicaţiile existente ale registrului comerţului;
5. trebuie să permită ataşarea documentului editabil şi a documentului scanat corespunzător actului operatorului economic care se doreşte a fi publicat;
6. trebuie să permită completarea şi înregistrarea în baza de date a informaţiilor legate de actul operatorului economic care se doreşte a fi publicat (care constituie metadescriptorii ataşaţi actelor comercianţilor);
7. trebuie să permită arhivarea electronică a buletinelor electronice şi a actelor publicate;
8. trebuie să fie capabilă să regăsească informaţiile legate de actele publicate în buletinul electronic pentru un anumit operator economic;
9. trebuie să fie capabilă să regăsească informaţiile legate de un anumit tip de act al operatorilor economici ce face obiectul publicarii in BERC;
10. trebuie să fie capabilă să regăsească informaţiile legate de un anumit buletin publicat;
11. trebuie să fie capabilă să gestioneze fluxuri de documente;
12. trebuie să fie capabilă să semnaleze anumite situaţii predefinite utilizatorilor (de stare inconsistentă, situaţii speciale, etc);
13. trebuie să permită realizarea unor căutări bazate pe atribute specifice;
14. trebuie să permită stabilirea unor nivele de auditare a operaţiunilor efectuate pentru fiecare act al profesioniștilor primit spre publicare;
15. trebuie să permită într-un mod facil şi flexibil colectarea informaţiilor în vederea furnizării de informaţii;
16. trebuie să permită realizarea unui istoric al actelor publicate în Buletinul electronic pentru un anumit profesionist;
17. trebuie să permită interconectarea cu aplicaţiile necesare din cadrul sistemului informatic integrat al ONRC în vederea atingerii scopului propus, aplicaţii care vor fi identificate în cursul fazei de analiză;
18. trebuie să permită integrarea cu Portalul ONRC implementat în cadrul proiectului „Servicii on-line (de e-guvernare) oferite de ONRC pentru comunitatea de afaceri prin intermediul unui portal dedicat”;
19. trebuie să permită interconectarea facilă cu alte sisteme informatice, prin utilizarea modularizării şi a serviciilor;
20. trebuie să permită realizarea unor rapoarte operaţionale şi analitice, pe baza informaţiilor stocate în bazele de date aferente publicării buletinului electronic.

Principalele rapoarte furnizate vor fi următoarele:

* + istoricul actelor publicate pentru un anumit profesionist;
  + istoricul acţiunilor efectuate de un utilizator;
  + sumarul actelor publicate într-un buletin;
  + lista actelor publicate într-un buletin;
  + raport statistic cu privire la volumul şi tipurile de acte publicate în buletinul electronic într-o anumită perioadă de timp;
  + rapoarte cu privire la volumul de acte procesat de utilizatorii interni şi la volumul de buletine publicate;
  + raport cu privire la volumul de informaţii furnizat în anumite perioade;
  + raport cu privire la numărul abonaţilor şi cu perioadele de abonare.

##### Integrare (CIBERC)

Componenta de integrare a Buletinului Electronic a Registrului Comerţului va răspunde următoarelor cerinţe funcţionale:

* Va permite schimbul bidirecţional între subsistemul BERC şi aplicaţiile registrului comerţului;
* Va permite schimbul bidirecţional între Sistemul de Arhivare Electronică (SAE) şi subsistemul BERC;
* Va permite interconectarea şi integrarea cu sistemul ERP al ONRC;
* Va permite integrarea cu sistemul electronic de plăţi al ONRC;
* Va permite interconectarea cu alte sisteme externe ONRC.

##### Interconectarea cu sistemele existente interne şi externe ONRC

**Sistem de arhivare electronică (SAE)**

Acest sistem existent în cadrul ONRC va prelua şi va arhiva actele primite de la profesionist spre publicare în Buletinul Electronic al Registrului Comerţului. Totodata, va arhiva buletinele electronice elaborate si publicate impreuna cu datele relevante aferente procesului de elaborare. Operaţiunea de arhivare a actelor primite pentru publicare în buletinul electronic se va efectua în etapa de procesare si verificare de la nivelul fiecărui ORCT, odată cu înmatriculările şi menţiunile efectuate în registrul comerţului.

**Integrarea cu aplicaţiile existente**

În momentul în care subsistemul BERC va fi funcţional, va trebui să se integreze cu alte module din cadrul fiecărui ORCT şi la nivel de ONRC (registrul comerţului local computerizat, registrul comerţului central computerizat, registratură, taxe etc.).

Pentru a avea acces la datele de identificare ale profesioniștilor (persoanelor supuse obligaţiei de înregistrare în registrul comerţului), integrarea cu aplicaţiile de registru devine imperioasă. De asemenea, un capitol important şi definitoriu al integrării în interiorul ONRC este integrarea cu modulele de plata electronică şi cu modulele financiar – contabile existente.

**Integrarea cu Portalul ONRC**

Subsistemul BERC trebuie să permită integrarea cu Portalul ONRC. Aceasta s-ar putea să impună unele restricţii legate de interfaţă, componenta web a platformei electronice trebuind să ţină cont de specificaţiile portalului în ceea ce priveşte interfaţa, pentru a asigura utilizatorului un aspect vizual şi funcţional, unitar şi coerent.

**Interconectarea cu alte sisteme externe ONRC**

Subsistemul BERC trebuie să permită interconectarea facilă cu alte sisteme externe ONRC prin folosirea serviciilor web. O astfel de abordare, va permite interconectarea cu alte sisteme – atât interne ONRC cât şi externe – datorită modului flexibil de utilizare a datelor şi informaţiilor din Buletinul Electronic al Registrului Comerţului. De asemenea, această abordare va permite reutilizarea serviciilor pentru cât mai mulţi utilizatori.

### Subsistemul Colaborativ

Subsistemul Colaborativ trebuie sa respecte urmatoarele cerinte functionale:

* Sa asigure gestiunea a cel putin 2 tipuri de proiecte (de ex. proiecte interne de dezvoltare software, proiecte de implementare contracte finantare) cu posibilitatea ulterioara implementarii de a gestiona si alte tipuri;
* Sa asigure implementarea a mediului colaborativ de tip Q&A pentru cel putin 3 comunitati interne de specialisti (de ex. referenti registratori, specialisti IT, specialisti arhiva) si sa permita unui administrator definirea si configurarea de alte comunitati similare. Fluxurile de procesare vor fi implementate pe baza rezultatelor etapei de analiza
* Sa asigure efectuarea deployment-urilor de release-uri ale aplicatiilor dezvoltate in proiect intr-un mod integrat cu aplicarea testelor unitare, de integrare si de performanta pe mediul de pre-productie si apoi pe mediul productiv
* Sa includa pentru aplicatiile dezvoltate in cadrul proiectului teste automate (unit tests cel putin pentru 60% din componentele principale, teste de integrare cel putin pentru 80% din integrari si teste functionale pentru cel putin 20% din scenariile de testare de acceptanta)
* Sa asigure accesul utilizatorilor prin integrarea cu sistemul de gestiunea a identitatii existent in SII al ONRC

### Subsisteme de monitorizare a performanțelor si asigurarea securitatii SII al ONRC

Din perspectiva monitorizarii Sistemului Informatic Integrat, subsistemul de monitorizare trebuie sa respecte urmatoarele cerinte functionale:

* Sa asigure monitorizarea performantei retelei interne a ONRC (la nivel central) in ansamblu, evidentiind interdependentele intre aplicatii si activele de retea (servere, instante de baze de date) si oferind suport in regim automatizat pentru diagnoza si remediere a blocajelor si/sau penalitatilor de performanta;
* Sa ofere suport pro-activ din punct de vedere a stringentelor necesare maximizarii performantei reletei pentru dezvoltarea/configurarea aplicatiilor ONRC (la nivel central) pe intregul ciclu de viata al acestora;
* Sa asigure monitorizarea experientei utilizatorilor ONRC (la nivel central) pentru zona de aplicatii web-based si/sau mobile;
* Sa asigure suportul pentru analiza aprofundata si corelata a traficului de retea pentru corelarea nivelului de performanta al aplicatiilor cu aspectele ce tin de securitate cibernetica in cadrul retelei.

Din perspectiva asigurarii securitatii Sistemului Informatic Integrat, subsistemele specializate in asigurarea securitatii trebuie sa respecte urmatoarele cerinte functionale:

* Sa asigure capabilitatile de analiza si testare de securitate a sistemului informatic (ce se va dezvolta in scopul proiectului) coroborate cu capabilitatile de mitigare/remediere a vulnerabilitatilor de securitate evidentiate;
* Sa asigure capabilitatile de protectie a aplicatiilor din cadrul sistemului informatic cat si de redistributie a accesului utilizatorilor catre acestea in scopul maximizarii performantelor serviciilor ONRC;
* Sa asigure capabilitati avansate de protectie antimalware cat si capabilitati avansate de protectie a resurselor la nivelul posturilor de lucru pentru utilizatorii sistemului informatic;
* Sa asigure capabilitati de analiza a accesarii si utilizarii resurselor penbtru prevenirea situatiilor de acces si/sau scurgere de informatii neautorizate in/din cadrul sistemului informatic;
* Sa asigure capabilitatile necesare pentru managementul datelor de audit pentru asigurarea unei vizibilitati complete la nivelul infrastructurii aferente sistemului informatic.

## Arhitectura generala a sistemului

Arhitectura aleasă de ONRC, ce trebuie respectată de ofertanți, îndeplinește principiile fundamentale ce stau la baza serviciilor publice, așa cum sunt acestea menționate în Cadrul Național de Interoperabilitate. Ofertanții trebuie să aibă în vedere aceste principii atât în oferta depusă cât și în implementarea soluției.

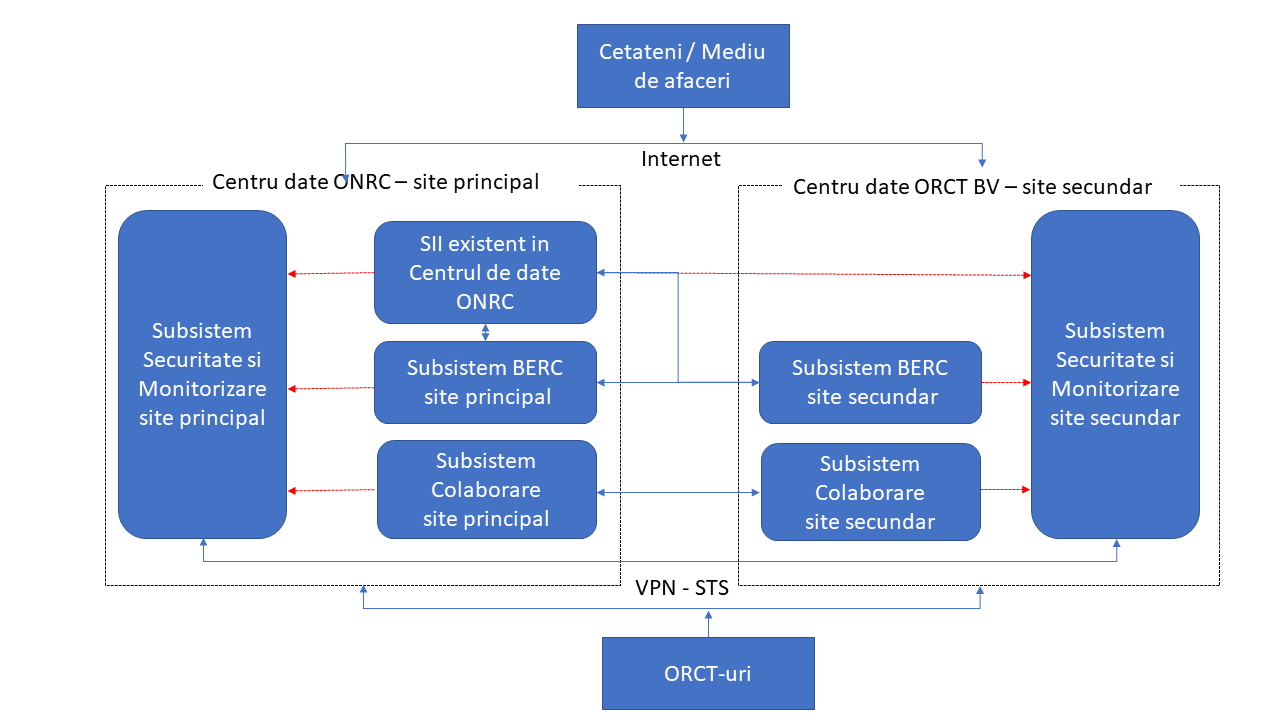
Arhitectura presupune instalarea componentelor soluţiei în doua centre de date ale ONRC.

Subsistemele BERC si colaborare din cele 2 centre de date trebuie sa fie geo-redundante asigurand astfel inalta disponibilitate nu numai la nivelul unui centru de date ci si in cazul in care centrul principal devine indisponibil.

Subsistemul de securitate si monitorizare trebuie sa acopere atat subsistemele BERC si Colaborare cat si infrastructura hardware/software a SII din centrul de date principal.

ONRC va asigura comunicatia intre cele 2 centre de date.

Cetatenii / Mediul de afaceri vor putea accesa doar componenta online a subsistemului BERC iar angajatii ONRC/ORCT vor avea acces atat la subsistemul BERC cat si la subsistemul Colaborare conform drepturilor de acces asignate.



Figură 9 Arhitectura generala a sistemului

**Scalabilitate, disponibilitate si continuitate**

Pentru a asigura o disponibilitate sporită, s-a ales soluţia tehnică centralizată şi gruparea în cluster atat a serverelor utilizate pentru publicarea web, autentificare, control acces, integrare, bază de date, aplicaţii cat si a platformelor de colaborare, securitate si monitorizare. Soluţia asigură în mod implicit şi transparent pentru utilizatorul web (web client), funcţia de distribuţie a cererilor (load-balancing), permiţând totodată o distribuţie optimă a solicitărilor către resursele disponibile (cluster activ-activ prin intermediul unui echipament hardware de load-balancing).

Totodata, pentru asigurarea continuitatii functionarii in caz de dezastru sistemul va fi distribuit in 2 centre de date (centru primar si centru secundar)

În vederea asigurării scalabilităţii şi disponibilităţii, soluţia va respectata următoarele cerinţe:

* Să suporte mecanisme de tip clustering (topologie activ-activ şi activ-pasiv) la nivelul fiecarui centru de date;
* Să implementeze mecanisme de “disponibilitate ridicata (24/7)” a platformei şi aplicaţiilor pentru execuţia continua a serviciilor instalate;
* Să implementeze mecanisme de replicare a obiectelor aplicaţiei între serverele aceluiaşi cluster si intre cele 2 centre de date (primar si secundar);
* Să permită ca, în cazul unei întreruperi a funcţionării unuia dintre noduri, cererile utilizatorilor să fie preluate automat (şi în mod transparent pentru utilizator) de către celălalt nod din cluster;
* Să permită ca, în cazul unei întreruperi a funcţionării unui centru de date (de exemplu indisponibilitate acces in internet), cererile utilizatorilor să fie preluate automat (cu impact minim pentru utilizator – la nivelul subsistemelor BERC si Colaborativ) de către centrul de date secundar;
* Să asigure utilizatorii si administratorii sistemului informatic în cazul oricarei defectiuni hardware şi/sau software, prin eliminarea totala a punctelor de „single point of failure” din arhitectura sistemului, si, implicit, implementarea mecanismelor de clusterizare/balansare la nivel hardware si software;
* Să permită stoparea temporară a unui nod pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale, prin implementarea mecanismelor de cluster;
* Să asigure securitate tranzacţională în cazul apariţiei unor erori hardware sau software în cluster;
* Să permită reconectarea automată la nodul sau nodurile rămase disponibile după apariţia unei defecţiuni;
* Să permită upgrade-ul nodurilor existente şi adăugarea de noi noduri, dependent de încărcarea sistemului, numărului de utilizatori, numărului de accesări şi de complexitatea aplicaţiilor;
* Să asigure disponibilitate permanentă 24x7, a serviciilor oferite.

Prestatorul va propune solutia tehnica avand in vedere asigurarea continuitatii si recuperarea in caz de dezastru. Procedurile operationale furnizate de Prestator vor fi incluse de Beneficiar in planul integrat al ONRC de asigurarea a continuitatii si recuperare in caz de dezastru.

**Fiabilitate şi stabilitate**

Prin utilizarea unor tehnici avansate de cluster, soluţia propusă asigură un nivel relativ ridicat de disponibilitate (availability) şi fiabilitate (reliability). Utilizarea tehnicilor avansate de cluster asigură, pe lângă un nivel crescut de scalabilitate şi o bună distribuţie a cererilor (load balancing), precum şi un nivel ridicat de fiabilitate prin creşterea nivelului de toleranţă la erori.

În vederea creşterii fiabilităţii şi stabilităţii soluţiei, trebuie utilizat un mediu de administrare şi monitorizare centrală a aplicaţiilor şi a bazelor de date. Acest mediu va trebui sa respecte următoarele cerinţe:

* Monitorizarea integrată a elementelor de infrastructură legate de reţea, sisteme, aplicaţii eterogene - Sisteme de operare şi aplicaţiile Proiectului - din punct de vedere al performanţelor, la nivel de Data Center;
* Măsurarea şi colectarea datelor de performanţă într-o bază de date pentru analiză şi raportare ulterioară;
* Diagnosticarea problemelor ce apar în cadrul soluţiei;
* Administrare web-based cu capabilităţi de monitorizare configurabile;
* Posibilitatea de a seta praguri pentru avertizări şi alerte critice;
* Alertare via e-mail la evenimente pe o ierarhie de priorităţi configurabilă;
* Posibilitatea de a oferi grafice de performanţă în timp real;
* Posibilitatea de a securiza comunicaţia între diferite componente ale soluţiei. Componentele subsistemului de monitorizare/securitate vor comunica intern doar securizat;
* Administrarea arhitecturilor de tip cluster;
* Posibilitatea de a defini mai mulţi administratori / utilizatori cu roluri diferite;
* Posibilitatea configurării sistemului de management astfel încât să execute acţiuni corective automate (fără intervenţia administratorilor) în cazul detectării de erori sau în cazul degradării performanţelor;
* Existenţa unor instrumente pentru realizarea operaţiilor de backup şi recovery pentru baza de date, pentru aplicaţii, cât şi pentru adăugarea de noi noduri în arhitectura de cluster;
* Includerea mecanismelor/sub-componentelor de optimizare a performantelor componentelor sistemului cu sugerarea operaţiunilor ce trebuiesc efectuate si/sau investigate de catre personalul tehnic in acest sens.

Agenţii pentru fiecare componentă de infrastructură urmărită nu trebuie să interfereze cu operaţiile normale ale componentei respective pentru a nu afecta performanţele acesteia

**Extensibilitate**

Arhitectura soluţiei este una deschisă orientată pe servicii (Service Oriented Architecture). Funcţionalităţile modulelor vor fi oferite prin intermediul unui set bine definit de servicii, acest lucru favorizând reutilizarea componentelor şi asigurând o bună integrare şi interoperabilitate cu sistemele externe.

Soluţia va fi pregătită pentru eventuale îmbunătăţiri şi extinderi realizate prin integrarea unor noi module în baza protocoalelor standard de comunicaţie şi prin API (Application Programming Interface), la nivelul aplicatiilor customizate. In mod analog, subsistemul de monitorizare a performantelor si asigurare a securitatii trebuie sa fie scalabil/extensibil.

Utilizarea serviciilor web (web Services) asigura o interoperabilitate ridicată a soluţiei, permiţând colaborarea cu aplicaţii bazate şi pe platforme heterogene.

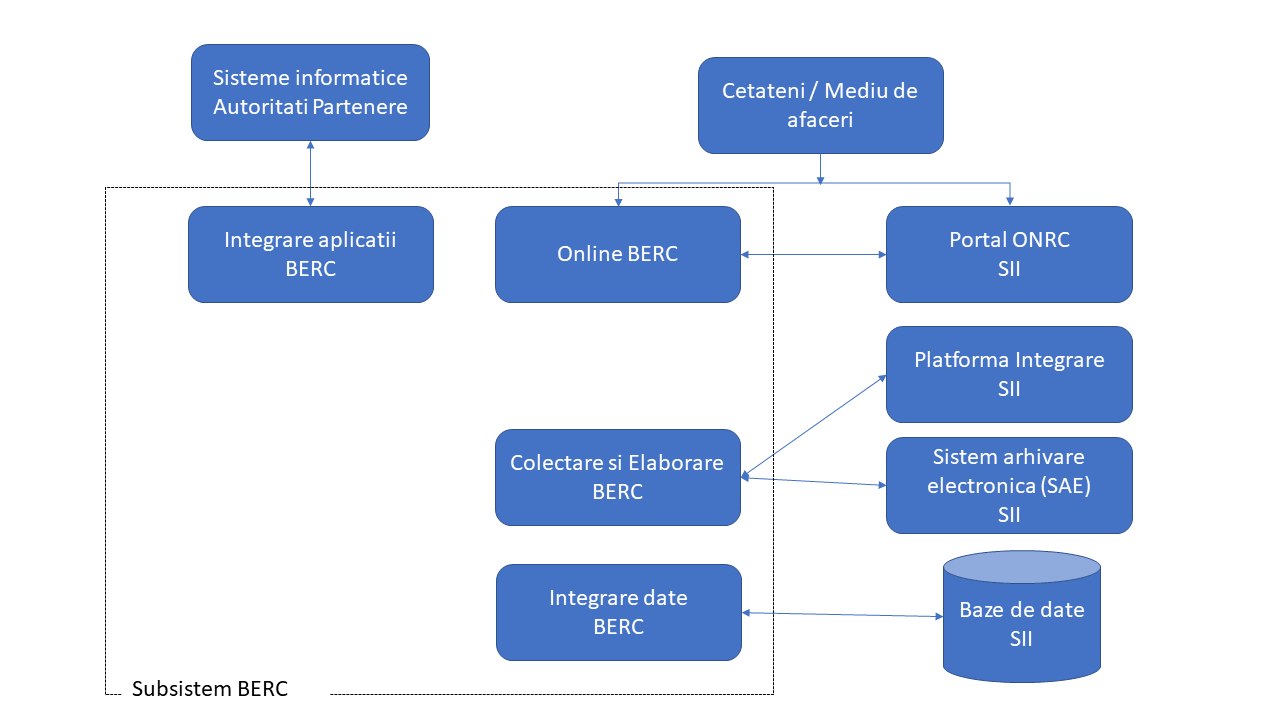
În vederea asigurării extensibilităţii, soluţia va trebui să respecte următoarele cerinţe:

* Soluţia va avea o arhitectură deschisă bazata pe standarde;
* Soluţia va oferi integrarea cu sisteme existente utilizând tehnologii moderne, de tip SOA;
* Soluţia trebuie să aibă la bază standarde în domeniu, ca de exemplu: Java 2 Enterprise Edition (J2EE), XML, suport pentru servicii web;
* Soluţia va fi flexibilă din punct de vedere al clienţilor de tip browser, al sistemelor de operare şi al suportului pentru bazele de date;
* Soluţia va oferi posibilitatea utilizării serviciilor web pentru a expune date şi servicii către sistemele externe platformei.

### Nivelul functional de aplicatie

* + - 1. Subsistemul Buletinul Electronic a Registrului Comertului

Descrierea logica a interactiunilor dintre componentele subsistemului BERC este descrisa in Figură 10.



Figură 10 Arhitectura logica subsistem BERC

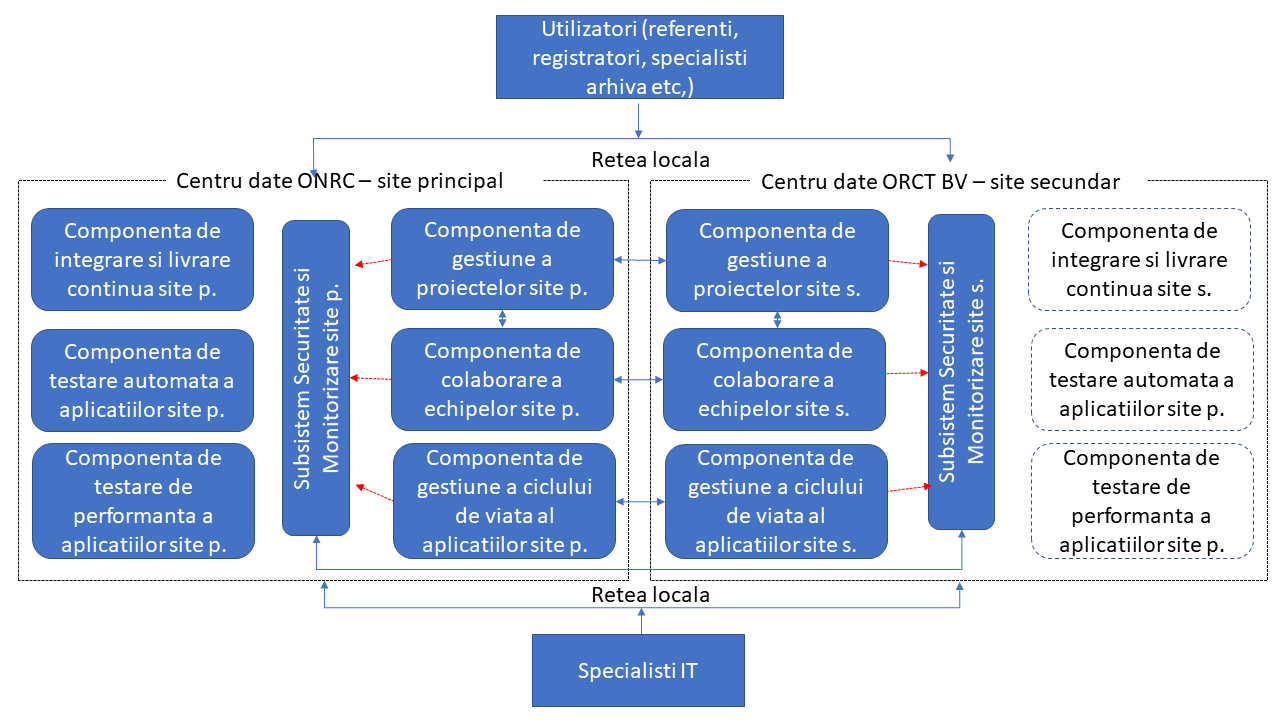
Componenta functionala de consultare online a BERC se va integra cu actualul portal al ONRC asigurand astfel autentificarea unica a utilizatorilor de portal in vederea accesarii atat a functionalitatilor existente in Portalul ONRC cat si a celor care vor fi furnizate de componenta functionala de consultare online a BERC.

Pentru integrarea cu aplicatiile existente din cadrul SII al ONRC componenta functionala de Colectare si Elaborare a BERC va apela serviciile disponibile in cadrul platformei de integrare a SII (bazata pe Oracle Service Bus) prin intermediul careia sunt interconectate aplicatiile SII.

Pentru integrarea la nivel de date componenta de Integrare date a BERC se va conecta direct bazele de date din cadrul SII.

* + - 1. Subsistemul Colaborativ

Descrierea logica a interactiunilor componentelor subsistemului Colaborativ este descrisa in Figură 11



Figură 11 Arhitectura logica Subsistem Colaborare

Asa cum se observa si din Figură 11 componentele functionale ce asigura gestiunea proiectelor, colaborarea echipelor si gestiunea ciclului de viata al aplicatiilor sunt prevazute a functiona geo-redundanta la nivelul aplicatiei iar componentele ce asigura testarea automata, testarea de performanta si livrarea/integrarea continua a aplicatiilor sunt prevazute a functiona in site-ul principal, geo-redundanta fiind asigurata la nivelul sistemului de virtualizare.

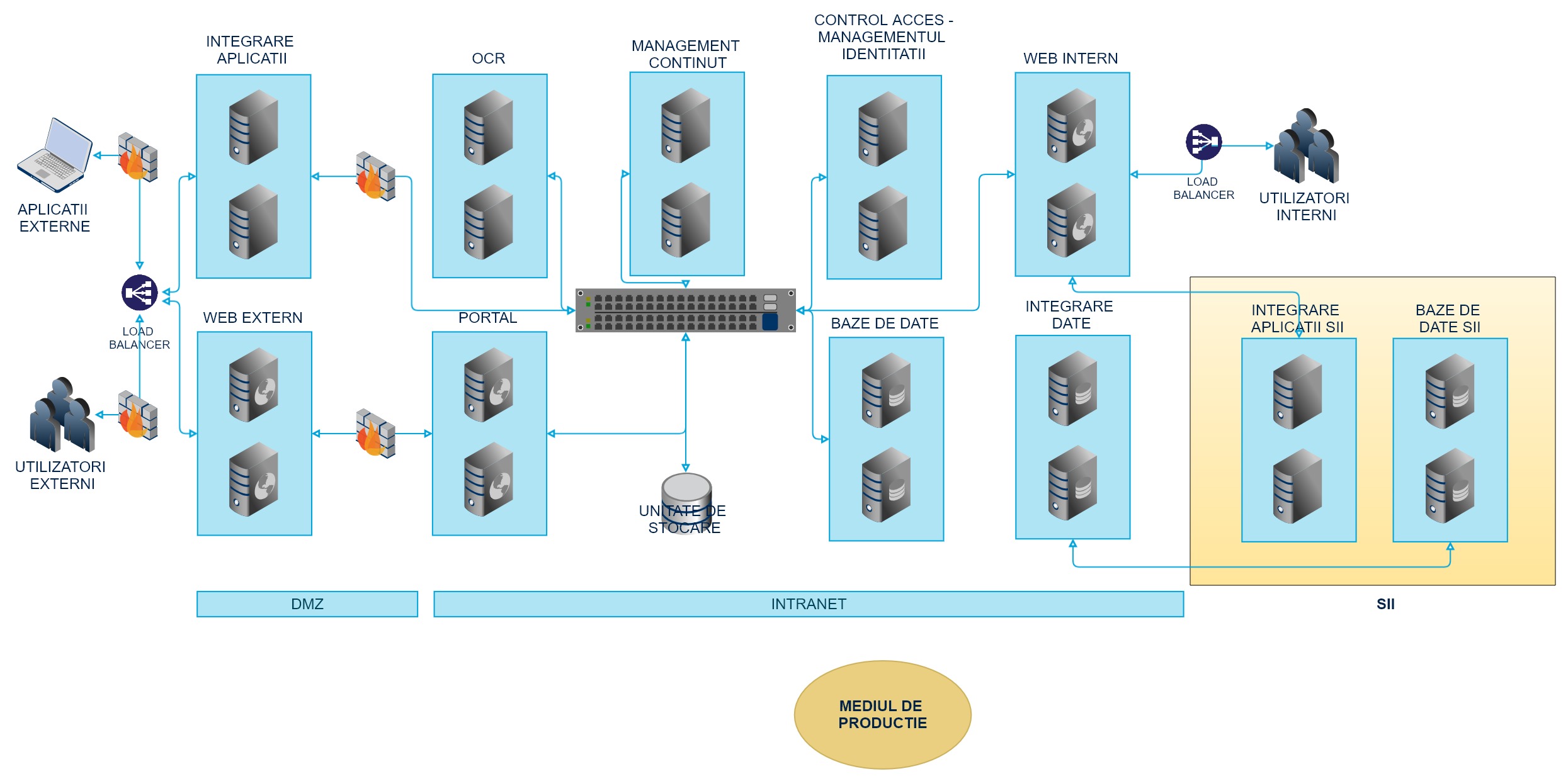
Componentele ce asigura testarea automata, testarea de performanta si livrarea/integrarea continua a aplicatiilor vor fi configurate astfel incat sa targheteze intregul mediu productiv al subsistemului BERC / Colaborare atat in ceea ce priveste testarea de performanta cat si instalarea de noi versiuni ale aplicatiilor customizate.

### Nivelul tehnic de aplicatie

* + - 1. Subsistemul Buletinul Electronic a Registrului Comertului

Toate serviciile on-line vor fi accesibile prin intermediul componentei Portal si a aplicatiei mobile dedicate clienţilor externi.

Arhitectura logica propusa pentru mediul de producţie al subsistemului BERC este prezentată în figură de mai jos:



Figură 12 Arhitectura logica propusa subsistem BERC

La nivel central sunt create structurile bazelor de date, inclusiv datele de gen nomenclatoare. La nivel central sunt instalate şi vor funcţiona toate componentele legate de securitatea platformei şi aplicaţiile interne. În plus, mediul va permite funcţionarea componentei de integrare şi interconectare cu aplicaţiile ONRC precum şi cu alte sisteme externe ONRC, dacă este cazul. De asemenea, la nivel central vor fi expuse informaţiile către utilizatorii externi şi persoanele interesate prin intermediul componentei Portal si a aplicatiei mobile.

In cadrul subistemului BERC se disting următoarele componente tehnice:

* Componenta Portal;
* Componenta server de aplicatie;
* Componenta de integrare aplicatii;
* Componenta de integrare a datelor;
* Componenta de gestiune a bazei de date;
* Componenta de procesare OCR;
* Componenta de gestiune conţinut şi documente;
* Componenta de dezvoltare a aplicatiilor mobile prin intermediul careia va fi dezvoltata si aplicatia mobila adresata utilizatorilor externi;

Functionalitatile de asigurare securitate / monitorizare centralizata (inclusiv backup-restore) sunt furnizate de subsistemul de securitate si monitorizare prezentat in cadrul acestui document.

Accesul la serviciile on-line se va face prin intermediul componentei **server web extern**. Accesul la aplicaţiile interne se va face prin accesarea componentei server web găzduit în intranetul ONRC (server web intern). Accesul la serviciile on-line, oferite prin intermediul componentei Portal a platformei, se va face prin intermediul unui cluster de servere web plasat în DMZ-ul ONRC (accesul se va face prin intermediul unei componente specializate hardware şi/sau software cu funcţionalităţi de load-balancing).

Componenta Server de Aplicaţii oferă contextul de rulare pentru componentele soluţiei: Portal, aplicaţiile de editare si elaborare a buletinului, integrare.

Aplicaţiile deservind utilizatorii - interni versus externi - vor fi găzduite după cum urmează:

* Utilizatorii interni vor accesa aplicaţiile interne instalate pe infrastructura de server de aplicaţii şi gestiune a conţinutului.
* Utilizatorii externi vor accesa numai componenta Portal a platformei pentru a obţine informaţii, a vizualiza conţinutul buletinelor electronice publicate, pentru a folosi serviciile disponibile.

În această manieră, se va realiza o delimitare strictă a utilizatorilor pe echipamente distincte, care să permită o utilizare judicioasă a resurselor de calcul puse la dispoziţie.

Serverul de aplicaţie destinat componentei Portal va găzdui toate serviciile on-line adresate utilizatorilor externi (din internet).

Aplicaţiile interne care vor deservi cu informaţii buletinele electronice vor rula pe o infrastructură de server de aplicaţii dedicată. Aplicaţiile interne vor fi construite pe baza cerinţelor funcţionale exprimate în acest document.

Pentru balansarea eficientă a cererilor utilizatorilor vor fi utilizate componente hardware şi/sau software de dirijare a încărcării către resursele soluţiei desemnate să rezolve optim aceste cereri.

Bazele de date utilizate de modulele soluţiei sunt găzduite de componenta server baze de date, instalat într-un segment de reţea separat. Pentru subsistemul BERC va exista o singură bază de date la nivel central. Totodata, prin intermediul componentei de integrare date se va asigura schimbul de date cu bazele de date din cadrul SII existent al ONRC.

Componenta de integrare aplicatii va asigura, în primul rând, atat interoperabilitatea aplicaţiilor BERC cu sisteme informatice ale autoritatilor partenere. Aceasta componentă va fi instalată pe un cluster dedicat de servere de aplicaţii. Integrarea la nivel aplicativ cu SII existent al ONRC va fi realizata prin intermediul componentei existente de integrare din cadrul SII.

Componenta de gestiune a continutului / documentelor va asigura gestiunea tuturor documentelor si versiunilor acestora pe perioada de la intrare/creare in ONRC pana la arhivare.

Componenta de procesare OCR va fi responsabila cu transformarea in format editabil a documentelor din format imagine (PDF, TIFF, JPEG, etc) in vederea reducerii timpilor de editare a buletinului electronic.

**Scenarii de utilizare**

***Utilizatorii interni ai ONRC***

* Utilizatorul ONRC/ORCT accesează prin intermediul browser-ului aplicaţia web;
* Autentificarea şi autorizarea utilizatorului este realizată de către serverul de control acces / SSO;
* În funcţie de drepturile asociate profilului, utilizatorul poate accesa anumite secţiuni din aplicaţia web;
* La nivelul fiecărui ecran de lucru utilizatorul poate efectua operaţii de citire, scriere şi ştergere.

***Utilizatorii externi***

* Utilizatorii externi ONRC, publicul larg, persoane fizice sau juridice, instituţii guvernamentale, care vor accesa componenta on-line a BERC;
* Autorizarea şi accesul se fac pe baza unui cont de utilizator (nume utilizator şi parolă); datorită arhitecturii folosite pentru autentificarea utilizatorilor pot fi utilizate şi alte soluţii (certificate digitale).
  + - 1. Subsistemul Colaborativ

Pentru deservirea componentelor functionale evidentiate in cap. 4.2.2, in cadrul subistemului Colaborativ au fost incluse următoarele componente tehnice:

* Componenta de gestiune proiecte;
* Componenta de colaborare a echipelor;
* Componenta de gestiune a ciclului de viata al aplicatiilor;
* Componenta de integrare si livrare continua a modificarilor de aplicatii;
* Componenta de testare automata a aplicatiilor;
* Componenta de testare de performanta a aplicatiilor;

Componenta de colaborare a echipelor si cea pentru gestiunea proiectelor sunt destinate utilizarii angajatilor ONRC/ORCT care vor fi implicati in proiecte sau care fac parte din comunitatile de specialisti pentru care se va implementat un cadru de colaborare digitala.

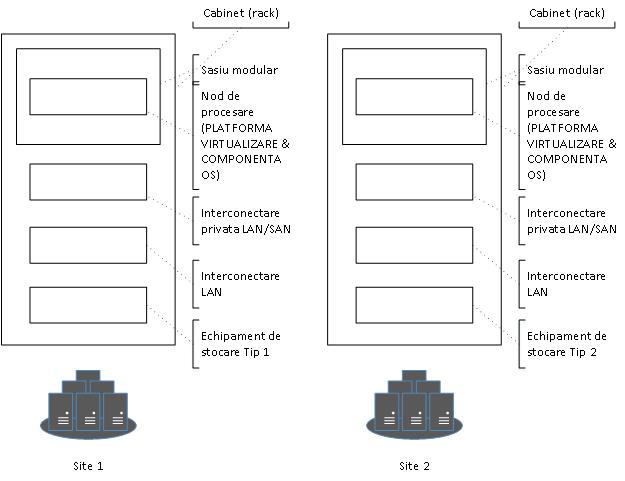
Celealte componente sunt destinate echipelor de specialisti IT pentru administrarea, intretinerea, mentenanta si testarea facila a aplicatiilor software personalizate.

### Nivelul tehnic de infrastructura

* + - 1. Subsistem tehnic de procesare

Subsistemul tehnic de procesare, stocare si integrare a datelor se compune din:

* Echipamente de tip sasiu modular,
* Echipamente de interconectare private LAN/SAN,
* Echipamente de procesare generala,
* Componenta de virtualizare sistem,
* Componenta de sistem de operare,
* Echipamente de integrare LAN,
* Echipament de stocare de Tip 1,
* Echipament de stocare de Tip 1.

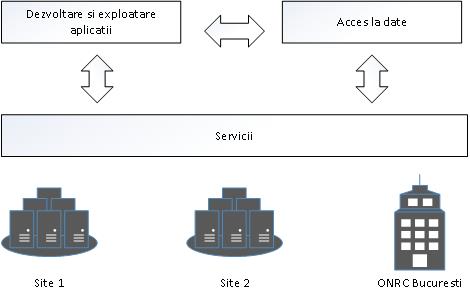


Figură 13 Schema de baza a subsistemului tehnic de procesare, stocare si integrare a datelor

* + - 1. Subsistem tehnic de monitorizare generala a datelor

Subsistemul tehnic de monitorizare generala a datelor se compune din:

* Componenta de monitorizare a dezvoltarii si explotarii aplicatiilor,
* Componenta de monitorizare a accesului la date,
* Componenta de monitorizare a serviciilor.

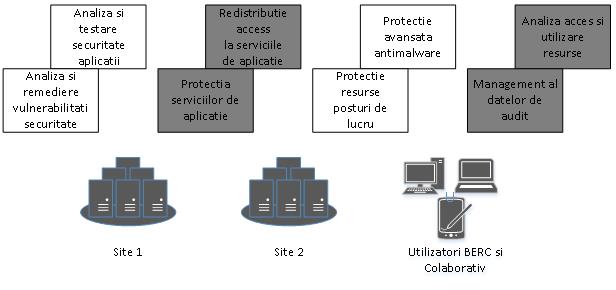


Figură 14 Schema de baza a subsistemului tehnic de monitorizare generala a datelor

* + - 1. Subsistem tehnic de securitate si audit

Subsistemul tehnic de securitate si audit se compune din:

* Componenta de analiza si testare de securitate a aplicatiilor,
* Componenta de analiza si remediere a vulnerabilitatilor de securitate,
* Componenta de analiza a accesarii si utilizarii resurselor,
* Componenta de redistributie la serviciile de aplicatie,
* Componenta de protectie a serviciilor de aplicatie,
* Componenta centrala de protective avansata antimalware,
* Componenta de protectie a resurselor la nivel de post de lucru,
* Componenta de management al datelor de audit.



Figură 15 Schema de baza a subsistemului tehnic de securitate si audit

### Arhitectura n-tier

Din punct de vedere tehnic, componentele funcţionale se vor sprijini pe anumite componente tehnice: server de aplicaţii, sistem de gestiune a bazelor de date, server web, platformă de integrare, etc.

În proiectarea, din punct de vedere tehnic, a sistemului informatic se pleacă de la următoarele premise, care constituie cerinţe minimale obligatorii:

* interfaţa utilizatorului este browserul web – aplicaţia fiind web-based;
* arhitectura aplicaţiei web trebuie să fie n-tier;
* componenta portal şi serviciile on-line trebuie să fie disponibile tuturor categoriilor de utilizatori;

De asemenea, noul sistem va trebui sa asigure interfaţarea şi interconectarea cu:

- Sistemul Informatic Integrat al ONRC;

- Sistemul de arhivare existent în tehnologie Captiva/IBM Content Manager şi JAVA;

- Plăţile on-line ONRC şi modulele economico – financiare.

Aplicaţiile software vor fi construite conform principiilor arhitecturii web multi-tier peste următoarele niveluri logice clar separate:

* ***Prezentare***

Interfaţa cu utilizatorul va asigura un meniu cu opţiuni de servicii cu posibilitatea de navigare între opţiuni şi sub-opţiuni*.* Interfaţa utilizator va fi intuitivă (facilă), informativă, fiabilă, atractivă şi stabilă.

* ***Business logic***

Modelul de business logic asigură transparenţa complexităţii acestuia faţă de utilizatori, fiind organizat conform următoarelor principii:

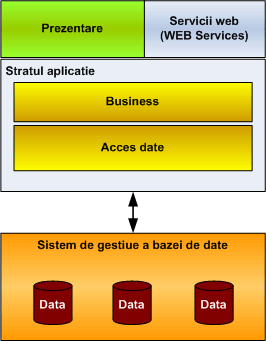
* Standardizare;
* Reutilizare;
* Separare clară între nivelul de prezentare şi business logic;
* Orientare servicii.

Nivelul de business logic asigură tratarea tuturor regulilor de procesare incluzând fără a se limita la:

* + Autentificare şi autorizări de securitate;
  + Managementul sesiunilor utilizatorilor;
  + Reguli de integritate date;
  + Reguli de orchestrare servicii;
  + Reguli de validare intrări;
  + Monitorizarea tranzacţiilor.
* ***Informaţii şi date***

Informaţia stocată în bazele de date şi utilizată în cadrul aplicaţiei prezintă următoarele particularităţi:

* volum mare de fişiere şi documente colectate în vederea publicării împreună cu datele aferente;
* acurateţe ridicată, obţinută prin verificarea surselor de intrare, cu raportarea eventualelor neconcordanţe;
* necesitatea de a suporta un proces de analiză complexă;
* diseminare internă.



Figură 16 Niveluri arhitecturale

## Descrierea nivelului tehnic al sistemului

### Caracteristici specifice ale subsistemelor tehnice

In elaborarea arhitecturii de sistem, respectiv a specificatiilor tehnice pentru fiecare echipament/categorie de echipamente s-au avut in vedere cerintele specifice pentru fiecare nivel de infrastructura coroborate cu cerintele si provocarile de natura tehnica pentru fiecare tip de functionalitate, astfel incat sa se obtina un sistem scalabil ce va oferi totalitatea resurselor tehnice necesare (capacitate, performanta si disponibilitate), fara a impune vreo limitare de natura tehnica.

* Prin implementarea solutiei preconizate se doreste obtinerea unui set comun de obiective functionale si operationale, atat pentru fiecare element/platforma din infrastructura cat si pentru arhitectura globala a proiectului:
* Complexitate redusa a platformelor, in scopul integrarii si extinderii cu usurinta, atat din punct de vedere operational cat si functional;
* Complet redundanta la nivelul tuturor elementelor componente, in scopul protejarii facile a datelor rezidente si efectuarii transparente a operatiunilor de administrare, update, upgrade si inlocuire a componentelor ce se pot defecta;
* Mecanisme native de redundanta locala, integrate cu restul elementelor de infrastructura, pentru protectia continua si completa a aplicatiilor, proceselor si serviciilor deservite in eventualitatea unor defectiuni majore;
* Scalabila in mod transparent pentru aplicatiile, procesele si serviciile deservite, in scopul extinderii ulterioare a solutiei, indiferent de necesitatea scalarii – capacitate, conectivitate si performanta;
* Bazata pe componente standard, in scopul integrarii si extinderii facile a setului de aplicatii/procese/servicii si cerinte existente in infrastructura, precum si cu orice alte noi cerinte viitoare;
* Unelte de administrare integrate si facil de folosit, ce acopera intreaga functionalitate, independente de anumite elemente de infrastructura (sistem de operare, tehnologie de aplicatie, etc), in scopul reducerii eforturilor operationale si costurilor de integrare in infrastructura;
* Functionalitati integrate de securitate, integrate cu restul elementelor de infrastructura, in scopul securizarii complete a accesului si manipularii datelor de catre utilizatori, aplicatii si servicii;
* Mecanisme integrate de agregare a resurselor fizice din infrastructura (procesare, stocare, comunicatie), mecanisme integrate de analiza predictiva si aplicare proactiva de politici asupra resurselor in scopul obtinerii maximului de performanta si eficienta indiferent de aplicatiile si serviciile deservite de platforme, asigurand disponibilitate maxima, timpi de raspuns la incidente si costuri operationale minime;
* Platforme integrate nativ ce vor permite reducerea semnificativa a timpilor de nefunctionare a aplicatiilor si serviciilor, reducerea proceselor operationale, respectiv a timpilor de solutionare a incidentelor, distribuirea uniforma a capacitatilor de procesare, stocare si comunicatie cu imbunatatirea semnificativa a gradului de utilizare relativ la fiecare resursa fizica, diminuarea costurilor operationale.

Sistemele/echipamentele ofertate trebuie sa respecte urmatoarele cerinte generale:

* Sistemele si echipamentele livrate trebuie sa fie noi, neutilizate si de ultima generatie. Ele trebuie sa asigure gradul necesar de performanta, fiabilitate si flexibilitate fiind proiectate si destinate pentru aplicatii critice de tip “enterprise level”;
* Dispozitivele hardware trebuie sa fie astfel proiectate incat sa poata asigura scalabilitatea sistemului in cazul cresterii ulterioare a necesarului de resurse de calcul;
* Dispozitivele hardware trebuie sa fie compatibile cu caracteristicile retelei electrice din Romania astfel incat sa fie garantata conectarea fara probleme a acestora la reteaua electrica existenta a beneficiarului;
* Toate aceste cerinte sunt dezvoltate la nivel de detaliu in cadrul cererii de oferta. In acelasi timp cerintele nu sunt limitative ofertantii avand libertatea de a le dezvolta si extinde conform solutiei pe care au in vedere sa o propuna si care trebuie să îndeplinească în totalitate cerintele beneficiarului;
* Ofertantii vor avea în vedere că toate cerintele si caracteristicile solicitate explicit pentru Solutia propusa in cadrul cererii de oferta au un caracter minim si obligatoriu.
  + - 1. Echipamente de tip șasiu modular

Soluţia/componentele oferite trebuie să îndeplinească următoarele **cerinţe functionale generale**:

* Arhitectura soluţiei propuse trebuie să includă următoarele caracteristici generale de fiabilitate, disponibilitate şi uşurinţă în efectuarea operatiunilor de intretinere/remediere a defectiunilor (Reliability Availability Serviceability-RAS) la nivel de servere sau şasiu:
  + Componente redundante în interiorul sistemului (surse de alimentare electrică, module de ventilatie, module de procesare, module de comunicatie);
  + Capabilităţi de auto-testare şi rezolvare a defectelor intermitente fără intervenţie umană;
  + Dealocarea “online” şi izolarea componentelor defecte ale sistemului (de exemplu discuri, ventilatoare, subsisteme de alimentare cu energie electrică, adaptoare PCI). In momentul reboot-ului componentele defecte vor fi deconfigurate;
  + Diagnosticarea erorilor în timp real;
  + Capabilităţi arhitecturale de prevenire a erorilor.
* Platforma de procesare reprezintă un ansamblu modular pentru suportul procesării, în arhitecturi mixte eterogene dedicat operatiunilor de procesare specifice, format din şasiu modular şi module de procesare generala, detaliate in subcapitolele urmatoare.

Echipamentul de tip şasiu modular trebuie sa respecte urmatoarele **cerinte functionale specifice**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Componenta de tip şasiu modular pentru suportul procesării centralizate, cu suport inteligent pentru optimizarea, balansarea si integrarea modulelor de procesare, de stocare si a extensiilor de I/O ale acestora, precum şi a modulelor de management; * Sasiul trebuie sa suporte interconectarea cu alte sasiuri similare si agregarea resurselor de procesare, stocare si a extensiilor I/O ale acestora intr-o singura platforma unificata, administrabila prin intermediul unui singur set unitar de unelte de management; * Şasiul trebuie configurat pentru instalarea a minim 8 noduri de procesare de tip blade sau similare, optimizate pentru asigurarea densităţii si puterii de calcul necesare; * Şasiul va fi echipat cu toate componentele redundante, hot-plug/hot-swap şi utilizabile în mod concurent, pentru alimentare şi ventilare, management (inclusiv procesoare de serviciu/management); |
| Functionalitati si performante | * Şasiu făra management local, a carui administrare să se poată face integrat, la nivelul întregului sistem, prin interfaţa unică de administrare; * Să nu necesite o configurare iniţială si să fie recunoscut automat de aplicaţia unică de administrare; * Midplane de tip pasiv, capabil să: * Asigure interfeţe de tip „10 Gigabit Ethernet” şi „40 Gigabit Ethernet” pentru nodurile de procesare; * Asigure minim 2(două) interfeţe pentru fiecare server blade; * Asigure o largime de bandă agregată pentru nodurile de procesare de minim 1,2Tbps; |
| Interconectare LAN/SAN | Se va face prin 2 dispozitive cu rol de extensie locală a echipamentelor externe pentru accesul unificat în cele două reţele. Cele două dispozitive vor asigura următoarele funcţionalităţi:   * Failover automat prin acces de tip „active – active” la midplane-ul şasiului şi la echipamentele pentru accesul unificat; * Autoconfigurare, prin sincronizarea automată a firmware-ului local cu cel de pe echipamentele pentru accesul unificat; * Fără management local, administrarea acestora făcându-se integrat, la nivelul întregului sistem, prin interfaţa unică de administrare; * Minim 32 porturi interne de tip „10 Gigabit Ethernet” şi 4 (patru) porturi externe de tip „40 Gigabit Ethernet”, capabile FCOE; * Performanţă de comutare: minim 960 Gbps; * Funcţionalităţi „Layer 2”: * Minim 1000 VLAN-uri şi VSAN-uri; * Suport pentru „jumbo frames” (9216 bytes) pe toate porturile; * La mutarea unei maşini de pe un nod de procesare pe altul conlucrează cu celelalte componente ale sistemului pentru a transfera automat identitatea de reţea a acesteia (adresă MAC, adresă IP, VLAN, QoS, politici de securitate, etc.) în noul context; * QoS: * Bazat pe standardul IEEE802.1p; * Cozi de servire a pachetelor, in iesire, bazate pe campul COS (Class Of Services) şi cu capabilităţi de prioritizare strictă; * Minim 8 cozi hardware per port; * Planificarea porturilor de ieşire prin WRR (Weighted Round Robin); |
| Surse de alimentare | * Surse de alimentare interne în şasiu, de tip „hot-swap”, care să asigure alimentarea redundantă în condiţii de încarcare maximă a şasiului; * Redundanţă de tip „N+1” si „N+N”, cu capabilităţi „load-balancing” şi „failover”; * Plaja de tensiune operabilă: 200-240V AC; * Plaja de frecvenţa suportată: 50– 60 Hz; * Echipare minimală: 4 surse; * Puterea minimă per sursă: 2500 W; * Sursele se livrează cu cablu de alimentare tip PDU; |
| Sistem de ventilaţie | * Sistem de ventilaţie de tip „hot-swap”, redundant, instalat intern în şasiu; * Flux de aer din fata catre in spate; * Echipare minimală: 8 ventilatoare; |
| Cerinte constructive | * Montabil în rack-uri standard de 19”; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Echipamente de interconectare privată LAN/SAN

Echipamentele de interconectare privata LAN/SAN trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | Complet redundanta bazata pe cel putin 2 module de comunicatie; |
| Funcţionalităţi si performanţe | * Echipamentul va asigura două funcţionalităţi majore: * Accesul unificat al nodurilor de procesare generala la reţeaua Ethernet şi la storage, prin tehnologia FCoE; * Managementul centralizat al resurselor infrastructurii – noduri de procesare generala (procesoare, memorie, BIOS, adaptoare CNA, interfeţe LAN şi SAN, etc), şasiu (surse de alimentare, ventilaţie, dispozitivele de extensie FCoE, etc) – şi al componentelor proprii de integrare în reţelele LAN şi SAN, printr-o interfaţă unică de administrare şi monitorizare; * Porturi: * Cel putin 40 de sloturi tip „QSFP” si „SFP+”, capabile FCoE, 10 si 40 Gigabit Ethernet, precum si 4, 8, 16G Fibre Channel (FC), pentru conectarea la şasiul de noduri de procesare şi la reţeaua Ethernet, precum si la platformele de stocare; * Cel putin 16 din aceste porturi trebuie să poată funcţiona, la alegere, ori in mod FCoE, ori in mod 10 Gigabit Ethernet, ori in mod 4, 8 sau 16G Fibre Channel (FC); * Cel putin 8 din aceste porturi trebuie să poată funcţiona atat ca 40 Gbps Ethernet cat si ca 4x10 Gbps Ethernet (cu transceiver de tip QSFP sau echivalent); * Capacitate de procesare: minim 2 Tbps; * Disponibilitate înaltă: * Cele două echipamente trebuie să poată lucra intr-o arhitectură de tip „cluster”, în care software-ul care asigură interfaţa unică de administrare a sistemului va funcţiona în mod „activ – pasiv”; * Interfeţele prin care se va face comunicaţia in interiorul cluster-ului trebuie să fie dedicate, altele decat cele mai sus menţionate; * Funcţionalităţi „Layer 2”: * Minim 1000 VLAN-uri şi VSAN-uri per echipament; * Suport pentru „jumbo frames” (9216 bytes) pe toate porturile; * Rapid Per-VLAN Spanning Tree Plus; * IGMP versiune 1, 2 şi 3 snooping; * EtherChannel bazat pe IEEE 802.3ad cu capabilităţi avansate de distribuire a traficului, prin funcţii de hashing ce iau în calcul informaţii Layer 2, 3 şi 4; * La mutarea unei maşini de pe un nod de procesare pe altul conlucrează cu celelalte componente ale sistemului pentru a transfera automat identitatea de reţea a acesteia (adresă MAC, adresă IP, VLAN, QoS, politici de securitate, etc.) în noul context; * QoS: * Bazat pe standardul IEEE802.1p; * Egress queuing, bazat pe COS şi cu capabilităţi de prioritizare strictă; * Minim 8 cozi hardware per port; * Planificarea porturilor de ieşire prin WRR (Weighted Round Robin); |
| Management | * Centralizat, pentru toate componentele sistemului, printr-o aplicaţie unică de administrare şi monitorizare care va rula în cadrul cluster-ului, în mod „activ – pasiv”; * Instanţa aplicaţiei (cea „activă”) trebuie să poată administra ambele echipamente pentru acces unificat, minim 16 şasiuri cu noduri de procesare generala şi minim 128 de noduri de procesare; * Accesul la aplicaţie trebuie să se poată face din reţeaua IP prin interfaţă GUI, prin interfaţă în linie de comandă (CLI) şi prin API XML public; * Aplicaţia trebuie să rezide în firmware-ul echipamentelor şi să nu necesite un server de management extern; * Comunicaţia dintre aplicaţie şi celelalte componente ale sistemului – şasiu, noduri de procesare, adaptoare unificate de comunicatie, dispozitivele de extindere trebuie să se desfaşoare automat şi să se bazeze pe funcţii de „autodescoperire”; * Aplicaţia trebuie să permită provizionarea nodurilor de procesare şi a parametrilor lor I/O prin definirea şi utilizarea de profiluri; * Profilurile trebuie să permită crearea unui nivel de abstractizare care să permită decuplarea identităţii unui nod de procesare (procesor, memorie, BIOS, interfeţe LAN şi SAN, adrese MAC si WWN), împreună cu drepturile de acces în reţea şi stocare necesare (VLAN, QoS, Security, VSAN, Zoning, LUN-uri) de hardware-ul şi infrastuctura LAN/SAN pe care, la un moment dat, acesta le foloseşte; * Aplicaţia trebuie să permită operaţionalizarea la cerere a unuia sau mai multor noduri de procesare fizice, prin configurarea automată a unuia sau mai multor noduri de procesare, adaptoare unificate de comunicatie, NIC şi HBA, dispozitive de extindere a accesului din şasiuri, şi a parametrilor necesari accesului în LAN şi SAN, pe echipamentele pentru acces unificat, avand drept referinţă un profil definit anterior; * Aplicaţia trebuie să asigure funcţii de inventariere, diagnostic, monitorizare, detecţie a erorilor, auditare şi colectare de statistici; * Aplicaţia trebuie sa poată exporta configuraţia întregului sistem, facilitând procese bazate pe ITIL; |
| Surse de alimentare | * Minim 2 surse de alimentare interne, de tip „hot-swap”, care să asigure alimentarea redundantă în condiţii de încarcare maximă a şasiului cu transceiver-e; * Redundanţă de tip „1+1”, cu capabilităţi „load-balancing” şi „failover”; * Plaja de tensiune operabilă: 100-240V AC; * Plaja de frecvenţa suportată: 50– 60 Hz; * Se livrează cu 2 cabluri de alimentare de tip PDU; |
| Sistem de ventilaţie | * Sistem de ventilaţie de tip „hot-swap”, redundant, instalat intern; * Flux de aer de tip “front to back”; * Echipare minimală: 2 ventilatoare, în configuraţie redundantă “1+1”; |
| Cerinte constructive | * Montabil în rack-uri standard de 19”; * Dimensiune maxima 1U; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Echipamente de procesare generală

Echipamentele de procesare generala trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Nod de procesare generala de tip blade, compatibil cu Şasiul modular pentru suportul procesării centralizate ofertat; * Suport multiprocesor pentru minim 2 procesoare fizice; |
| Procesor | * Număr de procesoare instalate: minim 2; |
| Memorie interna | * Tip memorie: DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4; |
| Interfeţe de reţea | * Minim 2x10 Gigabit Ethernet, prin adaptor de tip “Unified”: * Cu funcţionalitate FCOE; * Cu suport pentru failover si load balancing; * Capabil să furnizeze virtualizare la nivel de adaptor un minim de 64 interfeţe virtuale LAN şi SAN, care să poată fi create dinamic şi la cerere, şi care să fie văzute de serverul fizic ca dispozitive PCI-e locale, alocabile maşinilor virtuale; * Sa suporte procesarea in hardware a protocoalelor pentru virtualizarea retelelor VXLAN si NVGRE |
| Stocare | Doua carduri SD conectate la un controller RAID cu suport pentru RAID1; |
| Acces | * Suport pentru acces prin KVM local; * Suport pentru acces de tip „out of band” prin: * KVM la distanţă, bazat pe IP; * Protocol SSH; * Virtual Media şi IPMI (Intelligent Platform Management Interface); |
| Management | * Procesor de management integrat, cu capabilităţi de monitorizare a componentelor critice local şi de la distanţă; * La instalare şi pentru integrarea în sistem, nodul de procesare nu trebuie să necesite o configurare prealabilă; * Nodul de procesare trebuie să posede o facilitate de „autodescoperire”, prin care este recunoscut şi configurat automat de către aplicaţia unică de administrare a componentelor întregului sistem; |
| Compatibilitate sisteme de operare | Suport pentru Microsoft Windows Server 2012 R2/2016, VMware vSphere 6.0/6.5, Red Hat Linux 7.x; |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Componenta de virtualizare sistem

Solutia va include o componenta de virtualizare dedicata, bazata pe Hypervizor propriu, fara dependenta de un sistem de operare anume. Aceasta solutie va fi instalata direct in platforma de procesare si va beneficia de suportul acestei platforme atat la nivelul capacitatii de procesare cat si la nivelul optiunilor de conectica si integrare cu restul elementelor fizice de infrastructura.

Componenta de virtualizare sisterm trebuie sa indeplineasca urmatoarele **cerinte functionale specifice**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Functionalitati | * Hypervizorul trebuie sa fie matur, testat si implementat in infrastructuri de productie complexe si sa ofere performanta maxima pentru aplicatiile si serviciile instalate in masini virtuale indiferent de complexitatea si natura acestora.Nivelul de abstractizare a componentelor fizice din platformele de procesare, stocare si comunicatie nu trebuie sa adauge complexitate si/sau penalizari de performanta sesizabile in functionarea aplicatiilor si serviciilor deservite; * Platforma de virtualizare trebuie sa fie compatibila cu toti producatorii hardware recunoscuti: IBM, Dell, HP, Sun, Intel, iar hypervizorul pe care aceasta plaforma se bazeaza trebuie sa fie independent de producatorul sau de metoda de stocare interna/externa disponibila in platforma de procesare si/sau stocare pe care ruleaza; * Platforma de virtualizare trebuie sa ofere suport pentru urmatoarele sisteme de operare instalabile in masina virtuala: Windows Xp/Vista/7/10/2003/2008/2008 R2/2012 R2/2016, Linux Suse/Red Hat/CentOS, FreeBSD, Solaris, Netware si sa permita adaugarea de spatiu de stocare pentru masinile virtuale prin folosirea urmatoarelor protocoale: NAS – NFS ; SAN – iSCSI/FC/FCoE, asigurand astfel compatibilitate cu majoritatea tehnologiilor implementate in mod uzual atat in platformele de procesare cat si in platformele de stocare; * Platforma de virtualizare nu trebuie să depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea şi funcţionalitatea echipamentelor din platforma de procesare, respectiv a maşinilor virtuale care rulează pe aceste echipamente; * Amprenta pe disc a hypervisor-ului trebuie sa aiba dimensiuni reduse astfel incât instalarea hypervisor-ului să poata fi realizata foarte rapid chiar şi prin intermediul retelei de comunicatie, oferind totodată posibilitatea de rulare integrala din mediu de tip USB; * Platforma de virtualizare trebuie sa ofere suport nativ pentru USB 3.0 şi rularea de aplicaţii grafice (DirectX sau OpenGL2) in masinile virtuale rezidente, respectiv suport pentru accelerarea video in hardware pentru respectivele masini virtuale (suport pentru tehnologia de accelerare video oferita de NVIDIA GRID sau echivalent); * Platforma de virtualizare trebuie sa ofere suport nativ pentru conectarea pe port serial in orice masina virtuala, prin folosirea unui concentrator serial de retea; * Componentele virtuale ale platformei sa poata fi modificate cu usurinta permitand astfel crearea de configuratii diferite pentru seturi comune de masini virtuale, precum si crearea de configuratii unitare la nivelul intregii infrastructure virtuale, atat din prisma elementelor virtuale de procesare si stocare (integrate nativ in platforma sau prin integrarea nativa cu componente terte ale respectivelor platforme de proceare si stocare), cat si din prisma elementelor de comunicatie (posibilitatea integrarii directe cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea si asigurarea crearii unei retele virtuale unificate la nivelul intregii infrastructuri virtuale); * Platforma de virtualizare trebuie sa ofere mecanisme nativ integrate pentru adaugarea de resurse de procesare si memorie fara restartarea sistemului de operare din masina virtuala, (in masura in care sistemul de operare suporta aceste facilitati), mecanisme ce pot fi independente de platformele de procesare/stocare/comunicatie sau prin intermediul unor conectori/componente comune respectivelor platforme; * Prin integrarea nativa cu platformele de procesare, masinile virtuale definite in platforma de virtualizare trebuie sa beneficieze concomitent de suport de multiprocesare simetrica a minim 64 procesoare logice, minim 1 TB de RAM si acces la totalitatea porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile in infrastructura; * Resursele virtuale (resurse de procesare, stocare si comunicatie) disponibile la nivelul intregii platforme de virtualizare (prin integrarea nativa cu platformele fizice de procesare, stocare si comunicatie) trebuie sa fie adresabile si configurabile in totalitatea lor prin intermediul unei singure interfete de management si nu prin configurarea separata pentru fiecare echipament disponibil in respectivele platforme; * Platforma de virtualizare trebuie sa permita agregarea tuturor resurselor fizice (placi de retea, switch-uri de comunicatie integrate in platformele de procesare) si virtuale de comunicatie (switch-uri virtuale) intr-un singur nivel unitar de comunicatie, adresabil la nivelul intregii infrastructuri virtuale indiferent de complexitatea acesteia sau a platformelor de procesare si comunicatie ce se integreaza prin intermediul ei.Deasemenea trebuie sa ofere mecanisme automate de evaluare si prioritizare continua a accesului masinilor virtuale si aplicatiilor rezidente la resursele de comunicatie disponibile, permitand alocarea si realocarea dinamica a acestor resurse in functie de cerintele de moment sau conform unor politici prestabilite; * Platforma trebuie sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati, precum si izolarea acestor grupari de resurse, respectiv sa asigure flexibilitatea necesara maririi cantitatii de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari.Accesul masinilor virtuale si apartenenta la aceste grupari de resurse trebuie sa se faca atat in mod manual prin interventia unui operator cat si pe baza unor politici dinamice de acces; * Platforma trebuie sa ofere functionalitati integrate nativ de pornire/repornire a oricarei masini virtuale (indiferent de aplicatiile si serviciile ce ruleaza pe respectivele masini virtuale), in cadrul aceluiasi server sau pe servere diferite, in cazul detectarii nemijlocite a unei probleme de functionare a masinii virtuale au a aplicatiilor si serviciilor ce ruleaza pe aceste masini virtuale.Scenarii posibile ce necesita implementarea nativa a unui astfel de mecanism de recuperare ar putea fi: blocarea sistemului de operare ce ruleaza in masina virtuala, intreruperea cailor de comunicatie catre platformele de stocare, intreruperea cailor de comunicatie catre platforma comuna de management, etc; * Platforma trebuie sa ofere mecanisme integrate de balansare a incarcarii resurselor fizice si virtuale disponibile in infrastructura si redistribuire a sarcinilor generate de utilizatori, servicii si aplicatii, prin integrarea nativa cu platformele hardware, indiferent de producatorul respectivelor elemente de infrastructura.Aceste mecanisme trebuie sa fie disponibile atat la comanda prin interventia unui operator cat si prin operatiuni automate definite in functie de necesitati, gradul de ocupare al resurselor si/sau pe baza unor reguli/politici prestabilite; * Platforma de virtualizare trebuie sa ofere redundanta completa a arhitecturii, atat la nivelul elementelor virtuale distincte (procesoare, memorie, elemente de comunicatie, masini virtuale, etc) cat si la nivelul unor seturi intregi de echipamente de infrastructura (platforma de procesare, platforma de stocare, platform de comunicatie, etc) prin integrarea nativa cu mecanismele redundante existente in aceste platforme si prin folosirea unor tehnologii native de redundanta, balansare si fail-over aplicabile intregului spectru de functionalitate asigurata (masini virtuale, servcii, aplicatii, platforme de procesare, platforme de stocare, platforme de comunicatie); * Platforma de virtualizare trebuie sa permita configurarea spatiului de stocare virtual prin integrarea directa cu platforma de stocare aleasa prin intermediul unor conectori/componente native sau de la producatorul platformei de stocare, mecansim ce va permite extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri. Deasemenea prin integrare directa cu platforma de stocare, trebuie sa ofere mecanisme automate de monitorizare a incarcarii I/O si de alocare/realocare dinamica a resurselor I/O catre masinile virtuale in functie de cerintele acestora (ad-hoc sau conform unei politici prestabilite), realizand astfel o prioritizare inteligenta a accesului aplicatiilor la resursele de stocare; * Prin aceleasi mecanisme de integrare (inclusiv la nivelul componentelor apelabile si programabile din cadrul altor platforme, componente de tip API) cu platformele de stocare ofertate, trebuie sa permita identificarea si folosirea optima a mecanismelor de asigurare a cailor redundante de acces in platformele de stocare si a mecanismelor terte de protectie a datelor stocate, incluzand volumele adresate direct de platforma de virtualizare, respectiv volumele de date folosite de aplicatii, servicii si utilizatori; * Integrarea nativa cu platformele de stocare alese trebuie sa permita alocarea dinamica de spatiu catre masinile virtuale, chiar daca acel spatiu nu este fizic disponibil in aceste platforme, permitand functionarea corecta a aplicatiilor si serviciilor ce necesita resurse stricte de spatiu de stocare, respectiv cresterea transparenta a volumelor de date prin adaugarea de resurse fizice de stocare (discuri) doar in momentul cand acestea devin necesare; * Platforma trebuie sa includa mecanisme proprietare de catalogare si grupare a resurselor disponibile in platformele de stocare, indiferent de tipul, producatorul si numarul acestora (tipuri de discuri, latenta, tipul volumelor si metoda de export aplicata asupra lor ), permitand astfel crearea de profile de stocare si asocierea acestor profile cu distribuirea/redistribuirea masinilor virtuale in functie de cereri temporare ale aplicatiilor sau in baza unor politici predefinite; * Deasemenea trebuie sa includa atat mecanisme automate de evaluare continua a necesarului de resurse I/O cat si mecanisme de pozitionare si repozitionare a masinilor virtuale in gruparile de resurse de stocare in functie de cerintele initiale ale aplicatiilor, respectiv in functie de cerintele evaluate in mod continuu.Astfel se obtine o balansare permanenta a distributiei masinilor virtuale proportional cu gruparile de resurse de stocare, indiferent de cerintele de performanta si capacitate de stocare ale respectivelor masini virtuale; * Trebuie sa integreze nativ mecanisme de agregare a conexiunilor fizice de retea disponibile in platformele de procesare, astfel incat sa poata oferi un sigur nivel virtual si unificat de comunicatie, nivel ce va fi disponibil pentru intregul set de aplicatii si servicii gazduite in platforma de virtualizare.Mecanismele vor fi independente de platformele de procesare si de cele de comunicatii, permitand adaugarea transparenta de functionalitati specifice de comunicatie (management, control si tipuri de protocol suportate) de la producatori terti.Se va obtine astfel implementarea unui set comun de functionalitati, unitar la nivelul arhitecturii de retea (fizica si virtuala), set ce va permite distribuirea inteligenta, dinamica a incarcarii pe aceste conexiuni, respectiv redundanta nativa atat la nivelul conexiunilor de retea fizice/virtuale, cat si la nivelul strict al setului de functionalitati implementate, indiferent de producatorul platformelor de procesare si de comunicatie folosite; * Platforma trebuie sa implementeze nativ mecanisme de asigurare dinamica a prioritizarii accesului la aplicatii si servicii, prin integrarea directa cu platformele de stocare si de comunicatie ofertate, respectiv prin aplicarea de politici si profile asupra accesarii datelor ce constituie masinile virtuale respective si/sau sunt folosite de catre respectivele aplicatii, indiferent de locatia respectivelor date (rezidente in platforma de stocare sau tranzitate prin mediile de comunicatie fizice/virtuale).Se va obtine astfel garantarea accesului prioritar la aplicatiile si serviciile critice din infrastructura; * Platforma va trebui sa integreze mecanisme automate de instalare/provizionare a unei intregi imagini preconfigurate de hypervizor, mecanism necesar in cazul adaugarii rapide a unui nou server in platformele de procesare virtualizata, precum si mecanisme automate de instalare/provizionare a actualizarilor software la nivelul sistemelor de operare instalate in masinile virtuale, mecanisme idependente de, dar integrate cu functionalitatile de actualizare native ale respectivelor sisteme de operare; * Prin integrarea cu resursele de management, platforma de virtualizare trebuie sa permita mecanisme integrate de mutare a masinilor virtuale de pe un server pe altul sau dintr-un datacenter in altul fara oprirea sistemului de operare ce ruleaza in masina virtuala si fara intreruperea serviciului oferit de aplicatia/aplicatiile din masina virtuala.Aceleasi mecanisme trebuie sa permita atat mutarea intregului harddisk virtual concomitent pentru oricare masina virtuala in cadrul aceluiasi datacenter sau intre datacenter-e diferite, independent de platforma de stocare folosita si de mecanismele de replicare ale acesteia, precum si extinderea automata a harddisk-urilor virtuale pe masura ce sistemul de operare si aplicatiile din masinile virtuale o cer.In acest fel vor deveni posibile scenarii automate, prin politici pre-definite/definibile, de consolidare a masinilor virtuale pe un numar prestabilit de servere si oprirea automata a serverelor fara activitate sau cu subutilizare a resurselor de procesare; * Tot prin integrarea cu resursele de management, platforma de virtualizare trebuie sa permita operatiuni automate, bazate pe politici pre-definite/definibile, de repornire (pe o alta platforma de procesare) a masinilor virtuale individuale, precum si a seturilor de masini virtuale ce au fost definite ca deservind o singura aplicatie/serviciu sau un sub-set al unei aplicatii/serviciu, in eventualitatea unei defectiuni hardware majore la nivelul platformelor de procesare; * Platforma trebuie sa includa functionalitate nativa de rulare in paralel a unei masini virtuale sau a unui set de masini virtuale ce deservesc o singura aplicatie/serviciu, pe un numar de minim doua echipamente distincte din platformele de procesare.Mecanismul trebuie sa foloseasca tehnologii independente dar integrate cu platformele de procesare si de stocare, asigurand replicarea transparenta si sincrona a continutului de memorie si a continutului de disc asociat unei masini virtuale, respectiv unui set de masini virtuale, fara introducerea de latenta in respectivele platforme sau in functionarea masinilor virtuale; * Platforma trebuie sa includa o componenta de administrare si monitorizare dedicata, disponibila atat la nivelul echipamentelor fizice ce alcatuiesc platformele de procesare, stocare si comunicatie cat si la nivelul masinilor virtuale, ale resurselor virtualizate, aplicatiilor, serviciilor si protocoalelor insumate in infrastructura.In vederea accesului facil la functiile de administrare si monitorizare oferite, platforma trebuie sa permita acces atat prin consola locala/la distanta cat si prin browser web si prin platforma de management dedicata; * Componenta de management si monitorizare a infrastructurii trebuie sa permita autentificarea utilizatorilor bazata pe roluri si privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director.Deasemenea trebuie sa permita crearea facila de politici dinamice de acces la resursele de procesare, precum si de disponibilitate ale acestora; * Separarea privilegiilor administrative trebuie sa se poata face pe orice element disponibil in interfata de administrare (server, utilizator, resursa de procesare, stocare, retea, etc), permitand astfel crearea de zone/domenii de securitate in functie de aplicatii si/sau roluri functionale, nu in functie de elementele disponibile in infrastructura de procesare, stocare si comunicatie; * Platforma de management trebuie sa asigure si mecanisme de definire si aplicare a profilelor standard de configuratie pentru serverele ce fac parte din infrastructura virtuala.Deasemenea sa permita configurarea de politici de aplicare a acestor profile in functie de necesitatile de moment sau in concordanta cu politica stabilita in prealabil; * Componenta de management trebuie sa se integreze nativ sau prin intermediul unor conectori/componente cu platforma de procesare si cu platforma de stocare in vederea realizarii operatiunilor de backup direct din aceste platforme, precum si pentru crearea rapida a unor zone izolate atat din punct de vedere al securitatii cat si al gruparilor de resurse de procesare, stocare si retea, in scopul testarii si dezvoltarii; * Componenta de management trebuie sa integreze nativ functii de monitorizare analitica a integritatii si performantei platformei de virtualizare, functii ce vor permite anticiparea proactiva a problemelor de performanta si disponibilitate.Respectivele mecanisme trebuie sa se bazeze atat pe modele de utilizare predefinite, cat si pe functii integrate de auto-invatare, astfel incat sa se asigure vizibilitate completa asupra problemelor din infrastructura; * Trebuie sa integreze nativ functii de administrare si optimizare a spatiului disponibil in platformele de stocare si a gradului de disponibilitate si ocupare a resurselor virtualizate din plaformele de procesare si comunicatie, astfel incat sa balanseze in permanenta nevoile curente ale masinilor virtuale (atat la nivel individual cat si la nivel global) in raport cu resursele fizice din respectivele platforme, eficientizand utilizarea respectivelor resurse fizice; * Platforma trebuie sa integreze un portal de tip dashboard pentru afisarea si analizarea tuturor informatiilor legate de disponbilitate, grad de ocupare a resurselor, metrici de performanta, istoric al actiunilor administrative si corective, precum si recomandari de optimizare a intregii functionalitati puse la dispozitie de platforma de virtualizare.Portalul trebuie sa permita executarea directa de actiuni corective si administrative asupra elementelor de infrastructura vizate (masini virtuale, resurse de procesare, stocare si comunicatie), actiuni bazate pe recomandarile afisate in portal in urma analizelor efectuate asupra respectivelor elemente; * Datele monitorizate trebuiesc automat analizate si exprimate sub forma de metrici de stare, risc si eficienta, permitand identificarea rapida a potentialelor probleme in infrastructura; * Platforma trebuie sa ofere analize de capacitate si sa identifice explicit resursele ce sunt supra-utilizate, ajutand in procesul de redistribuire a sarcinilor de incarcare intre elementele platformei in scopul eficientizarii rularii aplicatiilor si serviciilor, respectiv sa ofere scenarii predefinite de simulare a incarcarii pentru a elimina procesele deductive de alocare a resurselor platformei; * Platforma trebuie sa ofere analize automate a proceselor de instalare si configurare a mediului virtualizat, in scopul detectarii rapide a eventualelor probleme ce pot aparea datorita configurarilor defectuoase sau a elementelor noi introduse in infrastrcutura; * Trebuie sa integreze functii automate de alertare in cazul depasirii pragurilor optime de functionare, atat pentru starea tuturor elementelor platformei de virtualizare, cat si pentru metrici de performanta si capacitate; |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin prin partenerul autorizat al acestuia; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Componenta de sistem de operare

Componenta de sistem de operare trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Cerinte generale | * Componenta trebuie sa ofere suport pentru cel putin urmatoarele arhitecturi de processor:   + x86,   + x86\_64 * Componenta trebuie sa ofere suport pentru lucrul cu memoria RAM, astfel:   + x86: minim 16 GB   + x86\_64: minim 1 TB   + x86\_64 * Componenta trebuie sa ofere suport pentru lucrul cu cel putin urmatoarele sisteme de fisiere:   + FAT32   + NTFS * Componenta trebuie sa ofere suport pentru lucrul in regim multi-tasking * Componenta trebuie sa ofere suport pentru lucrul cu memoria virtuala (SWAP) * Componenta trebuie sa ofere suport pentru cel putin o tehnologie de virtualizare a resurselor de procesare, stocare si retea * Componenta trebuie sa ofere suport pentru stocarea si replicarea datelor * Componenta trebuie sa ofere suport pentru lucrul cu containere * Componenta trebuie sa ofere suport pentru lucrul cu servere de aplicatie, web si/sau baze de date * Componenta trebuie sa ofere suport pentru controlul accesului si al identitatii, cel putin ACL si OpenLDAP * Componenta trebuie sa ofere suport pentru lucrul la nivel de retea (DNS, DHCP, SDN, VPN, QoS, Firewall, Load Balancing) * Componenta trebuie sa ofere suport pentru accesul de la distanta (Remote Desktop) * Componenta trebuie sa ofere suport pentru securitate sporita (user/password, tokens, Kerberos, TLS- SSL * Componenta trebuie sa ofere support pentru diagnoza * Componenta trebuie sa include o consola grafica de administrare * Componenta trebuie sa include o componenta de executie automatizata a sarcinilor * Componenta trebuie sa ofere suport pentru lucrul cu browsere de internet |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Echipamente de integrare LAN

Echipamentele de integrare LAN trebuie sa respecte fiecare urmatoarele **cerinte functionale specifice**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Complet redundanta bazata pe cel putin 2 module de comunicatie; * Arhitectura de tip „crossbar”, „non-blocking”, capabila sa asigure comunicatii fara pierderi de frame-uri intre oricare doua porturi, la viteza maxima de 10Gbps si 40Gbps, cu o intarziere minima, constanta, care sa nu depinde de lungimea frame-urilor; |
| Cerinte tehnice generale | * Echipamentul va avea caracteristicile unui modul de comunicatie destinat mediului de centru de date, care sa asigure simultan urmatoarele functionalitati: * Switch Ethernet Layer 2; * Switch Ethernet Layer 3; * Interfete fizice disponibile: * Minim 10 Gigabit Ethernet (cu conector SFP+); * Minim 40G Ethernet care sa suporte urmatoarele tipuri de transceivere:   + - 40GBase-SR4;     - 40GBase-LR4;     - 10GBase-SR;     - 10GBase-LR;     - 10GBase-ER; |
| Performante | * Comutarea la nivel 2: minim 1.4 Tbps si minim 1100 Mpps; * Tabela de adrese MAC de minim 96000 de inregistrari; * Minim 4000 de ID-uri pentru VLAN-uri per switch; * Comutare de tip “Cut-Trough” pentru asigurarea unei latente de comutare a pachetelor port-la-port mai mica de 2 microsecunde; * Procesor de control multi-core; |
| Functionalitati Layer 2 | * Incapsulare IEEE 802.1Q; * Rapid Per-VLAN Spanning Tree Plus sau echivalent; * Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minim 64 de instante; * Spanning Tree PortFast, Root Guard si Bridge Assurance; * Virtual Port Channel sau o tehnologie echivalenta care sa permita crearea unui “link-aggregation group” intre doua switch-uri pe de o parte si un alt echipament de tip client (server, switch, router, etc) de partea cealalta; * Link Aggregation Control Protocol (LACP): IEEE 802.3ad; * Posibilitatea balansarii legaturilor din Port Chanel utilizand informatii de nivel 2, 3 si 4; * Suport pentru “Jumbo frames” cu dimensiuni de 9216 bytes pe toate porturile; * Mecanisme de control al inundarii retelei cu trafic unicast, multicast si broadcast; * Private VLAN, inclusiv pe porturile de tip trunk 802.1Q si EtherChannel; * Suport pentru protocolul LLDP (IEEE 802.3ab); * Suport pentru protocoalele: IEEE 802.3ae, IEEE 802.3z, IEEE 802.1q VLAN, IEEE 802.1ad, IEEE 802.1ba, IEEE 802.3an; 802.1Q VLAN Tagging; 802.1p Class-of-Service (CoS) Tagging for Ethernet frames; 802.1x Port-based network access control; * Support pentru protocolul VXLAN si cel putin 256 Virtual Tunnel End-Points (VTEP); |
| Functionalitati Layer 3 | * Suport pentru urmatoarele protocoale Layer 3: * Open Shortest Path First (OSPF) versiunile 2 si 3; * Border Gateway Protocol (BGP); * RIP v2; * Multicast PIM SM, SSM si MSDP; * Cel putin 96000 intrari in tabela de routare; * Posibilitatea de a filtra accesul pe interfete dupa informatii despre adresa IP sursa sau destinatie si in acelasi timp si portul TCP/UDP sursa sau destinatie; * DHCP snooping cu posibilitatea de a adauga Optiunea 82; * Facilitatea de a filtra pe un port/VLAN a raspunsurilor la cererile protocolului ARP; |
| QoS | * Layer 2 IEEE 802.1p (CoS); * Configurare QoS per port; * Minim 4 cozi hardware de servire per port; * Posibilitatea de clasificare a traficului bazata pe liste de control al accesului; * Coada cu prioritate stricta; * Weighted Round-Robin (WRR) si Priority Queuing (PQ) pe cozile de iesire; |
| Management | * Suport pentru SPAN si Encapsulated Routed SPAN; * Suport pentru sflow sau echivalent; * Suport pentru revenirea la o configuratie anterioara; * Suport pentru standardul AAA, Tacacs+ si Radius; * Suport pentru interfata XML (Netconf); * Suport pentru monitorizarea utilizarii bufferelor interne; * Suport pentru protocolul SSHv2 si SCP; |
| Surse de alimentare | * Minim 2 surse de alimentare interne, de tip „hot-swap”, care să asigure alimentarea redundantă în condiţii de încarcare maximă; * Redundanţă de tip „1+1”, cu capabilităţi „load-balancing” şi „failover”; * Plaja de tensiune operabilă: 100-240V AC; * Plaja de frecvenţa suportată: 50– 60 Hz; * Se livrează cu 2 cabluri de alimentare de tip PDU; |
| Sistem de ventilaţie | * Sistem de ventilaţie de tip „hot-swap”, redundant, instalat intern; * Flux de aer de tip “front to back”; * Echipare minimală: 2 ventilatoare, în configuraţie redundantă “1+1”; |
| Cerinte constructive | * Montabil în rack-uri standard de 19”; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software (sistem de operare, firmware, etc). |

* + - 1. Echipament de stocare de Tip 1

In vederea atingerii obiectivelor operationale Solutia trebuie sa includa un sistem de stocare cu arhitectură internă flexibilă, în care nodurile active de control vor fi simultan conectate la toate structurile de tip bus sau loop (SAS loops şi similare), pentru a face posibilă arondarea iniţială şi reconfigurarea ulterioară facilă a alocării discurilor între nodurile de control, între diferitele volume (sau structuri similare), precum şi între servicii diferite (SAN/NAS).

Echipamentul de stocare de Tip 1 trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Platforma unificata de stocare trebuie sa fie echipata cu doua controller-e unificate (SAN/NAS) in acelasi sasiu pentru a putea dispune de o configuratie redundanta de tip cluster activ-activ la nivelul echipamentului; * Controller-ele trebuie sa fie de tip hot-swap; |
| Protocol de acces la date | Platforma de stocare trebuie să ofere acces la datele stocate atat prin protocol de tip block (SAN), prin FC (Fiber Channel) si iSCSI, precum si prin protocol de tip file (NAS), prin NFS (v2/v3/v4) si CIFS (SMB2/SMB3); |
| Memorie | * Platformava include extinderea memoriei cache Read/Write cu discuri intehnologie SSD, cu o capacitate totala minima de 1 TB (configurata redundant cu minim un disc de tip hot-spare), pentru intreaga platforma, indiferent de marimea volumelor de date accelerate, respectiv de tipul de protocol folosit pentru accesul la accesul la volumele de date accelerate (SAN/NAS); |
| Nivele RAID | Configurarea si optimizarea matricilor RAID in configuratii cu unul si doua discuri de paritate asociate fiecarui set de discuri componente al unei matrici RAID, precum si posibilitatea de a folosi aceste matrici RAID in mod de replicare integrala de tip mirror; |
| Conexiuni SAN | * Minim 1024 host-uri per platforma de stocare, prin conexiune intermediara de tip Full Fabric; * Pana la 8 host-uri conectate direct la platforma de stocare; * Minim 512 LUN-uri per platforma de stocare; |
| Dimensiune sistem de fisiere | Minim 256 TB; |
| Dimensiune LUN exportat | Minim 256 TB; |
| Hard discuri | * Trebuie sa permita utilizarea in paralel a discurilor de tip SAS 6/12 Gbps, NL-SAS 3 Gbps, SSD; * Capacitatile pentru un HDD minim disponibile trebuie sa fie de 2 TB pentru discurile NL-SAS, 600 GB pentru cele SAS, 400 GB pentru cele SSD; |
| Extensia capacitatii de stocare | Platforma de stocare trebuie să asigure următoarea capabilitate minimă de extensie a capacităţii de stocare:   * Suport pentru module de expansiune cu discuri de 3,5” respectiv 2,5”; * Modulele de expansiune trebuie sa se conecteze la echipamentul de stocare prin magistrale de date redundante, cu latime de banda de cel putin 48 Gbps (SAS 12 Gbps cu 4 cai de acces). |
| Managementul platformei | * Platforma de stocare trebuie să asigure un sistem de management şi monitorizare integrat; * Platforma de stocare trebuie să aibă capabilitatea de monitorizare şi management a mai multor echipamente din aceeaşi gamă într-o singură instanţă a interfeţei, atât pentru serviciile SAN, cât şi pentru cele NAS; * Platforma de stocare trebuie să asigure provizionarea automată a sistemelor de fişiere; * Platforma de stocare trebuie sa asigure monitorizarea performantei si capacitatii platformei de stocare atat la nivel fizic cat si la nivel virtual. Solutia trebuie sa asigure functionalitatile respective atat pentru platforma propusa cat si pentru alte platforme de la acelasi producator; * Platforma de stocare trebuie sa includa fara costuri aditionale cel putin posibilitatea administrarii prin intermediul unei interfete web securizate SSL si/sau aplicatie dedicata de management, precum si consola de administrare la distanta SSH/Telnet. Toate functiile native ale sistemului de stocare, precum si functionalitatea licentiata separat trebuie sa fie accesibile in mod integrat prin intermediul acestor unelte de administrare, astfel incat operatiunile de configurare si administrare sa poata fi efectuate indiferent de locatie si de modalitatea de acces; * Atat in scop administrativ cat si in vederea accesului la seturile de date, Platforma de stocare trebuie sa permita nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor si a drepturilor de acces la seturile de date partajate de sistem. Pentru sporirea securitatii in mecanismele de autentificare, echipamentul trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp. Mecanismele de export ale volumelor prin intermediul protocolului CIFS trebuie sa beneficieze nativ de suportul integrarii echipamentului de stocare cu sistemele de tip director si cu serverele de timp; * Uneltele de administrare prin interfata web si/sau aplicatie dedicata trebuie sa fie usor de folosit si sa implementeze majoritatea actiunilor administrative (definirea de volume, LUN-uri, exportul seturilor de date indiferent de protocolul folosit pentru export, configurarea functiilor de partajare, optimizare si backup, adaugarea/eliminarea de noduri la/din cluster, definirea relatiilor de replicare, etc) intr-o singura interfata fara a fi nevoie de acces la uneltele in linie de comanda, iar pentru un numar de operatiuni importante de configurare sa puna la dispozitie asistenti de configurare. Uneltele trebuie sa permita atat configurarea si administrarea sistemului curent cat si orice alt sistem existent de la acelasi producator, indiferent de gama si/sau generatie. Deasemenea trebuie sa integreze un panou unificat de afisare a informatiilor legate de performanta (inclusiv gradul de ocupare al procesoarelor, nivel I/O, latenta in functie de protocolul de comunicatie si tipul de export al volumelor, numarul de operatiuni efectuate asupra seturilor de date), informatiilor legate de gradul de ocupare (inclusiv gradul de ocupare per volum de date si tipul de partajare al resurselor), respectiv afisarea informatiilor legate de starea controller-elor, a relatiilor de replicare intre echipamente si a evenimentelor informationale si/sau de alertare survenite in functionarea oricarui element hardware sau functie software; * Tot ca parte a uneltelor standard de administrare, Platforma de stocare trebuie sa includa posibilitatea de integrare nativa cu platforma de procesare generala si platforma de procesare specializata astfel incat sa permita definirea volumelor, LUN-urilor, aplicarea politicilor si mecanismelor integrate de optimizare, backup si recuperare, efectuarea operatiunilor de instantiere rapida a seturilor de date ce apartin de masini, analizarea si corectarea dinamica a parametrilor de export ai seturilor de date catre platformele de procesare, identificarea si modificarea modului de aliniere logica a partitiilor din sistemele de operare, direct din uneltele de management puse la dispozitie de platformele de procesare, fara a folosi un alt set de unelte terte ce nu apartin nici de platforma de stocare, nici de cele de procesare. Astfel se obtine o platforma unitara de management, ce reduce efortul si costul administrativ, indiferent de natura operatiunilor efectuate; * Platforma de stocare trebuie sa permita accelerarea hardware a operatiunilor ce au loc intre platformele de procesare si sistemul de stocare, prin degrevarea unor procese de la nivelul platformelor de procesare si preluarea lor la nivelul echipamentului de stocare. Aceasta functionalitate trebuie sa permita accelerarea mutarii unei masini intre doua volume de date ale platformelor de procesare si accelerarea efectuarii unei copii identice a unei masini; * Platforma de stocare trebuie sa includa suport pentru VAAI, VASA si VVols; * Pentru asigurarea unui nivel optim de disponibilitate operationala, Solutia oferita va permite update si upgrade software si hardware al platformei fara intreruperea serviciilor; * In scopul alocarii eficiente si dinamice a spatiului de stocare in functie de cerintele previzionate sau de moment, Platforma de stocare trebuie sa includa nativ sau prin licentiere ulterioara, un mecanism de integrare directa la nivelul sistemului de operare ce acceseaza platforma de stocare, mecanism ce va permite executarea direct din sistemul de operare a actiunilor administrative ce privesc definirea de volume si LUN-uri, redimensionarea lor fara pierderea datelor stocate, configurarea si optimizarea parametrilor de conectare la aceste volume indiferent de protocolul folosit in exportul lor. Mecanismul trebuie sa fie disponibil cel putin pentru sistemele de operare de tip server pentru care platforma de stocare trebuie sa ofere suport de conectivitate directa: Windows, Linux, VMware vSphere; * Ca parte a functiilor de administrare si diagnosticare Platforma de stocare trebuie sa includa standard un mecanism de alertare pe e-mail, configurabil pentru un set specific de adrese e-mail si/sau catre o platforma de suport disponibila la producatorul sistemului de stocare. Deasemenea trebuie sa permita integrarea in unelte dedicate de management al infrastructurilor prin suport complet pentru protocolul SNMP versiunea 2 si 3 si prin existenta in mod gratuit a descriptorilor si parametrilor platformei astfel incat integrarea sa se faca in mod facil in uneltele de management ce nu au implicit profile definite pentru sistemul specific ofertat. Tot in scopul operatiunilor de management si diagnosticare sistemul trebuie sa integreze un set de led-uri ce afiseaza cel putin starea curenta a echipamentului; |
| Optimizarea capacitatii de stocare | * Platforma de stocare trebuie să aibă capabilitati de tip „Thin Provisioning” (alocarea către nodurile de procesare a unei capacităţi de stocare mai mare decât cea fizic disponibilă); * Platforma de stocare trebuie să asigure rebalansarea datelor pe matricile de discuri în cazul în care sunt adăugate discuri suplimentare; * Platforma de stocare trebuie sa includa un mecanism de instantiere a unui set de date disponibil la nivel de volum si/sau LUN, fara copierea datelor in instante multiple, ci prin folosirea unui singur set de date, dar adresabil de catre aplicatii si utilizatori ca instante complet diferite; * Platforma de stocare trebuie sa permita definirea de volume de date pe matrici ce suporta discuri in tehnologii diferite (SSD + SAS + NL-SAS), organizate in matrici cu nivele de protectie RAID diferite (Ex.: masiv format din matrici de discuri SSD in RAID 1 + discuri SAS in RAID 5 + discuri NL-SAS in RAID 6); * Platforma de stocare trebuie sa ofere nativ, fara licentiere ulterioara optiunea de prioritizare si accelerare a accesului la date in mod automat si transparent pentru aplicatiile si utilizatorii ce folosesc aceste seturi de date. Mecanismele de accelerare si prioritizare trebuie sa beneficieze de suportul hardware al unui set dedicat de discuri de mare viteza (SSD). Pentru economisirea spatiului si a costurilor asociate, sistemul trebuie sa permita instalarea lor in acelasi sertar cu un tip mai lent de discuri de la acelasi producator (SAS, spre exemplu). Pentru obtinerea celor mai buni timpi de acces si raspuns, intregul proces automat de accelerare si prioritizare trebuie realizat nu prin mecansime de copiere/mutare a datelor pe seturi de discuri mai rapide, ci prin stocarea lor temporara la citire si la scriere in suportul hardware al acestor procese (memoria cache sau discurile SSD). Integrarea mecanismelor de accelerare si prioritizare trebuie sa se faca transparent pentru datele stocate si aplicatiile ce acceseaza aceste date, indiferent de momentul la care se decide activarea acestor mecanisme. Deasemenea trebuie sa se integreze nativ cu restul tehnologiilor si proceselor aplicate la nivelul sistemului de stocare, respectiv asupra seturilor de date, fara a impiedica functionarea sau activarea acestora; |
| Protectia si replicarea datelor | * Platforma de stocare trebuie sa aiba incoporate baterii ce asigura protectia controller-elor si a memoriei cache la cadererile de curent prin salvarea automata a datelor din cache pe discuri dedicate flash/SSD, inainte de oprirea echipamentului; * Platforma de stocare trebuie sa includa mecanisme de realizare a copiilor complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp. Spatiul rezervat copiilor de date trebuie sa poata fi configurat pe discuri separate fata de cele unde stau datele de productie. Sistemul trebuie sa permita si realizarea de copii ale oricarei copii de date. Copiile de date complete, sau bazate pe imagini, trebuie sa poata fi accesate atat in mod „citire”, cat si in mod „scriere”. Se va asigura suport pentru minim 255 de copii ale fiecarui volum de date (LUN); * Suport software si hardware inclus pentru realizarea de copii de siguranță a datelor, local și la distanță, folosind o tehnologie de jurnalizare a tuturor operațiunilor de scriere, care să permită restaurarea datelor la orice moment de timp. Copiile de siguranță trebuie să poată fi grupate pe aplicație, pentru a asigura consistența recuperării aplicațiilor interdependente; * Suport software si hardware inclus pentru replicarea sincrona/asincrona a datelor la distanta, intre mai multe echipamente similare. Pentru utilizarea eficientă a canalelor de comunicatie dintre centrele de date, Solutia de replicare trebuie să ofere suport pentru replicare doar a datelor modificate, precum și transmiterea numai a blocurilor de date unice (deduplicare) si comprimate (compresie); * Trebuie sa permita schimbarea tipului de replicare, din sincron in asincron si invers, manual sau automat pe baza anumitor reguli de performanta prestabilite (Ex.: latime de banda disponibila); * Trebuie sa fie capabila sa ofere tipuri de replicare diferite (sincron, asincron), per aplicatie sau grup de aplicatii. * Toate functionalitatile software solicitate mai sus vor fi incluse in configuratia ofertata a echipamentului de stocare, respectiv pentru intreaga capacitate de stocare ofertata, fara costuri aditionale in cazul viitoarelor extensii de capacitate de stocare; |
| Licentiere | * Conectarea prin protocol iSCSI sa fie disponibila in configuratia initiala; * Conectarea prin protocol NFS (v2/v3/v4) sa fie disponibila in configuratia initiala; * Conectarea prin protocol CIFS (SMB2/SMB3) sa fie disponibila in configuratia initiala; * Conectarea prin protocol FC sa fie disponibila in configuratia initiala; * Licenta inclusa de replicare sincronă/asincronă in configuratia initiala; |
| Sisteme de operare suportate | Platforma de stocare trebuie să suporte minim următoarele sisteme de operare:   * Microsoft Windows Server 2012 R2/2016; * Microsoft Hyper-V; * VMware vSphere; * Red Hat Enterprise Linux;   Platforma de stocare trebuie sa includa licentele necesare accesului sistemelor de operare suportate; |
| Alimentare | Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al platformei de stocare (controller, sasiu discuri, etc) trebuie sa ofere alimentare redundanta prin cel putin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma; |
| Ventilatie | Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma; |
| Cerinte constructive | * Platforma de stocare trebuie să fie montabilă în rack-uri standard de 19”; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software (sistem de operare, firmware, etc). |

* + - 1. Echipament de stocare de Tip 2

Platforma de stocare de Tip 2 trebuie sa indeplineasca aceleasi **specificatii tehnice minimale precum echipamentul de stocare de Tip 1.**

* + - 1. Componenta de monitorizare a dezvoltării și exploatării aplicațiilor

Componenta de monitorizare a dezvoltarii si exploatarii aplicatiilor trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Instalare si configurare | * Posibilitatea de deployment local * Posibilitatea de monitorizare atat a infrastructurii locale – fizice si virtuale, cat si a infrastructurii disponibile via cloud * Interfata grafica web unitara dedicata utilizatorilor, pentru management si mentenanta, cu posibilitati de monitorizare via internet browser * Upgrade automatizat, fara necesitati de configurari manuale * Posibilitati de vizualizare automatizata a intregii topologii de retea (fara omiterea vreunei categorii de componente) * Posibilitati de identificare automatizata a:   + tranzactiilor de business   + tuturoror componente in cadrul tranzactiei de business   + sisteme tip back-end standard (baze de date, servicii web, etc.)   + sisteme tip back-end non-standard (via configuratii tip point-and-click) * Abilitatea de definire globalizata a alertelor folosind un motor de reguli integrat (versus definirea individuala per metrica) * Posibilitatea de definire a unui mediu multi-tenant (chiar si in implementarea locala) * Criptare SSL a traficului intre oricare sub-componente din componenta de monitorizare * Profilingul tranzactiilor distribuite sa poata fi realizat fara scriere/modificare de cod * Componenta trebuie sa impacteze cu maxim 3% incarcarea CPU in cazul scenariilor de incarcare masiva * Support pentru cel putin urmatoarele sisteme de baze de date: MS-SQL Server, MySQL, DB2, Oracle, Sybase, PostgreSQL si MongoDB * Posibilitatea de monitorizare a tuturor instantelor de baze de date fara impact asupra performantelor generale la nivel de mediu/sistem * Posibilitate de instalare non-invaziva - fara agenti. |
| Vizibilitate si control | * Suport pentru vizualizare corelata a tranzactiilor de business distribuite intre nivele si servicii * Suport pentru identificarea fiecarei componente in cadrul tranzactiilor,. In scopul identificarii exacte a problemelor de performanta la nivelul intregii configuratii * Suport pentru diagnoza la nivel de cod (vizibilitate in cadrul claselor si metodelor) in cazul tranzactiilor cu penalitati de performanta * Suport pentru monitorizarea mediului Java Virtual Machine (heap, garbage collector, generational spaces, etc.) * Suport pentrui monitorizare a metricelor hardware (utilizare CPU, OS memorie utilizata, disk I/O si network I/O) * Suport pentru ridicarea exceptiilor si detectia erorilor de executie * Sa existe facilitate de a nu se permite oprirea functionalitatii de monitorizare in situatiile de incarcare masiva a sistemului - in scopul reducerii impactului asupra aplicatiilor, tinand cont ca majoritatea problemelor apar in situatiile de incarcare masiva * Componenta trebuie sa permita identificarea:   + tranzactiilor de business incetinite sau stopate fara interventie manuala   + numararea, masurarea si evaluarea fiecari tranzactii   + tranzactiilor fara interventie manuala   + interogarilor SQL lente fara interventie manuala   + identificarea sistemelor back-end sau serviciilor externe fara interventie manuala   + in regim automatizat a situatiilor tip “code deadlocks” * Componenta trebuie sa ofere posibilitatea de access din interfata-utilizator catre zonele cu probleme de performanta prin intermediul alertelor cu hyper-link * Componenta trebuie sa permita trimiterea de email-uri ce contin hyper-link-uri catre zonele cu probleme de performanta * Componenta trebuie sa permita analiza automatizata a datelor aferente tranzactiilor integrale colectate de tip “root-cause analysis”. |
| Capabilitati de flux de lucru, reguli si alerte | * Definire fluxuri de lucru:   + Creare, editare si rulare pentru intregul mediu din cadrul unui singur produs integrat   + Definire ca o serie de activitati cu executie secventiala   + Rularea in parallel a unei secvente de sarcini pe noduri multiple ale unui cluster   + Utilizarea sabloanelor existente pentru sarcini comune (“startup tasks”, “build/ant”, “shell scripts/native tasks”)   + Crearea de sarcini tip custom si parametrizarea lor. * Executie fluxuri de lucru:   + Executia unui flux de lucru process din cadrul unui singur produs integrat   + Posibilitatea de executie a unui flux de lucru printr-un singur click la nivel de utilizator   + Executia automatizata a fluxului ca urmare a evaluarii unei regului si a unor conditii ce trebuiesc indeplinite   + Posibilitatea de programarea a executiei unui flux la o anumita ora pentru evitarea varfurilor de incarcare ale sistemului   + Existenta unui raport detaliat asupra statusului activitatilor/sarcinilor din cadrul fluxurilor ce se executa * Motor de regului si alertare:   + Existenta unei componente tip “wizard” de creare a regulilor in maniera point-and-click   + Posibilitate de includere in analiza de multiple categorii de date (“app performance data”, “machine data” si “customer provided data”)   + Posibilitate de combinare a conditiilor prin folosirea operatorilor logici booleeni AND si OR   + Posibilitate de stopare temporara a motorului de reguli pentru operatiuni curente de mentenanta a infrastructurii sistemului   + Generare alerte si notificari la incalcarea regulilor (email, SMS sau custom)   + Posibilitate de combinare logica a multiple metrici in cadrul unei singure alerte. |
| Platforma analitica | * Modulele aplicatiei si platforma analitica sunt disponibile in cadrul unui interfete-utilizator unitare * Interfata analitica sa fie web-based (fara instalare locala de client software) * Platforma analitica adreseaza intreg spectrul de date colectate la nivelul componentei/solutiei * Deposit (“repository”) scalabil orizontal capabil de colectare si stocare de volume mari de date aferente evenimentelor si metricelor * Fara dependenta de porturi SPAN sau echipamente de mirroring a traficului (network TAPs) * Mecanisme tip drill-down de navigare la nivel de context intre datele de monitorizare si cele analitice * Subcomponenta de creare a interogarilor (“querry buillder”) disponibil in interfata grafica * Adoptie Advanced Query Language * Abilitatea de ajustare a scalei timpului prin mecanisme “click and drag” in cadrul unui tablou de boord (“dashboard charts”) * Clasarea automata (top N) a relevantei fiecarui camp indexat la sectiunea curenta * Posibilitate de configurare a colectarii anumitor date/campuri aferente tranzactiilor * Colectare, stocare si analiza date imediata (“in near real time”) * Includere de biblioteci API dedicate “Input Custom Metrics”, “Analytics Events” si “Search” * Posibilitatea de afisare a rezultatelor in tablouri predefinite sau tablouri definibile custom * Control granular al accesului, bazat pe roluri (RBAC) * Analitici la nivelul tranzactiilor:   + Abilitatea de colectare si stocare a tranzactiilor de business de la nodurile monitorizate   + Abilitatea de filtrare parametrizabila a tranzactiilor utilizand o interfata grafica de definire a interogarilor (“graphical query builder”)   + Identificarea tuturor tranzactiilor la nivel de utilizator intr-o perioada de timp definibila utilizand ca si criteriu de cautare un ID, o adresa email sau alti identificatori unici * Analitici la nivel de fisiere tip “log file”:   + Abilitatea de colectare si stocare a fisierelor log de la nodurile monitorizate   + Posibilitate de logging via TCP   + Posibilitatea de auto-injectare a identificatorului BT pentru fiecare element al fisierului log   + Abilitatea de filtrare a rezultatelor utilizand o componenta de interogare pe baza de text si/sau o interfata grafica de definire a interogarilor (“graphical query builder”)   + Abilitatea de extragere a oricarui camp din fisierul de log in vederea procesarii. |
| Integrare | * Integrare cu componenta de monitorizare a accesului la date * Integrare cu componenta de monitorizare a serviciilor. |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Componenta de monitorizare a accesului la date

Componenta de monitorizare a accesului la date trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Capabilitati generale | * Componenta dedicate de monitorizare a accesului la date si a nivelului de performanta a sistemelor de baze de date implementate local sau disponibile via servicii tip cloud * Componenta trebuie sa o imagine de ansamblu in timp real asupra activitatii curente legata de bazele de date * Componenta ofera suport pentru alertare static si dinamica privind metricile colectate de la bazele de date functionale * Componenta dispune de capabilitati de evidentiere a tendintelor de utilizare si performanta a sistemelor de baze de date pe prioade de timp configurabile * Componenta dispune de capabilitati de monitorizare continua a activitatilor legate de baze de date in medii de productie cu volume mari de date |
| Instalare si configurare | * Componenta ofera suport pentru multiple platforme, precum:   + Sisteme de operare: Microsoft Windows, distributii Linux, Solaris, AIX.   + Sisteme de baze de date relationale/non-relationale: cel putin Microsoft SQL, Oracle Database, MySQL, IBM DB2, Sybase, Mongo DB, Couchbase.   + Clienti: cel putin Internet Explorer, Mozilla Firefox, Chrome, Safari. * Monitorizare a tuturor instantelor de baze de date fara impact asupra performantelor generale la nivel de mediu/sistem * Implementeaza o arhitectura non-invaziva de tip zero-agenti care scuteste beneficiarii de operatiuni de instalare/configurare/mentenanta pe serverele de baze de date * Suport pentru instalare si configurare facila in mediile de productie, atat locale cat si cele cu componente externalizate via cloud * Suport de monitorizare a oricate instante de baze de date, nelimitand astfel un potential beneficiar cu nevoi majore de scalare a mediilor operationale |
| Capabilitati de analiza aprofundata | * Suport pentru istoricizare, prin intermediul monitorizarii si retentiei datelor in proportie de 100% * Include rapoarte de baza privind activitatea bazelor de date, cel putin “Top SQL”, “Top Users” si “Top Programs” * Suport pentru identificarea profilelor/tendintelor de evolutie aferente activitatii bazelor de date in timp * Colectare si stocare a:   + tuturor evenimentelor tip “wait” si corelarea acestora cu procedurile SQL/stocate   + indicatorii de performanta asociati procedurilor SQL/stocate, ce putin “CPU”, “Count” si Reads/Writes   + statistici la nivel de instanta DB, cel putin “table size”, “row count” si indexes”   + indicatorii de performanta asociati serverelor de baze de date, ce putin “CPU”, “Count” si Reads/Writes * Posibilitatea de evidentiere a latentei componentelor procedurilor stocate * Includere de rapoarte de performanta comparate * Colectarea informatiilor aferente “SQL Explain” si “Execution plan” * Colectarea si stocarea datelor privind performanta obiectelor bazei de date precum scheme, tabele si indecsi * Colectarea indicatorilor de performanta asociati bazelor de date si corelarea acestor informatii cu resursele de procesare si stocare ale serverelor |
| Management si monitorizare a bazelor de date | * Evidentierea in timp real a performantei activitatii aferente bazelor de date * Includerea unui tablou de bord tip multi-instanta pentru crearea unei vederi de ansamblu la nielul tuturor instantelor de baze de date * Abilitatea de trimitere de alerte pro-active aferente nivelelor de performanta a bazelor de date * Includerea unui modul complex de raportare (aferente monitorizarii si performantei bazelor de date) atat pentru personal tehnic cat si pentru management * Posibilitate de export date catre aplicatii externe (3rd party). |
| Detectie anomalii si remediere | * Componenta ofera suport pentru evidentierea impactului direct al penalitatilor de performanta ale bazei de date la nivelul intregii aplicatii * Componenta ofera suport pentru vizualizarea dependintelor intre nivelul instantelor bazelor de date si celelalte niveluri (aplicatie, retea, server) * Componenta ofera suport pentru remedierea rapida a sistemelor de baze de date oferind metrice si informatie relevanta de diagnoza * Componenta ofera suport pentru identificarea apelurilor JDBC cu impact direct in performanta generala a aplicatiei/serviciului * Componenta include algoritmi tip self-learning care calculeaza dinamic nivelul de performanta al sistemelor de baze de date si ofera support in detectia anomaliilor * Pentru diagnosticarea problemelor de performanta, componenta dispune de capabilitati tip Drill-Down disponibile intr-o interfata centralizata de analiza * Componenta ofera suport pentru vizibilitate in metricile asociate bazei de date prin mecanisme de drill-down corelate cu contextul transactional de business |
| Integrare | Integrare cu componenta de monitorizare a serviciilor. |
| Garantie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Componenta de monitorizare a serviciilor

Componenta de monitorizare a serviciilor trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Analiza aporofundata a traficului | * Capabilitati de monitorizare in timp real a performantei serviciilor si securitate a retelei bazate pe un motor de tip Machine Learning * Suport pentru analiza aprofundata si corelata a intregului traficului la nivelul retelei, dispunand de capabilitati precum “transaction analysis”, “full-content analysis”, “full-stream reassembley”, “multi-packets”, “deep-packet inspection”, integrare cu NetFlow si incorporare de probe pentru captarea traficului la nivelul retelei. * Suport pentru o raportare care sa ofere o imagine dinamica de ansamblu dpdv securitate cibernetica a internetului * Suport pentru identificarea si categorisirea traficului de date la nivelul retelei in mod automatizat * Suport pentru cel putin 50 de protocoale sic el putin 3500 metrici asociate analizei correlate aferente acestor protocoale * Suport pentru creare/customizarea de metrici, tablouri de bord, decodare la nivel de protocol (UPA) si integrare de date pe baza Open Data Stream * Suport pentru lucrul cu pachete de date pierdute sau fragmentate la nivelul retelei * Suport pentru lucrul cu date la nivelele L2-L7 ale retelei (adrese IP si MAC, utilizatori, URI, fisiere) * Suport pentru analiza tip top-dows si bottom-up dintr-o singura interfata, in regim de flux de lucru * Suport pentru inspectia traficului in timp real, inainte de scrierea pe disk * Suport pentru monitorizarea traficului la nivel de utilizator (Real User Monitoring) * Suport complet pentru decriptarea SSL * Suport pentru minim 1 Gbps capacitate de trafic si analiza a datelor |
| Monitorizare echipamente server | * Suport pentru dignoza corelata a serverelor, pe baza de metrici si mecanisme tip drill-down * Suport pentru monitorizarea serverelor in mod orientat per aplicatie/serviciu * Suport pentru organizarea schemei asociata serverelor pe nivele ierarhice, cel putin data center -> rack - > servers * Suport pentru vizualizarea informatiilor de baza precum CPU, memorie si latime de banda consumata pentru toate serverele monitorizate, in cadrul unui tablou de bord * Suport pentru vizualizarea informatiilor detaliate asociate proceselor ce ruleaza pe servere * Suport pentru vizualizarea informatiilor de tip fire de executie, CPU si memorie consumata de procese * Suport pentru definirea regulilor si politicilor de automatizare a solutionarii problemelor si a penalitatilor de de performanta asociate serverelor/proceselor in executie * Suport pentru integrarea cu sisteme de alertare, cel putin ServiceNow, PagerDuty si JIRA * Suport pentru verificarea disponibilitatii precum si metrice minimale de performanta asociate serviciilor HTTP care nu sunt monitorizate de agentii componentei * Suport pentru alertare privind timpul de raspuns HTTP pe baza unei validari customizabile * Suport pentru monitorizarea echipamentelor tip mainframe sau load balancers * Suport extins pentru monitorizarea containerelor, minim Docker si VMware vSphere * Capabilitati de monitorizare, ce putin “Machine availability”, “CPU usage”, “Disk performance”, “Volume usage”, “Machine load”, “Memory”, “SWAP”, “Processes”, “Network Adapter(s)”, “Dynamic Baselining”, “Synthetic page checker” * Suport pentru monitorizarea a cel putin urmatoarelor platforme tehnologice Linux, UNIX, MS-Windows, VM * Suport pentru istoricizarea datelor de performanta si evolutie in timp * Suport pentru evidentierea imaginii de ansamblu la nivelul intregii arhitecturi corelata cu tranzactiile de business * O singura interfata la nivel de utilizator pentru monitorizarea serverelor si a aplicatiilor ce ruleaza peste acestea * Posibilitati de alertate bezate pe orice metrica * Posibilitati de alertare la devierile de la nivelele standard de performanta. |
| Monitorizare retea | * Suport pentru vizualizarea performantei intregii retele relative la contextual aplicatiei/serviciului * Suport pentru auto-descoperirea/identificarea topologiei retelelor si a inter-dependintelor, incluzand echipamente tip reverse proxy si/sau load balancers * Suport de centralizare/agregare a informatiilor de infrastructura aferente retelei locale si a celor externalizate via servicii de cloud * Suport pentru diagnoza rapida a problemelor retelei si/sau penalitatilor de performanta ale acesteia inainte ca impactul sa afecteze aplicatiile/serviciile * Suport pentru escalarea problemelor catre personalul dedicat (organizat in echipe multiple) * Suport pentru identificarea latentei, congestiei sau micro-burst-urilor de retea * Suport pentru monitorizarea indicatorilor de performanta asociati retelei precum throughput, packet loss, si RT rates * Suport colaborativ pentru echipele de DevOps prin:   + capabilitati de escalare a problemelor asociind informative de diagnoza pe baza careia se pot demara actiuni de remediere   + imbunatatirea practicilor in scrierea de cod ce conduc spre optimizarea performantelor retelei   + diagnoza a problemelor de retea in medii precum highly distributed microservices sau aplicatii SOA |
| Monitorizarea la nivel de utilizator | Capabilitati pentru platforme web:   * suport pentru browsere atat pentru desktop cat si pentru mobil * monitorizare a tuturor cererilor de pagini, AJAX si/sai iFrame * support pentru aplicatii tip single-page * detectie automatizata a erorilor JavaScript * afisare timp de raspuns pe Geo Map * colectare si afisare date Navigation Timing API/ Resource Timing API pentru cererile cu penalitati de performanta * corelarea tranzactiilor web cu trenzactiile din zona de server pentru analiza tip drill-down * oferirea de informatii la nivel de browser (“browser traces”) pentru slaba performanta sau cererileutilizatorilor * oferirea de analitice privind tipul si versiunea browserelor * oferirea de analitice privind tipul sistemului de operare si echipamentul * oferirea de analitice customizabile pentru analiza si diagnoza * oferirea de metrici privind cache-ul pentru fiecare cerere de pagina * evidentierea timpului de raspuns al serverului pentru fiecare cerere de pagina * corelare prin mecanisme drill-down pentru problemele de performanta ale cererilor de pagini cu zona de server in scopul unei diagnoze eficiente * monitorizare la nivel de sesiune (tracking) * abilitatea de generare de cereri de pagina sintetice * includerea unei librarii (SDK) de support a oricarui framework pentru single-page applications * validare a experientei utilizatorilor cu nivelul de performanta al palicatiei * includerea unui modul de raportare in interfata utilizator pentru zona de experienta a utilizatorilor * date utilizator disponibile la nivel de sesiune sau cerere de pagina * posibilitate de grupare de pagini la nivel root   Capabilitati pentru platforme mobile:   * suport pentru aplicatii mobile si browsere pentru platforme mobile * vizualizare a performantei aplicatiilor mobile, a erorilor HTTP sau de retea * vizualizare a performantei API calls din aplicatia mobile in zona de server * support pentru exceptii si intreruperi in monitorizare (track crashes) * oferirea de analytice privind intreruperile (crashes) * monitorizarea utilizatorilor pe baza de breadcrumbs * monitorizarea tranzactiilor de la echipament la zona de server * corelarea tranzactiilor mobile cu zona de server pentru analiza tip drill-down * oferirea de informatii privind utilizarea si performanta bazata pe: * tipul echipamentului * tipul sistemului de operare * versiunea sistemului de operare * includerea unei interfete utilizator centralizate pentru diagnoza problememor de mobil si celor de server. |
| Garantie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente sau prin partener autorizat; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 7 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Componenta de analiză și testare de securitate a aplicațiilor

Componenta de analiză și testare de securitate a aplicațiilor trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Analiză Vulnerabilități | * Solutia trebuie sa permita monitorizarea continua si concurenta a posturii de securitate a aplicatiilor dezvoltate, oferind mecanisme de evaluare continua a riscului cel putin pentru: * Vulnerabilitatile nou descoperite; * Metricile de identificare a modificarilor si imbunatatirilor msaurilor de securitate pentru o perioada de tip definibila; * Detectia si evaluarea automata a schimbarilor de cod efectuate asupra aplicatiilor web; * Solutia trebuie sa permita verificarea si prioritizarea rezultatelor proceselor de analiza a codului pentru elimina rezultatele de tip “false positive”, respectiv pentru a eficientiza procesul de remediere a vulnerabilitatilor, cel putin prin urmatoarele mecanisme: * Vulnerabilitatile trebuie sa poata fi prioritizate in functie de risc, pentru a putea remedia eficient vulnerabilitatile cu grad ridicat de risc; * Notificari si recomandari de actiuni ce pot fi intreprinse pentru a remedia vulnerabilitatile detectate; * Eliminarea automata si/sau manuala a rezultatelor de tip “false positive” pentru a economisi timpul si resursele dedicate procesului de analiza; * Solutia trebuie sa permita urmarirea in timp real si/sau bazata pe istoricul asociat unei periode definibile de timp, a tuturor datelor ce tin de gradul de risc, cel putin prin urmatoarele mecanisme: * Panou de afisare unificat pentru evaluarea expunerii la risc, respectiv progresul de remediere a fiecarei vulnerabilitati identificate si asociate gradului respectiv de risc; * Comparari ale profilului de securitate asociat institutiei raportat la profilele altor institutii/companii similare (in functie de marime, tip de industrie, etc); * Vzibilitate asupra intregului set de aplicatii cu identificarea aplicatiilor cel mai putin securizate, respectiv cele mai securizate; * Solutia trebuie sa permita analiza codului din punct de vedere al posturii de securitate in orice punct al procesului de dezvoltare a aplicatiilor (chiar si pentru cod partial dezvoltat); * Solutia trebuie sa suporte a mare varietate de limbaje de programare: .NET, Java, PHP, ASP, ColdFusion, Perl, etc; * Solutia trebuie sa permita programarea rularii mecanismelor de evaluare si analiza a codului in functie de parametrii de timp si/sau la cerere; * Solutia trebuie sa permita scanarea codului sursa la origine (in locatiile interne institutiei/companiei), respectiv la distanta (in locatiile in care functioneaza – servere de aplicatii, servere de baze de date, etc ce ruleza in alte locatii decat cele interne institutiei/companiei); * Solutia trebuie sa permita mecanisme rapide de scanare a codului sursa; * Solutia trebuie sa permita identificarea rapida a tuturor aplicatiilor/artefactelor de aplicatie in structura completa a serverelor de aplicatii web, atat pentru servere interne cat si pentru servere externe; * Solutia trebuie sa permita prioritizarea aplicatiilor si a proceselor de analiza a vulnerabilitatilor in functie de gradul de risc relevant pentru fiecare departament al instituiei/companiei; * Solutia trebuie sa permita procese personalizabile de testare a codului sursa de aplicatie in urma remedierii vulnerabilitatilor cel putin prin analiza introducerii de date in aplicatie, analiza cererilor de schimbare de stare a aplicatiei, analiza functionalitatilor critice; * Solutia trebuie sa asigure integritatea codului sursa al aplicatiilor analizate prin injectarea de cod benign in locul codului sursa de aplicatie; * Solutia trebuie sa permita remedierea vulnerabilitatilor folosind urmatoarele metode/mecanisme: * Utilizarea unor segmente precise de cod; * Oferirea unui set de librarii si actualizari (patch-uri) gata dezvoltate de producatorul solutiei ofertate pentru un numar cat mai mare de vulnerabilitati; * Testarea/re-testarea nelimitata a aplicatiilor si codului sursa; * Integrarea nativa cu solutiile de protectie a serviciilor de aplicatie (in speta cu solutia de protectie a serviciilor de aplicatie ofertata); |
| Performanțele analizei | * Solutia nu trebuie sa introduca nici un fel de latenta si/sau penalizare de performanta in functionarea aplicatiilor ce sunt analizate din perspectiva vulnerabilitatilor, prin posibilitatea personalizarii extensive a procesului de analiza; |
| Integrare | * Solutia trebuie sa permita integrarea nativa cu uneltele uzuale folosite de dezvoltatori, indiferent de limbajul de programare folosit in dezvoltarea codului sursa: * Integrari native cu medii de dezvoltare uzuale: Eclipse, Xcode, Visual Studio, IntelliJ, etc – Detaliile despre vulnerabilitatile identificate trebuie sa fie disponibile direct din mediul de dezvoltare; * Integrari native cu sistemele uzuale de management al erorilor de cod: Atlassian Jira – Trebuie sa permita deschiderea automata a tichetelor de urmarile a erorilor de cod in urma procesului de detectie a vulnerabilitatilor, respectiv inchiderea tichetelor de urmarile a erorilor de cod in urma procesului de remediere a vulnerabilitatilor; * Integrari native cu sistemele uzuale de tip repository de cod: Git, SVN, Perforce, CVS, TFS, etc – Trebuie sa permita procesele de evaluare si analiza a vulnerabilitatilor direct din aceste repository, fara descarcarea prealabila a codului sursa; * Integrari native cu sistemele uzuale de management al dependintelor: Jenkins, Nuget, Maven, Gradle, etc – Trebuie sa permita rezolvarea automata a dependintelor de cod, pentru a putea fi incluse in procesele de analiza si evaluare a vulnerabilitatilor codului sursa, respectiv trebuie sa permita analiza individuala a fiecarei librarii terte de cod inclus, cel putin din perspectiva licentierii, valabilitatii si versiunii (cu indicarea posibilitatilor si versiunilor de actualizare in vederea reducerii vulnerabilitatilor si gradului de risc asociat); * Integrari native cu sistemele uzuale de management al ciclului de viata al aplicatiilor: Atlassian Jira, Borland StarTeam, HP ALM, HP Quality Center, IBM Rational Team Concert, IBM Rational Requirements Composer, Microsoft Team Foundation Server, ThoughtWorks Mingle, Rally, VersionOne, Bugzilla, Serena Business Manager, ServiceNow , etc – Trebuie sa permita integrarea bi-directionalaa artfactelor de securitate (vulnerabilitati detectate, status remediere, grad de risc, etc) oferite de solutia propusa; * Integrarile native cu sistemele enumerate trebuie sa se realizeze pe baza standardelor deschise (Open API), astfel incat solutia ofertata sa permita extinderea ulterioara cu sisteme ce suporta respectivele standarde, fara a impune limitari de licentiere si functionalitate; * Solutia trebuie sa fie compatibila si sa permita integrarea nativa in procesele de certificare PCI DSS la nivelul proceselor de analiza si evaluare a vulnerabilitatilor, respectiv la nivelul provceselor de remediere si raportare; |
| Identificarea vulnerabilităților din surse multiple | * Solutia trebuie sa asigure actualizarea semnăturilor și informațiilor despre vulnerabilități în mod automat; * Solutia trebuie sa permita introducerea manuală a definițiilor inclusiv a celor definite de administratori; |
| Administrare sistem | * Solutia trebuie sa asigure crearea rolurilor de administrare și a drepturilor aferente acestora pentru setarea politicilor de scanare și controlul priorităților; * Solutia trebuie sa includă politici de analiză și scanare asociabile unor grupuri de active, pentru a realiza analiză de context; * Solutia trebuie sa permită rularea scanărilor în mod manual sau automat inclusiv configurarea și definirea unor intervale de scanare a activelor sau a grupurilor de active; * Solutia trebuie sa asigure administrarea prin intermediul unei interfețe web care permite modificarea informațiilor afișate în funcție de necesități. Accesul la interfața grafică se va realiza în mod securizat, prin protocol SSL; |
| Clasificarea activelor | * Solutia trebuie sa asigure definirea unei structuri ierarhice de grupuri de active; * Solutia trebuie sa permita realizarea de clasificări pe diverse criterii (de exemplu criteriul organizațional, topologic, geografic sau la nivel de sistem); |
| Raportare | * Solutia trebuie sa furnizeze rapoarte per activ sau grup de active pentru următoarele nivele ierarhice: * Rapoarte pentru managementul de top; * Rapoarte pentru managementul secundar; * Rapoarte pentru tehnicieni; * Solutia trebuie sa asigure capabilități de notificare prin e-mail; * Solutia trebuie sa asigure emiterea rapoartelor în mod programat sau rularea ad-hoc a acestora; * Solutia trebuie sa asigure furnizarea de rapoarte de remediere; * Solutia trebuie sa asigure emiterea de rapoarte privitoare la tendințele de schimbare privind managementul vulnerabilităților; * Solutia trebuie sa asigure stabilirea unei linii de bază și urmărirea evoluției în timp a vulnerabilităților existente (emiterea de rapoarte ce evidențiază diferențele identificate între sesiuni de scanare separate în timp); * Solutia trebuie sa furnizeze informații suplimentare despre vulnerabilitățile identificate: descriere, criticitate, risc, identificator specific producătorului, metode pentru remediere (inclusiv patch-uri software, configurări de administrare sau căi alternative destinate acoperirii vulnerabilităților detectate); * Solutia trebuie sa dispună de șabloane de raportare predefinite și de posibilitatea de creare a altor șabloane personalizate; * Rapoartele să poată fi exportate cel puțin în format PDF și CSV; * Gruparea si repartizarea automata/definibila a rapoartelor in functie de tipul raportului, domeniului de interes, departamentului, gradului de risc, tipului de aplicatie, etc; * Capabilitati avansate de raportare cu posibilitatea urmaririi continue a tendintelor si parametrilor cheie (rate de remediere, timpul de rezolvare a vulnerabilitatilor, timpul de viata al vulnerabilitatilor, etc); * Generarea unor indecsi de securitate pentru fiecare tip de aplicatie analizata; * Generarea unor liste de atacuri posibile relativ la fiecare vulnerabilitate descoperita; |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software. |

* + - 1. Componenta de analiză și remediere a vulnerabilităților de securitate

Se va livra o componenta de analiză și remediere a vulnerabilităților de securitate, cu modul de identificare automată și catalogare a tuturor activelor autorității contractante, plus toate licențele aferente, ce va indeplini urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Analiză Vulnerabilități | * Solutia trebuie sa permită instalarea motorului de scanare cel puțin pe următoarele sisteme de operare: * Microsoft Windows Server 2012 R2/2016; * RedHat Enterprise Linux 6/7; * Trebuie sa ruleze fără a necesita instalarea unui agent pe activele existente în rețea (agentless); * Trebuie sa permită rularea de fișiere de comenzi (script-uri și API-uri) personalizate fără actualizarea codului aplicației; * Trebuie sa asigure emularea atacurilor informatice: capacitatea de a efectua teste de penetrare într-o manieră neinvazivă sau invazivă, în scopul analizei efectelor unor atacuri reale. Se va asigura integrarea cu o soluție de exploatare a vulnerabilităților care va fi inclusă în soluția pentru managementul vulnerabilitaților ofertată; * Trebuie sa asigure automatizarea procesului de identificare, prioritizare, analiză și indicații pentru remedierea vulnerabilităților, prin validarea acestora cu soluția de exploatare a vulnerabilităților ofertată; * Trebuie sa asigure rularea de scanări pentru identificarea vulnerabilităților rețelei și ale sistemelor existente (Active discovery scan); * Trebuie sa asigure prioritizarea scanărilor și a analizei în funcție de criticitatea activelor identificate în rețea; * Trebuie sa asigure scanarea sistemelor ce dețin adrese IPv4 și IPv6; * Trebuie sa fie validată și aprobată PCI Council Approved Scanning Vendor (ASV); |
| Performanțele analizei | * Soluția trebuie să asigure scanarea unui număr nelimitat de segmente de rețea diferite; * Soluția trebuie să asigure scanarea unui număr nelimitat de IP-uri diferite; * Soluția trebuie să suporte un număr nelimitat de motoare de scanare; |
| Identificarea vulnerabilităților din surse multiple | * Solutia trebuie sa asigure actualizarea semnăturilor și informațiilor despre vulnerabilități în mod automat; * Solutia trebuie sa asigure importul de definiții Microsoft Group Policy; * Solutia trebuie sa asigure capacitatea de a integra vulnerabilități indicate de sistemele IPS; * Solutia trebuie sa permita introducerea manuală a definițiilor inclusiv a celor definite de administratori; |
| Administrare sistem | * Solutia trebuie sa asigure crearea rolurilor de administrare și a drepturilor aferente acestora pentru setarea politicilor de scanare și controlul priorităților; * Solutia trebuie sa includă politici de analiză și scanare asociabile unor grupuri de active, pentru a realiza analiză de context; * Solutia trebuie sa permită rularea scanărilor în mod manual sau automat inclusiv configurarea și definirea unor intervale de scanare a activelor sau a grupurilor de active; * Solutia trebuie sa asigure administrarea prin intermediul unei interfețe web care permite modificarea informațiilor afișate în funcție de necesități. Accesul la interfața grafică se va realiza în mod securizat, prin protocol SSL; |
| Identificarea și urmărirea activelor | * Solutia trebuie sa scaneze și să identifice cel puțin: * Software de bază pentru echipamente de rețea (routere, switch-uri); * Sisteme de operare pentru desktop-uri și servere (cel puțin Microsoft Windows XP, 7, 8.x, 10, Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, Red Hat Enterprise Linux, Oracle Linux și Solaris); * Echipamente de tip IDS/IPS; * Echipamente de tip firewall; * Aplicații de tip baze de date (cel puțin Microsoft SQL Server 2005, 2008, 2012, MySQL, Oracle, IBM DB2 și PostgreSQL); * Servere și servicii web, cel puțin Microsoft IIS și Apache; * Funcționalitatea trebuie să fie disponibilă pentru utilizare fără o configurare specială (out of the box); |
| Tehnici de identificare a activelor | Soluția trebuie să suporte cel puțin următoarele tehnici de identificare a activelor:   * Ping sweep; * UDP probe; * Asset fingerprinting; * Rapid discovery; * NetBIOS-based discovery; * TCP discovery; * UDP port discovery; * OS fingerprinting; * Application fingerprinting; * Integrated NMAP database; |
| Clasificarea activelor | * Solutia trebuie sa asigure definirea unei structuri ierarhice de grupuri de active; * Solutia trebuie sa asigure importul din Active Directory; * Solutia trebuie sa permita realizarea de clasificări pe diverse criterii (de exemplu criteriul organizațional, topologic, geografic sau la nivel de sistem); |
| Raportare | * Solutia trebuie sa furnizeze rapoarte per activ sau grup de active pentru următoarele nivele ierarhice: * Rapoarte pentru managementul de top; * Rapoarte pentru managementul secundar; * Rapoarte pentru tehnicieni; * Solutia trebuie sa asigure capabilități de notificare prin e-mail; * Solutia trebuie sa asigure emiterea rapoartelor în mod programat sau rularea ad-hoc a acestora; * Solutia trebuie sa asigure furnizarea de rapoarte de remediere; * Solutia trebuie sa asigure emiterea de rapoarte privitoare la tendințele de schimbare privind managementul vulnerabilităților; * Solutia trebuie sa asigure stabilirea unei linii de bază și urmărirea evoluției în timp a vulnerabilităților existente (emiterea de rapoarte ce evidențiază diferențele identificate între sesiuni de scanare separate în timp); * Solutia trebuie sa furnizeze informații suplimentare despre vulnerabilitățile identificate: descriere, criticitate, risc, identificator specific producătorului, metode pentru remediere (inclusiv patch-uri software, configurări de administrare sau căi alternative destinate acoperirii vulnerabilităților detectate); * Solutia trebuie sa dispună de șabloane de raportare predefinite și de posibilitatea de creare a altor șabloane personalizate; * Rapoartele să poată fi exportate cel puțin în format PDF și CSV; |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software. |

* + - 1. Componenta de analiză a accesării și utilizării resurselor

Componenta de analiza a accesarii si utilizarii resurselor trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Capabilitati tehnice | Soluția permite valorificare inteligentă a datelor martor de audit generate la nivel de sesiune utilizator:   * Indexarea textului care apare pe ecran, inclusiv la nivelul imaginilor, în sesiuni de tip remote desktop sau în aplicații Java; * Capabilități de căutare, inclusiv identificarea utilizatorilor care au văzut pe ecran un anume text, respectiv redarea înregistrării sesiunilor de lucru la nivel de desktop în care acesta a apărut; * Posibilitatea de a căuta prin identificarea exactă a textului, ca atare, sau prin utilizarea de simboluri și formule specializate, inclusiv de tip wildcard, și expresii regulate * Posibilitatea de a formula reguli care determină o anumită acțiune, în funcție de textul care apare pe ecran, inclusiv în ceea ce privește mascarea parțială a textului în înregistrări, sau, după caz, oprirea unei aplicații și blocarea accesului utilizatorului la aceasta, respectiv cu, sau fără, notificarea utilizatorului.   Soluția permite monitorizarea activității în timp real, cu posibilitatea înregistrării și a redării filmului acesteia:   * Streaming în timp real al filmului activității utilizatorului vizat, la nivel de post de lucru; * Accesul, exclusiv pentru administratori specific autorizați la redarea înregistrării, pe diverse platforme, inclusiv de tipul terminalelor mobile inteligente; * Posibilitatea de exportare / descărcare a înregistrărilor, într-un format standadardizat; * Posibilitatea de căutare, pe baza informației martor de audit (loguri), și de regăsire rapidă a înregistrărilor de interes.   Soluția asigură posibilitatea de a identifica și, respectiv, de a permite sau de a bloca activități la nivel de utilizator.  Protectia caracterului privat al situației și, respectiv, al informației va fi asigurată prin:   * Utilizarea de profile de monitorizare pentru configurarea parametrilor aplicabili; * Activarea și/sau dezactivarea monitorizării în funcție de o multitudine de criterii, inclusiv in funcție de aplicație sau website, precum și pe bază de program orar.   Posibilitatea de a identifica și de urmări, la nivel de post de lucru și de utilizator va include:   * Mesajele email primite sau trimise; * Conectarea locală de medii de stocare amovibile; * Transferul de local fișiere; * Aplicațiile care rulează; * Utilizarea tastaturii; * Paginile de Internet vizitate; * Căutările pe Internet; * Documentele imprimate.   Soluția va asigura posibilitatea de acces interactiv și de preluare efectivă a controlului, în situații asimilate incidentelor de securitate, exclusiv pentru administratori specific autorizați;  Soluția va asigura posibilitatea de definire a unor acțiuni (și secvențe de acțiuni) specifice pentru situații specificate, inclusiv:   * Blocarea încercării de trimitere a unui mesaj de email către o destinație neautorizată; * Blocarea imdediată a accesului la stația de lucru în cazul copierii neautorizate a unui fișier pe un suport de stocare amovibil; * Limitarea duratei zilnice de utilizare a unei aplicații specificate, cu posibilitatea de blocare ulterioară a accesului la aceasta; * Blocarea accesului de la distanță al utilizatorilor externi în afara programului de lucru specificat; * Blocarea lansării neautorizate de către utilizatori a unor programe fără legătură cu rolul acestora.   Soluția va asigura analiza de risc și orchestrarea reacției specifice asociate setului activ de reguli și politici de utilizare a resurselor la nivel de post de lucru, inclusiv:   * Identificarea posturii generale de securitate, la nivel de organizație; * Definirea de reguli care să poată fie bloca proactiv o mare varietate de acțiuni nedorite, cu sau fără notificarea administratorilor, fie notifica proactiv și îndruma utilizatorul; * Blocarea acțiunilor nedorite va putea fi însoțită de blocarea accesului utilizatorului la stație; * Operarea cu niveluri de risc pre-definite în raport de care pot fi definite și regrupate politicile de securitate; * Operarea cu scoruri de risc, rezultate din analiza, care pot fi asociate la nivel de utilizator sau de departament.   Mecanismele de monitorizare, inclusiv înregistrare, și cele de aplicare a politicilor de securitate vor fi continua să fie active și în cazul pierderii temporare a conectivității de rețea:   * În acest caz, regulile vor ține seama de profilul aplicat la cea mai recentă conectare la server; * După reconectare, datele colectate vor fi sincronizate automat, în mod transparent și controlat, cu serverul.   Soluția va include instrumente de analiza a productivității, relativ la accesul utilizatorilor la resurse și la utilizarea efectivă a acestora;  Solția va dispune de mecanisme interne de alertare automată, în timp real, și de raportare.  Arhitectura soluției constă în agenți instalați la nivelul instanțelor de sisteme de operare de post de lucru suportate, coordonați și controlați de cel puțin o instanță virtualizată de tip server.  Platformele suportate pentru componenta de tip agent vor include cel puțin Windows 7/8/10 (32-bit / 64-bit), Windows Server 2008 /2008 R2 /2012 /2012 R2.  Instalarea agenților se va purtea face atât în mod manual, pe bază de pachete de tip .msi, cât și în mod programatic, inclusiv la nivel de Group Policy, local sau de la distanță și cu opțiune de instalare automată, transparentă, fără notificarea și fără intervenția utilizatorului.  Comunicarea între agenți si instanțele de tip server vor presupune lărgime de bandă redusă la nivel LAN (de ordinul a 10kbs). |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; * Garantia va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day); * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Componenta de redistributie a accesului la serviciile de aplicatie

Platforma de redistributie a accesului la serviciile de aplicatietrebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Platforma va suporta implementarea in oricare din urmatoarele scenarii: Active-Standby, Active-Active si configuratii N+1; * Solutia va permite sincronizarea configuratiilor, starea conexiunilor si persistenta pentru asigurarea disponibilitatii aplicatiilor in caz de failover; |
| Redistributie a accesului la serviciile de aplicatie | * Platforma va oferi suport IPv4, IPv6, topologii NAT64, IP anycast; * Platforma va furniza raspunsuri de autoritate DNS (server autoritar DNS/server secundar DNS) indreptand traficul catre adresele IP corecte; * Platforma va obtine informatiile despre starea obiectelor si metrica in mod automat din ADC; * Platforma va oferi posibilitatea deservirii raspunsurilor pentru obiectele configurate din memoria cache de mare viteza; * Platforma va include functionalitatea de authoritative slave DNS server si va raspunde si la cereri pentru hostname-uri nebalansate; * Platforma va oferi posibilitatea validarii cererilor de la clienti pe baza de RFC; * Platforma va suporta DNS SEC si pentru raspunsuri la hostname-uri balansate; * Platforma va oferi suport de SSL offloading si DNSSEC in hardware; * Platforma va include o baza de date de geolocatie in scopul directarii utilizatorilor catre cel mai apropiat data center; * Platforma va permite colectarea/constructia unei baze de date de geolocatie pentru adrese IP private; * Platforma va permite balansarea pe baza urmatoarelor metrici: * Round Trip Time; * Hops; * Topology; * Completion Rate; * Packet Rate; * Virtual Server Capacity; * Bits/second; * Link Capacity |
| Disponibilitate | * Solutia va suporta mirroring pentru conexiunile non-SSL in configuratie Active-Standby; * Solutia va permite backup si restore pentru fisierul de configurare din interfata grafica; * Solutia va permite failover intre modulele sau echipamentele corespondente configurate, in functie de: defectiuni hardware, defectiuni de sistem, nefunctionarea acceleratorilor SSL, nefunctionarea retelei, nefunctionarea gateway-ului; * Solutia va suporta implementarea intr-un mediu / topologie cu o singura sub-retea (subnet); |
| Management | * Platforma va permite primirea de mesaje SOAP/XML de la instrumente externe pentru modificarea configuratiei controller-elor de aplicatii; * Solutia permite management-ul prin interfata seriala, CLI (cu SSH) si https GUI; * Platforma va permite colectarea de informatii statistice si istorice despre utilizarea memoriei, procesorului, conexiuni si trafic si afisarea acestora in grafice disponibile in interfata grafica. Unitatile de timp minim disponibile vor fi: per ora, zi, saptamana sau luna; * Solutia va permite generarea si afisarea unei harti a retelei pentru adresele IP si pool-urile serverelor virtuale; * Solutia va suporta generarea unei tabele de rutare ierarhizata compusa din diferite segmente (tip "parent" "child") pentru spatiile de IP-uri izolate sau suprapuse; * Platforma / Solutia va permite alocarea dinamica si controlabila a resurselor tip CPU si memorie RAM (ex. dedicat, functionare nominala, functionare minima); * Solutia va putea trimite alerte despre diverse erori prin SNMP, syslog, e-mail; * Solutia va permite definirea de multiple domenii de administrare; * Solutia va permite resetarea la configuratiile initiale ("din fabrica"); |
| Alimentare | Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al platforma de protectie a serviciilor de aplicatie trebuie sa ofere alimentare redundanta prin cel putin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma; |
| Ventilatie | Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma; |
| Cerinte constructive | * Platforma de protectie a serviciilor de aplicatie trebuie să fie montabilă în rack-uri standard de 19”; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Componenta de protecție a serviciilor de aplicație

Platforma de protectie a serviciilor de aplicatie trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Platforma va suporta implementarea in oricare din urmatoarele scenarii: Active-Standby, Active-Active si configuratii N+1; * Solutia va permite sincronizarea configuratiilor, starea conexiunilor si persistenta pentru asigurarea disponibilitatii aplicatiilor in caz de failover; |
| Optimizare si balansare/rebalansare | * Platforma de protectie a serviciilor de aplicatie trebuie sa poata functiona in mod full proxy, respectiv in mod reverse proxy; * Capacitate de a procesa trafic TCP si UDP generat de diferite aplicatii; * Multipli algoritmi sau metode de balansare a traficului: round-robin, ratio si priority (cu un numar minim de membri activi); * Multipli algoritmi sau metode dinamice de balansare a traficului: fastest-response, least-connections, combinatia fastest-response least-connections, precum si bazate pe resursele serverelor de aplicatii (ex: utilizare CPU, incarcarea memorie, gradul de incarcare al retelei etc); * Capacitatea de trimite cereri gradual catre serverele de aplicatii nou adaugate; * Capacitatea de redirectare a traficului pentru diferite tipuri de (ex: http to https); * Monitorizarea aplicatiilor “content based”, cum ar fi: HTTP/HTTPS, FTP (passiv/activ), POP3, IMAP, SIP, SMTP, telnet, RADIUS, LDAP (cu TLS sau peste canal SSL), SASP, Oracle, MSSQL, SNMP DCA, WMI, RPC si SOAP; * Capabil sa proceseze cereri bazat pe IP sursa/destinatie, SSL, hash persistence; * Capabil sa utilizeze diferite metode pentru “cookie persistence”: pasiv, insert, rewrite; * Capabil sa utilizeze metode de persistenta a sesiunilor in functie de orice variabila din header-ul pachetelor TCP/UDP sau din payload; * NAT (network address translation) si NAPT (network address port translation) bazat pe IP sursa si/sau IP destinatie; * Capabilitate de a returna pachete bazata pe adresa MAC a ultimului hop (asigurarea routarii asimetrice); * Capacitatea de a decide directionarea traficului in functie de URI, method, HTTP host,version, cookie, tipul borowser-ului folosit de client, etc; * Capacitate de a genera reguli noi pentru managementul traficului in functie de anumite evenimente, folosind un limbaj de scripting; * Capacitate de a controla fluxul de trafic bazat pe continutul acestuia, in mod bi-directional; * Capabil de a folosi o combinatie mixta de adrese virtuale si noduri IPv4 si IPv6; * Capabil sa translateze trafic IPv6-IPv4 si IPv4-IPv6; * Capabil de insertie XFF in header-e HTTP, cu IP-ul de origine al clientului; * Redirectare URL catre mai multe servere virtuale in functie de HTTP response code sau URL pattern; * Capacitatea de a returna o pagine de eroare in cazul in care resursele/serverele de aplicatii nu sunt disponibile. Pagina de eroare si mesajul trebuie sa poata fi customizate si sa poata contine grafica; * Capabilitatea de a folosi “chunked transfer encoding” pentru mentinerea persistentei sesiunilor; * Capabilitatea de a agrega si refolosi multiple sesiuni client intr-o singura sesiune server-side; * Capabilitatea de a transforma sesiuni HTTP 1.0 in sesiuni HTTP 1.1 pentru consolidare sesiunilor server-side; * Capabilitate built-in de compresie HTTP pentru reducerea traficului; * Capabilitate built-in pentru accelerare si caching HTTP; * Capabilitate built-in pentru optimizare simetrica de date, compresie, criptare si tunneling; * Capabilitate de criptare AES SSL; * Capabilitate pentru caching multi-store pentru continut dinamic si static (RFC2616); * Capabilitati pentru optimizarea traficului LAN/WAN conform: RFC2582 (optimizare Reno asimetrica), RFC1323 (extensii TCP pentru retele de mare viteza), RFC3042, RFC2018, RFC3168; |
| Procesare SSL/TLS | * Platforma va suporta terminarea de trafic SSL/TLS; * Platforma va dispune de acceleratori SSL pentru SSL offloading; * Platforma va putea comunica prin SSL/TLS cu un server de aplicatii backend; * Platforma va suporta ajustarea parametrilor SSL precum metoda de criptare utilizata, versiunea; * Platforma va suporta SSLv3 si TLSv1; * Platforma va suporta certificate wildcard; |
| Protectie a serviciilor de aplicatie Web | * Capabilitate de inspectie a cererilor/raspunsurilor HTTP; * Capabilitatea de blocare a codurilor de eroare generate de anumite servere de aplicatii; * Capabilitatea de a bloca atacuri tip DoS prin connection proxy; * Abilitatea de a folosi ambele modele de securitate: pozitiva si negativa * Capabilitate de filtrare a pachetelor OSI L3-L7; * Capabilitatea de a ascunde informatiile despre serverele de aplicatii si mesajele generate de acestea (“Resource cloaking” ); * Capabilitatea de a detecta si bloca anomaliile de protocol TCP/UDP, pentru protectie DoS; * Solutia trebuie sa aiba capacitatea de a construi in mod automat politici de securitate; * Solutia trebuie sa aiba capacitatea de a accepta prin interventie manuala fals-positives; * Solutia trebuie sa poate defini politici diferite de securitate pentru diverse aplicatii; * Capabilitate de definire a politicilor de blocare pentru atacuri tip DoS; * Capabilitate de combinare a mecanismelor detectie si prevenire; * Mecanism de roll-back a politicilor de securitate; * Mecanism de versionare a politicilor de securitate; * Mecanism de construire a politicilor de securitate real-time, cu functie de auto-invatare; * Politici predefinite pentru diferite aplicatii (ex: MS SharePoint, Oracle Application 10g etc); * Capabilitate de monitorizare a aplicatiilor protejate pentru prevenirea, detectarea si raportarea anomaliilor de trafic precum si pentru protectia impotriva atacurilor L7 DoS; * Solutia va suporta urmatoarele metode / tehnici de detectie: * Decodare URL; * Null byte string termination; * Self-referencing paths (ex. utilizarea /./ si echivalente codate); * path back-references (ex. utilizarea /../ si echivalente codate); * Combinatii de litere mari si mici; * Utilizarea excesiva de spatii libere; * Eliminarea comentariilor (ex. transformarea DELETE/\*\*/FROM in DELETE FROM); * Conversia caracterelor backslash in forward slash (suportat in windows); * Conversia codarii unicod specifica IIS (%uXXYY); * Decodarea entitatilor HTML (ex. &#99;, &quot;, &#xAAA); * Caractere speciale (ex. \t, \001, \xAA, \UAABB); * Suport pentru modelul de securitate pozitiva - "permite tot traficul cunoscut" si blocheaza tot traficul necunoscut; * Traseu/conexiune specifica per aplicatie; * Motor integrat de detectie pentru tentativele de evitare a inspectiei; * Operarea intr-o arhitectura full Proxy si control inline complet asupra traficului prin echipament; * Detectie bazata pe semnaturi; * Platforma de protectie a serviciilor de aplicatie ajuta la implementarea unui model de securitate pozitiva. Acest model trebuie sa poata fi configurat atat manual cat si automat fara utilizarea de instrumente aditionale / externe (bazat pe traficul de productie si fara impact asupra acestuia); * Solutia trebuie sa suporte gruparea semnaturilor; * Solutia trebuie sa suporte cel putin urmatoarele categorii de semnaturi: * Baze de date: Microsoft SQL, ORACLE, MySQL, PostgreSQL, Sybase, MariaDB; * Sisteme de operare: Windows, Linux, UNIX; * Limbaje si contexte de aplicatie: .NET, PHP, Java; * Servere web: Apache, Microsoft IIS; * Generarea manuala sau automata a politicilor de securitate pozitiva trebuie sa includa minim urmatoarele: * Metode HTTP; * URNs; * Header-e; * Parametri permisi pentru un URN specific; * Seturi de caractere speciale pentru fiecare valoare de parametru; * Semnaturi pentru valori specifice de parametru; * Solutia trebuie sa permita dezvoltarea politicii de securitate fara script-uri aditionale; * Solutia trebuie sa permita generarea automata a politicii de securitate; * Solutia trebuie sa recunoasca host-urile/entitatile (IP-urile) de incredere (trusted). Cererile acestora trebuiesc tratate corespunzator; * Solutia trebuie sa permita asimilarea structurii unei aplicatii (URN, parametri, tipuri de parametri, semnaturi si caractere speciale per parametru) fara interventia operatorului uman; * Solutia trebuie sa suporte detectia parametrilor ascunsi/dinamici; * Utilizatorii vor putea inspecta politica de securitate (audit si raportare); * Solutia va putea proteja obiectele / paginile cu continut nou fara a fi nevoie de a crea politica de securitate de la zero; * Solutia va permite relaxarea sau inasprirea (adaptarea) ulterioara a politicii de securitate generata automat; * Interactiunea cu instrumente third party de evaluare a vulnerabilitatilor; * Va fi posibila constructia politicii de securitate pe baza de instrumente third party de evaluare a vulnerabilitatilor - spre exemplu prin import); * Platforma de protectie a serviciilor de aplicatie va fi pre-integrata cu producatorii de top: Qualys, IBM etc; * Managementul configuratiei; * Platforma de protectie a serviciilor de aplicatie va permite definirea de roluri pentru utilizatori si va solicita autentificare; * Platforma de protectie a serviciilor de aplicatie va permite inlocuirea / customizarea paginilor cu mesaje de eroare sau de blocare; * Platforma de protectie a serviciilor de aplicatie va permite definirea de pagini HTML, AJAX si JSON cu mesaje de blocare; * Platforma de protectie a serviciilor de aplicatie va permite actualizarea manuala sau automata a semnaturilor (mentinute si publicate de furnizori); |
| Disponibilitate | * Solutia va suporta mirroring pentru conexiunile non-SSL in configuratie Active-Standby; * Solutia va permite backup si restore pentru fisierul de configurare din interfata grafica; * Solutia va permite failover intre echipamentele corespondente configurate, in functie de: defectiuni hardware, defectiuni de sistem, nefunctionarea acceleratorilor SSL, nefunctionarea retelei, nefunctionarea gateway-ului; * Solutia va suporta implementarea intr-un mediu / topologie cu o singura sub-retea (subnet); |
| Management | * Platforma va permite primirea de mesaje SOAP/XML de la instrumente externe pentru modificarea configuratiei controller-elor de aplicatii; * Solutia permite management-ul prin interfata seriala, CLI (cu SSH) si https GUI; * Platforma va permite colectarea de informatii statistice si istorice despre utilizarea memoriei, procesorului, conexiuni si trafic si afisarea acestora in grafice disponibile in interfata grafica. Unitatile de timp minim disponibile vor fi: per ora, zi, saptamana sau luna; * Solutia va permite generarea si afisarea unei harti a retelei pentru adresele IP si pool-urile serverelor virtuale; * Solutia va suporta generarea unei tabele de rutare ierarhizata compusa din diferite segmente (tip "parent" "child") pentru spatiile de IP-uri izolate sau suprapuse; * Platforma / Solutia va permite alocarea dinamica si controlabila a resurselor tip CPU si memorie RAM (ex. dedicat, functionare nominala, functionare minima); * Solutia va dispune de template-uri de configurare generice customizabile in functie de nevoile specifice; * Solutia va putea trimite alerte despre diverse erori prin SNMP, syslog, e-mail; * Solutia va permite definirea de multiple domenii de administrare; * Solutia va permite resetarea la configuratiile initiale ("din fabrica"); |
| Alimentare | Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al platforma de protectie a serviciilor de aplicatie trebuie sa ofere alimentare redundanta prin cel putin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma; |
| Ventilatie | Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma; |
| Cerinte constructive | * Platforma de protectie a serviciilor de aplicatie trebuie să fie montabilă în rack-uri standard de 19”; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Componenta centrală de protecție avansată antimalware

Componenta centrală de protecție avansată antimalware trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Platforma hardware dedicata de detectie, analiza si protectie impotriva amenintarilor avansate, ce monitorizeaza traficul pe toate porturile pentru mai mult de 100 de protocoale de retea si aplicatii; * Platforma va asigura acoperire si vizibilitate completa in toate punctele din retea, astfel incat permite detectarea atacurilor directionate, de tip ransomware si a amenintarilor avansate persistente; * Platforma va primi traficul de retea prin porturi mirror, SPAN, TAP sau mecanisme similare de copiere a traficului si va permite monitorizarea pentru cel putin trafic de tip HTTP, SMTP, FTP, DNS, CIFS, etc; * Va include functionalitate de tip sandbox nativa prin intermediul aceleasi platforme hardware, fara a necesita platforma hardware dedicata acestei functionalitati; |
| Detectie amenintari avansate | * Solutia va asigura detectie si analiza in toate fazele unui atac, raportand descoperirile pentru fiecare faza in parte: * Colectarea de informatii; * Punctul de intrare; * Comunicatia de tip Command & Control; * Miscarea laterala; * Descoperirea de resurse si date; * Extragerea datelor; * Solutia va asigura suport de detectie si analiza in retele de date IPv4 si IPv6, respectiv va oferi suport pentru comunicarea parametrilor de stare prin protocol SNMPv2/v3 si netSNMP; * Solutia trebuie sa permita crearea de reguli si definitii de scanare a resurselor de infrastructura atat in mod individual cat si prin grupari de reguli, reguli si grupari de reguli ce vor putea fi activate/dezactivate individual; * Solutia va asigura detectia continutului malitios cel putin prin urmatoarele mecanisme: * Scanare de malware cu motoare bazate pe semnaturi, respectiv prin metode euristice, pentru detectarea de malware cunoscut si necunoscut; * Detectie a kit-urilor de exploatare a browser-elor web; * Decodare si decompresie fisiere embedded; * Simulare in sandbox pentru fisiere suspicioase; * Solutia va asigura detectarea si analiza comunicatiei suspecte cel putin prin urmatoarele mecanisme: * Analiza de destinatii (URL, IP, domenii, e-mail, IRC, etc) prin blacklisting si whitelisting dinamic local; * Detectie e-mailuri de tip Spear Phishing si/sau Phishing; * Detectie comunicatie de tip Command & Control; * Analiza reputationala pentru toate URL-urile solicitate si integrate in alte resurse (ex: fisiere Office); * Reguli de amprentare a traficului de comunicatie; * Solutia va asigura urmatoarele mecanisme de analiza comportamentala: * Reguli de analiza euristica; * Identificare si analiza pentru utilizarea a peste 100 de protocoale si aplicatii, inclusiv aplicatii web (SMTP, POP3, IMAP4, HTTP, HTTPS, Kerberos, RADIUS, LDAP, DCE-RPC, SMB, SMB2, DNS request, DNS response, DHCP, DHCPv6, FTP, TFTP, File Transfer, RDP, SSH, TELNET, VNC, Cisco-TELNET, RADMIn, MODBUS-UDP, MODBUS-TCP, SQL, MySQL, MSSQL,Oracle, PostGres, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Gmail, Hotmail, Yahoo mail, ARP, IGMP, MMS, ICMP, IRC, SIP2, Bittorent, Direct Connect, Kazaa, Google Talk, MSN, YMSG, Skype, Yahoo Web Messenger, Ares, Blubster, Cabos, Deepnet Explorer, eDonkey\_eMule, eDonkey, Foxy, FreeWire, Gnucleus LAN, Gimme, GnucDNA GWebCache, Gnutella/Limewire/Bearshare/Shareaza, iMesh, Jubster, Kceasy, KuroMiranda, MLDonkey, MoodAmp, MyNapster, Nova GWebCache, OpenNap, Ppstream, SoulSeek, Swapper GWebCache, Winny, WinMX, Xnap, Xolox, Zultrax, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, etc); * Fingerprinting de comportamente; * Solutia trebuie sa identifice si sa marcheze sursele de incredere pentru transmiterea datelor (sisteme si aplicatii marcate ca nefiind infectate cu elemente malitioase), cel putin pentru urmatoarele tipuri de resurse: * Gama de adrese IP; * Domenii; * Tipuri de servere: Kerberos, Active Directory, FTP, SMTP, HTTP proxy, Domain Controller, Contain Management Server, File Server (SMB), RADIUS, DNS, Database server, Web Server, Software Update Server, etc; * Solutia trebuie sa ofere protectie impotriva amenintarilor malware comune, cel putin pentru: * Vulnerabilitati (CVE): Apache Struts, Foxit Reader, MS SilverLight, Mozilla, Joomla, Sun Java, IE, Shellshock, SSL CCS Injection, etc; * Unelte si kit-uri de penetrare: Cobaltstrike, Metasloit reverse (shell, bash, telnet, perl, netcat, etc), Poisonivy, Meterpreter reverse (PHP/Python/Perl), PsExec, Keylogger http request, IRCbot connection, DDOS tools (HOIC, LOWC, LOIC), TOR, Bitcoint request, etc; * Amenintari de tip ransomware: Cerber, Locky, Cryptesla, etc; * Unelte si kit-uri de exploatare a vulnerabilitatilor: Neutrino, Magnitude, Rig, Angler, Nuclear, Range HTTP, Ghost SMTP, etc; * Solutia trebuie sa permita definirea intervalului orar de lucru, respectiv a proceselor de detectie si analiza ce ruleza in functie de respectivul orar; * Solutia trebuie sa permita definirea de exceptii de la regulile de analiza si detectie cel putin pentru urmatoarele tipuri de resurse: Host, Protocol, Adresa IP, Gama de adrese IP, etc; * Solutia trebuie sa permita crearea rapida de filtre de analiza, detectie si raportare, bazate cel putin pe urmatoarele tipuri de resurse: sisteme afectate, sisteme cu un numar mare de detectii/evenimente de securitate, obiecte suspicioase (adrese IP, domenii, fisiere, etc); * Solutia trebuie sa permita transmiterea manuala a fisierelor de analiza, precum si un API de interfatare cu alte produse terte pentru transmiterea de solicitari de analiza si extragere de rezultate, inclusiv partajare de obiecte suspicioase si indicatori de compromis; * Solutia trebuie sa permita integrarea nativa cu Componenta de protecție a resurselor la nivel de post de lucru, asigurand monitorizarea la nivel de context a posturii de securitate a intregului ecosistem, respectiv raportarea activitatilor detaliate de sistem, precum si natura si dimensiunea oricarui atac survenit; * Solutia trebuie sa permita trimiterea obiectelor malitioase identificate (amprenta criptografica a fisierelor, adrese IP, domenii, adrese URL, etc) catre toate sistemele cu care se integreaza nativ astfel incat amenintarile si obiectele malitioase sa poata fi blocate in intreaga infrastructura deservita; |
| Functionalitati de tip Sandbox | Platforma ofertata va include functionalitate integrata hardware pentru procesele specifice activitatilor de tip “sandbox”:   * Va permite analiza elementelor suspecte, dupa filtrarea lor prealabila efectuata de modulele de detectie a amenintarilor avansate; * Va permite functionalitati avansate de evitare a evadarii din sandbox, precum si un mod de "safe live" pentru analiza unor descarcari multi-nivel, URL, Command & Control, etc; * Va oferi urmatoarele metode de analiza si detectie: * Soluția trebuie să fie capabilă să detecteze și să prevină software-ul malițios avansat, atacuri de tipul „zero-day” și de tip APT (Advanced Persistent Threat) direcționate; * Soluția trebuie să detecteze software-ul malițos de tip “zero-day multi-stage” și atacuri direcționate fără o cunoaștere prealabilă a software-ului malițos; * Analiza statica, euristica si comportamentala; * Analiza bazata pe reputatia adreselor si fisierelor pentru URL-uri; * Analiza conexiunilor de retea outbound sau de mesagerie suspicioase; * Analiza fisierelor suspicioase ce efectueaza conexiuni la servere de tip Command & Control; * Analiza atacurilor de tip ransomware, deception, social-engineering, hijack, redirectionare si/sau furt de date, rootkit cloaking; * Analiza operatiunilor cu fisiere: file drop, download, partajare si/sau replicare de fisiere; * Analiza operatiunilor ce vizeaza modificarile de procese, servicii sau obiecte de memorie; * Evaluarea continua a amenintarilor, actiunilor intreprinse de elementele malware si impactul asupra sistemului analizat; * Mecanisme incluse de analiza de tip forensics, cel putin prin captura pachetelor de date relevante (PCAP); * Soluția trebuie să asigure procese de analiză cu suport atât pentru arhitecturi de tip x86 cât și pentru arhitecturi de tip x64; * Soluția trebuie să asigure restaurarea mașinilor virtuale de analiză la o configurație de bază după finalizarea analizei unui software malițios, automat sau manual; * Mașinile virtuale preinstalate vor avea configurate aplicații de tip browser (cel puțin Internet Explorer, Mozilla Firefox, Google Chrome, Safari), plugin-uri (cel puțin Adobe Flash, Adobe Shockwave, Adobe Air) precum și aplicații uzuale (cel puțin Adobe Acrobat Reader, Microsoft Office Word, Excel, Powerpoint, Outlook, Oracle Java JRE, Windows Media Player, Quicktime Player); * Soluția trebuie să asigure cel puțin analiza celor mai comune tipuri de fișiere cunoscute ca fiind folosite pentru distribuirea sau găzduirea de aplicații malware (fișiere executabile – EXE, DLL, documente Microsoft Office – DOC, DOCX, XLS, XLSX, PPT, PPTX, documente PDF, fișiere JAR, BAT, fișiere de tip imagine, fișere de tip video, Flash, arhive – ZIP, RAR, SFX); * Soluția trebuie să asigure extinderea tipurilor de fișiere ce pot fi analizate; * Soluția trebuie să asigure cel puțin analiza obiectelor Web prin furnizarea unui URL; * Soluția trebuie să fie capabilă să simuleze acțiuni ale utilizatorilor finali (interacțiunea dintre mașina virtuală de analiză și utilizator) în scopul de a forța executarea de software malițios care se bazează pe astfel de acțiuni (de exemplu un click de mouse, răspuns la ferestre dialog sau parcurgerea unor pași de instalare) sau pe observarea prezenței utilizatorului (prin apelarea unor funcții Windows native sau din interfața Windows API); * Soluția trebuie să asigure jurnalizarea apelurilor de funcții Windows native și din interfața Windows API relevante pentru depistarea comportamentului malițios; * Soluția trebuie să asigure identificarea și rularea software-ului malițios care are capabilitatea de a identifica mediile virtualizate sau emulate; * Soluția trebuie să genereze un set de indicatori de compromitere după execuția virtuală a software-ului malițos; * În cazul unui atac soluția trebuie să raporteze cel puțin IP-ul sursă, IP-ul destinație, serverul de tip Command & Control, URL-ul, botname-ul, clasa de malware, protocoalele utilizate și severitatea infecției; |
| Raportare | * Soluția trebuie să prezinte rezultatele analizei software-ului malițios sub forma unui tablou de bord grafic (dashboard) și/sau a unui raport care detaliază comportamentul amenințării; * Solutia trebuie sa permita reconfigurarea tabloului de bord grafic prin folosirea unor elemente de tip widget (cel putin elemente pentru gradul de incarcare CPU/RAM/Disc, top amenintari/URL-uri, top sisteme cu evenimente de securitate, top comportamente suspicioase, top sisteme infectate, top sisteme exploatate, top aplicatii/fisiere cu comportament suspicios, traficul in timp real generat de procesele de analiza si detectie, etc); * Raportul furnizat va conține cel puțin următoarele informații: * Tipul fișierului analizat; * Sumele de control (MD5, SHA) ale fișierelor analizate sau create pe mașina virtuală de analiză; * Dacă fișierul este executabil se va preciza dacă au fost folosite aplicații de tip packer și tipul acestora; * Informații extrase din header-ul fișierelor executabile; * Modificările produse la nivelul sistemului de operare; * Modificările produse la nivelul aplicațiilor instalate; * Modificările produse asupra sistemului de fișiere; * Modificările produse asupra regiștrilor; * Librării DLL încărcate la rulare; * Funcțiile API apelate, în ordine cronologică; * Informații despre procesele create/modificate/oprite; * Informații despre serviciile create/modificate/oprite; * Obiecte de tip Mutex create; * Eventuale hook-uri SSDT, IDT sau IRP create; * Eventuale conexiuni de rețea create și protocoalele de transport folosite; * Interogările DNS; * URL-urile accesate; * Adrese IP contactate și porturile logice folosite; * Informatii de localizare geografica a adreselor IP contactate; * Captura zonelor de memorie aferente proceselor suspecte de comportament malițios; * Tipul de exploit folosit; * Solutia trebuie sa permita ordonarea/re-ordonarea campurilor din raport dupa coloana/coloanele selectate (indicator de risc al sistemelor, faza de atac, numele sistemelor, adresa IP, data la care a survenit atacul, etc); * Soluția trebuie să permită exportul rapoartelor și al alertelor despre software-ul malițios cel puțin în format PDF, HTML si XLS; * Soluția trebuie să suporte automatizarea raportării cel puțin pentru următoarele intervale de timp: zilnic, săptămânal, lunar și definit de utilizator; |
| Integrare | * Solutia ofertata trebuie sa se integreze nativ cel putin cu urmatoarele tipuri de servicii oferite de producatorul solutiei (servicii ce vor permite actualizarea automata, neasistata a definitiilor de elemente malware): * La nivelul filtrarii URL: Serviciu de analiza bazat pe reputatia adreselor si fisierelor pentru URL-uri, respectiv motor intern responsabil de scanarea, detectarea si atasarea unui scor de risc fiecarei resurse URL solicitate si accesate. Acest motor trebuie sa permita si scanarea retroactiva pentru elementele malitioase de tip Command & Control; * La nivelul filtrarii de fisiere: Serviciu de analiza bazat pe reputatia fisierelor cunoscute de la producatori cunoscuti, pentru a putea efectua procesele de comparare cu fisierele detectate in analiza locala, respectiv serviciu global de identificare a fisierelor malitioase prin colectarea datelor de la toti senzorii pe care producatorul solutiei ofertate ii are instalati la nivel global; * La nivelul aplicatiilor mobile: Serviciu de analiza bazat pe reputatia aplicatiilor mobile, in vederea detectarii unor activitati malitioase, utilizarii de resurse si incalcarii ale nivelurilor de confidentialitate; * Solutia trebuie sa ofere un API de interfatare cu alte produse terte (specific cu producatorul Componentei de protectie la nivel de retea ofertate, respectiv cel putin cu urmatorii producatori de solutii de securitate: Check Point, IBM Security, Palo Alto Networks, F5 Networks, BlueCoat, A10 Networks, etc) pentru transmiterea de solicitari de analiza si extragere de rezultate, inclusiv partajare de obiecte suspicioase si indicatori de compromis; * Solutia trebuie sa permita integrarea nativa cu Componenta de protecție a resurselor la nivel de post de lucru ofertata, asigurand monitorizarea la nivel de context a posturii de securitate a intregului ecosistem, respectiv raportarea activitatilor detaliate de sistem, precum si natura si dimensiunea oricarui atac survenit; * Solutia trebuie sa permita integrarea nativa cu produse de tip SIEM pentru transferul evenimentelor cel putin prin mecanisme UDP/TCP/SSL; * Solutia trebuie sa permita integrarea descriptorilor malware cu solutii terte (ex: YARA); |
| Management | * Soluția trebuie să asigure administrarea sa prin intermediul unei console web, fără instalarea de software suplimentar; * Solutia permite management-ul prin interfata seriala, CLI (cu SSH) si https GUI; * Soluția trebuie să utilizeze un canal de comunicatie criptat intre administratori și consola de administrare; * Platforma va permite colectarea de informatii statistice si istorice despre utilizarea memoriei, procesorului, conexiuni si trafic si afisarea acestora in grafice disponibile in interfata grafica; * Soluția trebuie să asigure crearea de conturi cu roluri diferite în administrarea sau monitorizarea alertelor; * Soluția trebuie să poată identifica numele stației de lucru implicate în alertă; * Soluția trebuie să asigure păstrarea logurilor arhivate. Aceste loguri trebuie să poată fi descărcate pe stația de lucru a unui utilizator cu rol de administrare a soluției; * Solutia va putea trimite alerte despre diverse erori prin SNMP, syslog, e-mail; * Solutia va permite definirea de multiple domenii de administrare; * Soluția trebuie să poată fi actualizată online și offline; * Soluția trebuie să poată utiliza un proxy cu autentificare pentru contactarea serverului de update; * Solutia va permite resetarea la configuratiile initiale ("din fabrica"); |
| Alimentare | Pentru asigurarea redundantei complete a echipamentului propus fiecare element major component al componentei centrale de protecție avansată antimalware trebuie sa ofere alimentare redundanta prin cel putin doua surse independente de alimentare. Sursele trebuie sa ofere functionalitate hot-swap pentru inlocuirea rapida, fara oprirea alimentarii sistemului si fara intreruperea serviciilor asigurate de platforma; |
| Ventilatie | Toate elementele de asigurare a ventilatiei sistemului trebuie sa fie de tip hot-swap pentru inlocuirea lor rapida in caz de avarie, fara intreruperea functionalitatilor oferite de platforma; |
| Cerinte constructive | * Componenta centrala de protecție avansată antimalware trebuie să fie montabilă în rack-uri standard de 19”; * Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporţi, şuruburi/captive); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivelor echipamente; * Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software (sistem de operare, firmware, etc). |

* + - 1. Componenta de protecție a resurselor la nivel de post de lucru

Componenta de protectie a resurselor la nivel de post de lucru trebuie sa indeplineasca urmatoarele specificatii tehnice minimale:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Solutia va asigura protectia mediilor fizice (cu suport pentru o plaja larga de sisteme de operare), a mediilor virtuale (in principal pentru platforma de virtualizare ofertata, respectiv pentru VMware vSphere, Microsoft Hyper-V, Citrix Xen Server, Open Stack, containere Docker, etc) si sistemelor de tip cloud public (VMware, Amazon AWS, Microsoft Azure, etc); * Solutia va oferi flexibilitate in licentiere, configurare, distributie si operare, astfel incat se va putea configura local, Software-as-a-Service sau prin intermediul Marketplace in Amazon AWS si Microsoft Azure; * In mediile virtuale trebuie sa functioneze in mod agentless, asigurand protectie avansata pentru toate sistemele instalate in platforma de virtualizare, respectiv automatizarea fluxurilor de securitate prin izolarea sistemelor in zonele de carantina ale retelelor virtuale segmentate; * Platforma va asigura acoperire si vizibilitate completa in toate punctele din retea, astfel incat permite detectarea atacurilor directionate, de tip ransomware si a amenintarilor avansate persistente; * Va include functionalitate de tip sandbox nativa prin intermediul componentei centrale de protecție avansată antimalware, fara a necesita platforma hardware dedicata acestei functionalitati; |
| Detectie si protectie amenintari avansate | * Solutia trebuie sa includa un motor de detectie si preventie a elementelor de tip malware, bazat pe serviciu de reputatie al aplicatiilor/serviciilor/proceselor, motor ce va oferi cel putin urmatoarele functionalitati: * Analiza si detectia elementelor de tip virus, spyware, grayware, ransomware, expoit, etc; * Analiza proceselor si a zonelor de memorie in care respectivele procese ruleaza; * Analiza comportamentala pentru aplicatii si procese; * Corelarea amenintarilor detectate in toate sistemele de tip endpoint analizate (sisteme de lucru, servere, etc); * Detectarea amenintarilor inainte de a se executa efectiv, folosind algoritmi matematici de predictie, dar si analiza comportamentala, proces ce va ajuta la detectarea amenintarilor in timpul executiei acestora, folosind sabloane comportamentale; * Solutia trebuie sa includa un motor de detectie si preventie a elementelor de tip malware, bazat pe un serviciu de reputatie a adreselor web, motor ce va oferi cel putin urmatoarele functionalitati: * Va colabora cu motorul anti-malware descris mai sus, pentru a furniza un rating al resurselor URL accesate de sistemul analizat; * Va permite functionarea in mod detectie/protectie cu comportament asemanator cu cel al unui proxy de retea, insa pentru sistemul pe care ruleaza; * Solutia trebuie sa includa un motor de detectie si preventie a elementelor de tip malware, bazat pe un serviciu de tip host firewall/IDS/IPS, motor ce va oferi cel putin urmatoarele functionalitati: * Motor de tip firewall flexibil ce poate functiona in mod restrictiv sau permisiv, prin utilizarea modurilor tap si/sau inline; * Va putea aplica politici de detectie/monitorizare sau de protectie/blocare, plus strategii permisive ("alow all/deny explicit") sau restrictive ("deny all/alow explicit"); * Blocarea/filtrarea se va putea face dupa: sursa/destinatie, adresa IP/MAC, porturi de comunicatie, tip de trafic (TCP/UDP); * Ve permite scanarea porturilor deschise pe sistemele de tip endpoint si va oferi optiuni de blcare sau doar de jurnalizare a evenimentelor; * Motor de tip IDS/IPS ce va permite actualizarea software (Virtual Patching) pentru sisteme de operare, aplicatii si servere de aplicatii; * Motor de scanare de vulnerabilitati, ce se va putea initia printr-un proces de scanare recomandata si va permite identificarea in mod particularizat a informatiilor (profiling) legate de sistemul pe care ruleaza agentul: sistem de operare, aplicatii, servere de aplicatii, etc, respectiv va descarca semnaturile actualizarilor software pentru elementele detectate; * Semnaturile detectate prin procesul de scanare se vor putea aplica in mod automat pe sistem, la fiecare activitate de scanare, astfel incat sa nu necesite interventie din partea administratorului. Aplicarea automata a patchurilor virtuale nu va impacta disponibilitatea si/sau functionalitatea serviciilor; * Motorul de scanare de vulnerabilitati va asigura detectia continua si aplicarea automata a actualizarilor software din momentul zero al aparitiei vulnerabilitatilor respective; * Va permite inspectia traficului de tip SSL; * Solutia trebuie sa includa un motor de control automatizat al aplicatiilor, motor ce va oferi cel putin urmatoarele functionalitati: * Va asigura urmarirea devierilor de la setul initial de aplicatii instalate, prin compararea unui baseline de inventar de aplicatii cu situatia curenta rezultata dintr-o operatiune de analiza; * Se vor putea folosi seturi de reguli (inventar de configurare) partajate intre mai multe sisteme cu inventare asemanatoare de aplicatii; * Se vor putea urmari modificari ale aplicatiilor la mai multe niveluri: denumire fisier, cale sau locatie, marca de timp, permisiuni, continut fisiere, folosind metode de comparatie la nivel de hash, dimensiune fisier, cale sau denumire fisier; * In urma detectarii unor modificari in lista de aplicatii instalate, se vor putea configura actiuni de blocare sau aprobare a executiei; * Solutia trebuie sa includa un motor de asigurare a integritatii fisierelor, serviciilor si aplicatiilor, motor ce va oferi cel putin urmatoarele functionalitati: * Detectarea modificarilor realizate la nivel de fisiere sau zone critice de sistem (fisiere de tip DLL/EXE, directoare, registrul Windows, procese, porturi de retea deschise, in directoare temporare, in Recycle Bin, fisierul hosts, aplicatiile ce ruleaza la pornirea sistemului de operare, fisierele de configurare a setarilor de retea, in Task Scheduler, a conturilor de utilizator, a aplicatiilor de tip browser, in directorul Windows, System32, etc) ce pot indica o activitate suspicioasa; * Motorul va dispune de reguli predefinite pentru sistemele de operare cunoscute, astfel incat, in urma unui proces de analiza, se va construi un baseline ce va ajuta la identificarea tuturor tipurilor de fisiere prezente pe sistem; * Va permite configurarea analizelor intr-un interval orar, respectiv in timp real, cu prioritate de resurse ridicata sau scazuta; * Solutia trebuie sa includa un motor de inspectie a jurnalelor de sistem, motor ce va oferi cel putin urmatoarele functionalitati: * Va permite identificarea evenimentelor importante din multitudinea de evenimente de securitate/operationale ce sunt generate in mod curent de sistemele de operare/servicii/aplicatii (Squid, jurnale de sistem Windows, jurnale de sistem generate de aplicatii si servicii native Microsoft Windows Server: IIS, Routing and Remote Access Server, Terminal Server, AD Server, Exchange Server, DHCP, DNS, etc); * Va permite detectarea comportamentelor suspicioase, colectarea evenimentelor din sisteme de operare si servere de aplicatii diverse, identificarea evenimentelor operationale problematice, crearea si mentierea unei liste de evenimente administrative, precum si satisfacerea unor cerinte de conformitate (ex: PCI DSS); * Evenimentele vor fi detectate in baza unei analize ce va detecta categoria de evenimente ce se doresc urmarite (ex: Database Server - MSSQL, FTP Server - ProFTPD, Mail Server - Microsoft Exchange, etc); * Solutia va oferi urmatoarele mecanisme integrate de detectie si preventie a amenintarilor informatice avansate: * Descoperirea sistemelor prin maparea structurii extrase din sisteme de tip directory (Active Directory sau similar), prin analiza unui set de adrese IP, prin integrarea directa cu paltformele de management al mediilor de virtualizare (in special cu platforma de management al solutiei de virtualizare ofertate, VMware vSphere, Microsoft Hyper-V, etc); * Va permite aplicarea de politci in mod automat in functie de apartenenta la un astfel de grup de resurse descoperite, astfel ca orice sistem virtual din platforma de virtualizare, respectiv orice sistem fizic (statie de lucru si/sau server) va putea fi automat protejat in functie de criteriile de apartenenta; * Solutia va oferi suport pentru urmatoarele sisteme de operare: Microsoft Windows Server 2003/2003 R2/2008/2008 R2/2012/2012 R2/2016, Microsoft Windows 7/8/8.1/10, Red Hat Linux 5/6/7, CentOS 5/6/7, Suse Linux, Oracle Linux, Debian, Ubuntu; * Solutia va include o platforma de management dedicata, integrata nativ cu componenta centrală de protecție avansată antimalware, respectiv cu functionalitatea de tip sandbox disponibila in aceasta; * Platforma de management va oferi suport de instalare pentru urmatoarele baze de date: Microsoft SQL, Postgres, etc; * Platforma de management va putea fi instalata in topologie redundanta de tip cluster activ-activ; * Platforma de management va permite integrarea cu sisteme de tip directory (Active Directory, LDAP, etc) si platforme de management al mediilor de virtualizare (in special cu platforma de management al solutiei de virtualizare ofertate, VMware vSphere, Microsoft Hyper-V, etc); * Platforma de management va permite nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor si a drepturilor de acces. Pentru sporirea securitatii in mecanismele de autentificare, platforma trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp; * Platforma de management va permite activarea agentilor pe sitemele endpoint in mod automat/manual, cu/fara parola de activare, respectiv reactivarea agentilor pe masinile virtuale ce au fost clonate/copiate; * Platforma de management va oferi acces securizat prin HTTPS (TLS), respectiv va oferi optiuni de autentificare multi-factor; * Platforma de management va oferi posibilitatea de trimiterea a jurnalelor si evenimentelor catre sisteme de tip Syslog/SIEM, respectiv va oferi mesaje SNMP catre sistemele de monitorizare a infrastructurii; |
| Functionalitati de tip Sandbox | Prin integrarea nativa cu componenta centrală de protecție avansată antimalware solutia ofertata va include functionalitate integrata pentru procesele specifice activitatilor de tip “sandbox”:   * Va permite analiza elementelor suspecte, dupa filtrarea lor prealabila efectuata de modulele de detectie a amenintarilor avansate; * Va permite functionalitati avansate de evitare a evadarii din sandbox, precum si un mod de "safe live" pentru analiza unor descarcari multi-nivel, URL, Comamnd & Control, etc; * Va oferi urmatoarele metode de analiza si detectie: * Soluția trebuie să fie capabilă să detecteze și să prevină software-ul malițios avansat, atacuri de tipul „zero-day” și de tip APT (Advanced Persistent Threat) direcționate; * Soluția trebuie să detecteze software-ul malițos de tip “zero-day multi-stage” și atacuri direcționate fără o cunoaștere prealabilă a software-ului malițos; * Analiza statica, euristica si comportamentala; * Analiza bazata pe reputatia adreselor si fisierelor pentru URL-uri; * Analiza conexiunilor de retea outbound sau de mesagerie suspicioase; * Analiza fisierelor suspicioase ce efectueaza conexiuni la servere de tip Command & Control; * Analiza atacurilor de tip ransomware, deception, social-engineering, hijack, redirectionare si/sau furt de date, rootkit cloaking; * Analiza operatiunilor cu fisiere: file drop, download, partajare si/sau replicare de fisiere; * Analiza operatiunilor ce vizeaza modificarile de procese, servicii sau obiecte de memorie; * Evaluarea continua a amenintarilor, actiunilor intreprinse de elementele malware si impactul asupra sistemului analizat; * Mecanisme incluse de analiza de tip forensics, cel putin prin captura pachetelor de date relevante (PCAP); * Soluția trebuie să asigure procese de analiză cu suport atât pentru arhitecturi de tip x86 cât și pentru arhitecturi de tip x64; * Soluția trebuie să asigure restaurarea mașinilor virtuale de analiză la o configurație de bază după finalizarea analizei unui software malițios, automat sau manual; * Mașinile virtuale preinstalate vor avea configurate aplicații de tip browser (cel puțin Internet Explorer, Mozilla Firefox, Google Chrome, Safari), plugin-uri (cel puțin Adobe Flash, Adobe Shockwave, Adobe Air) precum și aplicații uzuale (cel puțin Adobe Acrobat Reader, Microsoft Office Word, Excel, Powerpoint, Outlook, Oracle Java JRE, Windows Media Player, Quicktime Player); * Soluția trebuie să asigure cel puțin analiza celor mai comune tipuri de fișiere cunoscute ca fiind folosite pentru distribuirea sau găzduirea de aplicații malware (fișiere executabile – EXE, DLL, documente Microsoft Office – DOC, DOCX, XLS, XLSX, PPT, PPTX, documente PDF, fișiere JAR, BAT, fișiere de tip imagine, fișere de tip video, Flash, arhive – ZIP, RAR, SFX); * Soluția trebuie să asigure extinderea tipurilor de fișiere ce pot fi analizate; * Soluția trebuie să asigure cel puțin analiza obiectelor Web prin furnizarea unui URL; * Soluția trebuie să fie capabilă să simuleze acțiuni ale utilizatorilor finali (interacțiunea dintre mașina virtuală de analiză și utilizator) în scopul de a forța executarea de software malițios care se bazează pe astfel de acțiuni (de exemplu un click de mouse, răspuns la ferestre dialog sau parcurgerea unor pași de instalare) sau pe observarea prezenței utilizatorului (prin apelarea unor funcții Windows native sau din interfața Windows API); * Soluția trebuie să asigure jurnalizarea apelurilor de funcții Windows native și din interfața Windows API relevante pentru depistarea comportamentului malițios; * Soluția trebuie să asigure identificarea și rularea software-ului malițios care are capabilitatea de a identifica mediile virtualizate sau emulate; * Soluția trebuie să genereze un set de indicatori de compromitere după execuția virtuală a software-ului malițos; * În cazul unui atac soluția trebuie să raporteze cel puțin IP-ul sursă, IP-ul destinație, serverul de tip Command & Control, URL-ul, botname-ul, clasa de malware, protocoalele utilizate și severitatea infecției; |
| Functionalitati de detectie si preventie a scurgerilor de date | Solutia ofertata trebuie sa includa un motor de detectie si prevenire a scurgerilor de informatii, motor ce va oferi cel putin urmatoarele functionalitati:   * Recunoașterea în timp real a conținutului și contextului unui anumit fișier sau a unei informații; * Învățarea folosind informații confidențiale/senzitive deja existente (exemplu: conținutul documentelor definite ca fiind confidențiale să poată fi identificat în alte documente dacă procentul de asemănare depășește o valoare prestabilită și care poate fi configurată); * Recunoașterea și analizarea conținutului a cel puțin 300 de tipuri de fișiere diferite (funcționalitatea trebuie să fie disponibilă pentru utilizare fără o configurare specială - out of the box); * Asigurarea lucrului cu documente scrise în limba română (cel puțin activitățile de detectare, amprentare și indexare a acestora); * Setarea unui procent minim de detecție pentru fișierele amprentate; * Inspectarea conținutului în baza unor liste de cuvinte/fraze cheie mari, fără degradarea performanței; * Asigurarea detectării pe baza conținutului și nu pe baza extensiei fișierelor; * Protejarea conținutului prin metode de detecție bazate pe un set redus de documente care să asigure o detecție corectă a unor documente similare; * Specificarea coloanelor de date amprentate care să declanșeze un incident (de exemplu, prenume, nume de familie, adresă și CNP) și a celor care să nu declanșeze un incident (de exemplu, prenume și nume de familie); * Detectarea comunicațiilor sau a fișierele criptate; * Posibilitatea de a utiliza o singură politică de scanare a conținutului indiferent dacă informația este stocată sau utilizată în rețea sau pe stația de lucru; * Stocarea incidentelor și a detaliilor aferente acestora în mod criptat în baza de date a platformei de management; * Posibilitatea de a normaliza diverse variante ale prezentării datelor (exemplu: dacă documentul conține un string "123456789", să se declanșeze alerte cel puțin la variante de forma "123-456-789", "123.456.789", "[123][456][789]"); * Definirea unor tipuri de noi de fișiere care să fie recunoscute și analizate chiar dacă nu sunt în lista de fișiere recunoscute implicit; * Configurarea de reguli multiple de răspuns la un incindent cel puțin ȋn funcție de severitate și politica ce a declanșat incidentul; * Evidențierea în pagina de afișare a incidentului a motivelor principale care au dus la violarea unei politici; * Corelarea după expeditor, destinatar, nume fișier, propietarul fișierului, numele utilizatorului sau politica declanșată; * Emiterea de rapoarte de sumarizare pe nivele multiple (grupate cel puțin pe utilizatori, politici, severitate sau alte criterii disponibile); * Extragerea de atribute despre utilizatori din structura de tip Active Directory existentă și includerea acestora în informațiile despre incidentele generate; * Permiterea adăugării oricărui atribut structură de tip Active Directory în platforma de management a soluției și în detaliile incidentelor; * Se vor putea rula cel puțin următoarele tipuri de rapoarte aferente incidentelor: lista incidentelor, lista personalizată a incidentelor după caracteristici specifice, lista incidentelor declanșate de funcțiile de căutare la nivelul stațiilor de lucru; * Filtrarea avansată pe nivele a incidentelor după diverse reguli definibile: configurația agentului, starea configurației agentului, numele aplicației care a generat incidentul, numele fișierului, locația fișierului, mărimea fișierului, adresa de email a propietarului fișierului, numele proprietarului fișierului, adresa de IP a destinației, data detecției, identificatorul stației care a generat incidentul, numele domeniului asociat incidentului, locația stației care a generat incidentul, ultima dată la care a fost modificat fisierul, data la care au fost generate incidentele, adresa de IP a stației care a generat incidentul, protocol, lista de control a accesului la fișierul care a generat incidentul, lista de control a partajării fișierului care a generat incidentul, existența anterioară a incidentului, etc; * Monitorizarea și identificarea datelor confidențiale din fișierele arhivate (comprimate); * Inspectarea recursivă a arhivelor (zip, rar, tar) și detecția în interiorul arhivelor incluse pe mai multe niveluri; * Efectuarea de acțiuni manuale sau automate ca răspuns la încălcarea unei politici (pe care le poate lua o persoană competentă sau soluția în urma configurării politicilor); * Furnizarea unui set extins de politici predefinite bazate pe legislație și/sau standarde de conformitate sau pe bunele practici în domeniu, set care să poată fi modificat/particularizat în funcție de necesități; * Definirea de politici bazate pe informații din structura de tip Active Directory (cel puțin departament, OU, group, user); |
| Raportare | Platforma de management inclusa in componenta de protecție a resurselor la nivel de post de lucru trebuie sa ofere urmatoarele capabilitati de raportare centralizata, indiferent de tipul si numarul agentilor din solutie:   * Solutia trebuie să prezinte rezultatele analizei software-ului malițios sub forma unui tablou de bord grafic (dashboard) și/sau a unui raport care detaliază comportamentul amenințării; * Solutia trebuie sa permita reconfigurarea tabloului de bord grafic prin folosirea unor elemente de tip widget (cel putin pentru top amenintari/URL-uri, top sisteme cu evenimente de securitate, top comportamente suspicioase, top sisteme infectate, top sisteme exploatate, top aplicatii/fisiere cu comportament suspicios, traficul in timp real generat de procesele de analiza si detectie, etc); * Raportul furnizat va conține cel puțin următoarele informații: * Tipul fișierului analizat; * Sumele de control (MD5, SHA) ale fișierelor analizate sau create pe mașina virtuală de analiză; * Dacă fișierul este executabil se va preciza dacă au fost folosite aplicații de tip packer și tipul acestora; * Informații extrase din header-ul fișierelor executabile; * Modificările produse la nivelul sistemului de operare; * Modificările produse la nivelul aplicațiilor instalate; * Modificările produse asupra sistemului de fișiere; * Modificările produse asupra regiștrilor; * Librării DLL încărcate la rulare; * Funcțiile API apelate, în ordine cronologică; * Informații despre procesele create/modificate/oprite; * Informații despre serviciile create/modificate/oprite; * Obiecte de tip Mutex create; * Eventuale hook-uri SSDT, IDT sau IRP create; * Eventuale conexiuni de rețea create și protocoalele de transport folosite; * Interogările DNS; * URL-urile accesate; * Adrese IP contactate și porturile logice folosite; * Informatii de localizare geografica a adreselor IP contactate; * Captura zonelor de memorie aferente proceselor suspecte de comportament malițios; * Tipul de exploit folosit; * Solutia trebuie sa permita emiterea de rapoarte de sumarizare pe nivele multiple (grupate cel puțin pe utilizatori, politici, severitate sau alte criterii disponibile); * Se vor putea rula cel puțin următoarele tipuri de rapoarte aferente incidentelor de scurgere de informatii: lista incidentelor, lista personalizată a incidentelor după caracteristici specifice, lista incidentelor declanșate de funcțiile de căutare la nivelul stațiilor de lucru/serverelor; * Solutia trebuie sa permita ordonarea/re-ordonarea campurilor din raport dupa coloana/coloanele selectate (indicator de risc al sistemelor, faza de atac, numele sistemelor, adresa IP, data la care a survenit atacul, etc); * Soluția trebuie să permită exportul rapoartelor și al alertelor despre software-ul malițios cel puțin în format PDF, HTML si XLS; * Soluția trebuie să suporte automatizarea raportării cel puțin pentru următoarele intervale de timp: zilnic, săptămânal, lunar și definit de utilizator; |
| Integrare | * Solutia ofertata trebuie sa se integreze nativ cel putin cu urmatoarele tipuri de servicii oferite de producatorul solutiei (servicii ce vor permite actualizarea automata, neasistata a definitiilor de elemente malware): * La nivelul filtrarii URL: Serviciu de analiza bazat pe reputatia adreselor si fisierelor pentru URL-uri, respectiv motor intern responsabil de scanarea, detectarea si atasarea unui scor de risc fiecarei resurse URL solicitate si accesate. Acest motor trebuie sa permita si scanarea retroactiva pentru elementele malitioase de tip Command & Control; * La nivelul filtrarii de fisiere: Serviciu de analiza bazat pe reputatia fisierelor cunoscute de la producatori cunoscuti, pentru a putea efectua procesele de comparare cu fisierele detectate in analiza locala, respectiv serviciu global de identificare a fisierelor malitioase prin colectarea datelor de la toti senzorii pe care producatorul solutiei ofertate ii are instalati la nivel global; * La nivelul aplicatiilor mobile: Serviciu de analiza bazat pe reputatia aplicatiilor mobile, in vederea detectarii unor activitati malitioase, utilizarii de resurse si incalcarii ale nivelurilor de confidentialitate; * Solutia trebuie sa ofere un API de interfatare cu alte produse terte (specific cu producatorul Componentei de protectie la nivel de retea ofertate, respectiv cel putin cu urmatorii producatori de solutii de securitate: Check Point, IBM Security, Palo Alto Networks, F5 Networks, BlueCoat, A10 Networks, etc) pentru transmiterea de solicitari de analiza si extragere de rezultate, inclusiv partajare de obiecte suspicioase si indicatori de compromis; * Solutia trebuie sa permita integrarea nativa cu Componenta centrală de protecție avansată antimalware ofertata, asigurand monitorizarea la nivel de context a posturii de securitate a intregului ecosistem, respectiv raportarea activitatilor detaliate de sistem, precum si natura si dimensiunea oricarui atac survenit; * Solutia trebuie sa permita integrarea nativa cu produse de tip SIEM pentru transferul evenimentelor cel putin prin mecanisme UDP/TCP/SSL; * Solutia trebuie sa permita integrarea descriptorilor malware cu solutii terte (ex: YARA); |
| Garanţie si suport | * Pentru toate elementele si modulele integrate, solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Componenta de management a datelor de audit

Componenta de management a datelor de audit trebuie sa indeplineasca urmatoarele **specificatii tehnice minimale**:

|  |  |
| --- | --- |
| **Caracteristica** | **Cerinta tehnica minimala** |
| Arhitectura | * Solutia va asigura managementul datelor de audit din mediile fizice (cu suport pentru o plaja larga de sisteme de operare) si mediile virtuale (in principal pentru platforma de virtualizare ofertata); * Solutia va oferi flexibilitate in licentiere, configurare, distributie si operare, astfel incat se va putea configura local, Software-as-a-Service sau prin intermediul Marketplace in Amazon AWS si Microsoft Azure; * Platforma va asigura acoperire si vizibilitate completa in toate punctele din retea, astfel incat va permite managementul datelor de audit pentru intreaga infrastructura; * Solutia va permite instalarea in topologie multiplu-redundanta de tip cluster activ, cu posibilitatea de scalare orizonatala (multiple noduri de procesare) si verticala (adaugarea de resurse de procesare), respectiv va permite instalarea in topologie multi-site; |
| Functionalitati de management a datelor de audit | Solutia ofertata trebuie sa asigure urmatoarele capabilitati si functionalitati:   * Va permite importul datelor din sisteme relationale de baza de date, cu suport cel putin pentru: Microsoft SQL Server, Oracle Database, MySQL, PostgreSQL, etc; * Va permite agregarea datelor din fisiere sistem, jurnale de audit specifice si comunicatie directa de tip syslog (peste retea prin porturi definibile TCP/UDP) pentru sisteme de operare, echipamente hardware, aplicatii, servicii, servicii API, etc; * Analiza datelor de audit se va face in baza unor metrici (puncte numerice de date in relatie directa cu datele de audit colectate intr-un anumit interval de timp) ce pot fi comprimati, stocati si procesati mult mai eficient decat datele de jurnalizare clasice; * Cautarea datelor relevante pentru analiza informatiilor de audit se va face pe baza unei scheme de cautare (parametrii de cautare agregati) ce va fi construita in timp real la momentul executarii cautarii si va putea fi rulata inclusiv asupra datelor ce sunt colectate in timp real; * Datele de audit colectate vor fi stocate in format brut pentru a nu fi nevoie de transformari mari consumatoare de timp si resurse de procesare, respectiv pentru a facilita procesul de cautare in timp real asupra datelor colectate; * Determinarea automata a marcilor temporale, atat pentru datele ce sunt colectate si analizate in timp real (chiar si pentru formate atipice de marci temporale), cat si pentru datele ce nu contin o marca temporala (solutia trebuie sa ataseze o marca temporala bazata pe context); * Procesele de cautare si investigatie asupra datelor de audit colectate trebuie sa se realizeze in timp real indiferent de tipul si marimea seturilor de date colectate, respectiv sa ofere suport pentru cel putin urmatoarele tipuri de corelare a datelor: timp, tranzactii, cautari/cautari subsecvente in rezultatele regasite, alipiri ale termenilor de cautare, etc; * Solutia trebuie sa permita atat cautarea in timp real asupra datelor de audit colectate, cat si afisarea rezultatelor in context istoric asupra aceluiasi set de date analizate. Trebuie sa permita cautarea cu operatori de tip Boolean, bazata pe campuri multiple de cautare, cautarea statistica, respectiv cautarea subsecventa in rezultatele regasite. Rezultatele si modele de date trebuie sa poata fi afisate pe masura ce procesele de cautare se executa, permitand corelarea facila a evenimentelor de audit. Cautarile trebuiesc sa poata fi salvate si rulate la o data ulterioara, respectiv sa poata fi integrate ca obiecte de tip widget in panoul de afisare central; * Solutia trebuie sa permita agregarea, corelarea si cautarea unor colectii de evenimente din sisteme si aplicatii diferite ce fac insa parte dintr-o singura tranzactie/set de tranzactii (evenimente ce sunt generate de o actiune/un set de actiuni de un anumit tip insa la indeplinirea lor se genereaza evenimente de audit intr-un set larg de echipamente, sisteme si aplicatii – Ex.: Trimiterea unui e-mail, plasarea unei comenzi intr-un site web, plasarea unui apel de video-conferinta, etc); * Solutia trebuie sa permita afisarea interactiva a rezultatelor cautarii datelor de audit, cu posibilitatea de a mari/micsora in timp real perioada de timp, pentru a identifica tendinte, varfuri si anomalii ale datelor analizate. Trebuie sa includa posibilitatea de a face “drill-down” asupra reprezentarilor grafice a evenimentelor de audit pentru a afisa direct datele in format brut ce au generat respectivele grafice, respectiv posibilitatea de a defini afisari customizate pentru oricare set de date; * Solutia trebuie sa ofere posibilitatea de esantionare a seturilor de date de audit, astfel incat sa permita regasirea si analiza rapida a datelor relevante la termenii de cautare folositi; * Solutia trebuie sa permita corelarea evenimentelor complexe din seturi de date foarte mari, respectiv dintr-un numar foarte mare de surse (sisteme, aplicatii, servicii, etc) pentru evenimente de audit ce aparent nu au nici o legatura evidenta. Corelarea trebuie sa se faca cel putin in functie de: timp, locatia geografica, tranzactii, cautarea subsecventa in rezultatele regasite, cautarea bazata pe campuri, alipiri ale termenilor de cautare, etc); * Solutia trebuie sa permita adnotarea evenimentelor de audit pentru a adauga context suplimentar de corelare; * Solutia trebuie sa permita detectia modelelor relevante indiferent de sursa si tipul datelor de audit; * Solutia trebuie sa permita folosirea a diferite seturi de date (modele de date pentru a descrie relatiile dintre evenimentele de audit, tabele pentru afisarea structurata a datelor complexe de audit, “lookups” pentru extinderea si imbogatirea datelor de audit prin integrari cu surse externe de date) pentru a defini si mentine colectii structurate a datelor ce pot fi folosite/refolosite in constructia modelelor de analiza si raportare; * Posibilitatea de a crea afisari pe baza de tabele, afisari ce permit imbunatatirea, rafinarea, filtrarea si agregarea datelor de audit. Afisarile vor putea fi exportate si partajate cu alti utilizatori ai solutiei, respectiv vor permite crearea de rapoarte si elemente in panoul centralizat de afisare; * Solutia va permite generarea de afisari personalizate a tabloului de bord (dashboard) pentru tulizatori diferiti ai solutiei, respectiv va permite generarea, exportul si distributia de rapoarte personalizate cel putin in format PDF; * Solutia va permite folosirea de reprezentari grafice de tip chart predefinite, pentru a reprezenta datele de audit corelate, respectiv va permite definirea de noi vizualizari grafice ce vor putea fi partajate cu alti utilizatori ai solutiei; * Solutia va permite definirea de alerte pentru evenimentele de audit critice, alerte ce vor putea declansa actiuni sau seturi de actiuni de alertare a utilizatorilor solutiei (alertare prin e-mail, SNMP, executarea scripturilor de remediere, etc). Alertele vor fi personalizabile si vor putea fi definite cel putin in functie de: limite variabile realtiv la datele de audit, tendintele evenimentelor de audit, modele complexe de corelare a evenimentelor de audit (ex: atacuri de forta bruta, scenarii de frauda, etc); * Solutia va permite integrarea nativa cu aplicatii terte prin intermediul unui API ce exporta intregul set de functionalitati, respectiv prin conexiune directa de tip ODBC; * Solutia va permite integrarea nativa cu sisteme de tip Hadoop, oferind mecanisme integrate de import bi-directional si cautare in seturile de date de audit; * Solutia va permite extinderea functionalitatilor prin aplicatii terte, nativ compatibile, aplicatii ce se vor instala ca module in solutia ofertata; |
| Management | * Solutia va permite nativ definirea de utilizatori locali si roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile actiunilor administrative si/sau seturilor de date. Deasemenea trebuie sa permita integrarea cu un sistem director de tip LDAP (Active Directory, Sun e-Directory, etc) pentru sincronizarea utilizatorilor si a drepturilor de acces, respectiv cu sisteme Single Sign-On in tehnologie SAML (Okta, Ping Federate, Azure AD, CA SiteMinder, OneLogin, etc). Pentru sporirea securitatii in mecanismele de autentificare, platforma trebuie sa permita integrarea cu un sistem NTP/SNTP pentru sincronizarea informatiilor de timp; * Solutia va oferi acces securizat prin HTTPS (TLS), respectiv prin protocol SSH; * Solutia va oferi un panou central de monitorizare a modulelor si componentelor (afisari ale topologiei, starea generala a sistemului, starea individuala a componentelor cu posibilitati de alertare, performanta si capacitatea sistemului, interconectarea componentelor sistemului, etc); |
| Garanţie si suport | * Solutia va include garantie de minim 36 de luni. Suportul si garantia trebuie asigurate in Romania de producatorul respectivei solutii sau prin partener autorizat; * Se va asigura acces 24x7 in centrul de suport al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora in functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri software. |

* + - 1. Componenta portal

Componenta Portal ce va asigura interacţiunea utilizatorilor externi cu Buletinul Electronic al Registrului Comertului trebuie să respecte următoarele cerinţe tehnologice:

* Va oferi suport pentru tehnologii şi standarde deschise;
* Va oferi suport multi-lingvistic pentru prezentare;
* Va oferi suport multi-home pentru instalarea de servere multiple pe aceeaşi maşină fizică;
* Va fi compatibilă cu standardele platformei Java 2 Enterprise Edition (J2EE) sau echivalentă;
* Va oferi Portleţi predefiniţi care să permită gestiunea publicarii de pagini web, gestiunea de documente, gestiunea de formulare web,etc ;
* Va oferi suport multi-site, multi-portal pentru aplicaţii distincte instalate pe aceeaşi maşină fizică;
* Va furniza un unic punct de acces către aplicaţiile şi serviciile electronice din sistem;
* Accesul la continut se va face printr-un navigator Web de tip Internet Explorer, Mozilla Firefox, Safari, Chrome sau echivalent;
* Va oferi o vedere unică, consistentă asupra unei game variate de surse de informaţii şi in concordanţă cu acţiunile pe care utilizatorul le are de realizat;
* Interfaţa prezentată utilizatorului după autentificare va conţine modalităţile de acces strict legate de aplicaţiile la care utilizatorul are drepturi de acces în funcţie de drepturile acordate;
* Conţinutul accesat va fi automat ajustat, pe baza rolurilor predefinite ale utilizatorilor în funcţie de drepturile acordate;
* Sa includa suport pentru integrarea cu sistemul de gestiune a identitatii utilizat in cadrul ONRC (Oracle Access Manager);
* Sa includa suport pentru autentificare prin LDAP, producator SAML si consumator OAuth;
* Interfaţă web standardizată, simplă şi intuitivă;
* Interfaţă cu utilizatorii bogată în funcţionalităţi, care să ofere un nivel ridicat de accesibilitate, conform cu cerinţele de accesibilitate WCAG versiunea 1.0 sau echivalente;
* Interfaţă web cu template disponibil gratuit pentru look & feel comun organizaţiei;
* Grad ridicat de securitate a sistemului, care va garanta confidenţialitatea şi securitatea datelor utilizatorilor pentru accesul neautorizat atăt dinafară cât şi din interiorul sistemului;
* Serviciile şi extensiile vor fi modulare şi vor permite dezvoltarea ulterioară de noi functionalităţi;
* Soluţia de federalizare de conţinut va oferi suport pentru WSRP 1.0 si 2.0 sau echivalent;
* Administrarea şi configurarea componentei se va putea realiza facil, utilizând doar un browser web;
* Va conţine un motor de căutare performant, care va permite efectuarea de interogări în toate sursele de informaţii prezente în mediul portal;
* Soluţia de portal va oferi un motor de căutare avansat, care să permită utilizarea unor criterii de relevanţă pentru obţinerea rapidă a informaţiilor căutate;
* Motorul de căutare va include mecanisme de învăţare pe baza căutarilor deja efectuate pentru strângerea informaţiilor referitoare la relevanţă;
* Motorul de căutare va include capabilităţi de căutare în cadrul documentelor XML;
* Motorul de căutare va permite utilizarea expresiilor booleene în cadrul căutărilor;
* Motorul de căutare va permite căutarea de documente similare cu un anumit document dat;
* Motorul de căutare va oferi mecanisme de tip proximitate pentru regăsirea mai uşoară a informaţiilor căutate;
* Va îmbunătăţi experienţa utilizatorilor prin utilizarea unor tehnologii bazate pe Web 2.0 şi AJAX sau echivalente;
* Va oferi acces către toate resursele prezente în cadrul interfeţei consolidate printr-o singură autentificare, la deschiderea sesiunii;
* Componenta de portal va oferi suport pentru standardele deschise JSR 168, JSR 286 sau echivalente, standarde ce permit publicarea de portleţi moderni şi uşor de construit;
* Va include suport pentru standardul JSR 170 sau echivalent, în vederea administrării şi gestionării elementelor de conţinut;
* Soluţia oferită va asigura suport pentru standardul deschis JSF sau echivalent;
* Posibilitatea de a avea portleţi obligatorii în secţiuni predefinite şi portleţi selectabili de către utilizatori;
* Suport pentru monitorizarea activităţii (capturi de metrici, statistici, audit, etc.);
* Va oferi utilizatorilor versiuni diferite ale interfeţei consolidate în funcţie de tipul utilizatorului;
* Soluţia va oferi suport pentru RSS sau echivalent;
* Soluţia de portal va permite interfaţarea cu sisteme de content management precum: Oracle Webcenter Content, Microsoft Sharepoint, EMC Documentum si Alfresco sau echivalente;
* Soluţia de portal va oferi capabilităţi avansate pentru reunirea mai multor portaluri / aplicatii web într-o singură interfaţă, agregată;
* Servicii de Single Sign-On la nivelul tuturor informaţiilor prezentate în portal.
* Să permită rularea platformei de integrare pe distribuţiile majore de sisteme de operare prezente pe piaţă (cel putin Windows şi Linux).
* Componenta Portal va rula pe infrastructura de servere de aplicatie pusă la dispoziţie de componenta server de aplicatie.
* Să se integreze şi utilizeze mecanismele scalabilitate şi failover puse de dispoziţie de componenta server de aplicatie.
* Să existe posibilitatea de a utiliza de mecanisme de clustering, balansare.
* Sa includa pe durata garanției servicii de suport si mentenanta software de la producator

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta server de aplicatie

În arhitectura n-tier, serverul de aplicaţii este cel care expune nivelul logic şi procesele de business, pentru a fi accesate/utilizate de către celelalte aplicaţii/componente.

Caracteristicile tehnice ale serverului de aplicaţii sunt următoarele:

* Compatibil cu specificaţiile platformei Java Enterprise Edition 7 sau echivalent;
* Platformă tehnologică completă pentru instalarea şi execuţia site-urilor web dinamice, serviciilor web şi aplicaţiilor JEE sau echivalent;
* Suport complet pentru specificaţiile Java Servlets 3.1 sau echivalent;
* Suport complet pentru specificaţiile JavaServer Pages 2.3 sau echivalent;
* Suport complet pentru specificaţiile Enterprise JavaBeans 2.0, 2.1, 3.0, 3.1, 3.2 sau echivalent;
* Suport pentru servicii web conform specificaţiilor WS-I Basic Profile 1.1, 1.2 şi 2.0 sau echivalent;
* Suport complet pentru servicii web utilizând specificaţiile JAX-WS 2.2 şi JAX-RPC 1.1 sau echivalent;
* Suport pentru Simple Object Access Protocol (SOAP) versiunile 1.1 si 1.2 şi SOAP with Attachments API for Java (SAAJ) sau echivalent;
* Transformarea datelor în format XML utilizând standardul W3C Extensible Stylesheet Language (XSL) sau echivalent;
* Securizarea serviciilor web utilizând standardele WS-Security şi WS-SecurityPolicy sau echivalente;
* Suport complet pentru standardul Java Database Connectivity (JDBC) sau echivalent;
* Suport pentru conectarea la multiple sisteme de gestiune a bazelor de date relaţionale;
* Suport complet pentru standardul Java Messaging Service (JMS) versiunile 2.0 sau echivalent;
* Suport complet pentru managementul tranzacţiilor utilizând specificaţia Java Transaction API (JTA) versiunile 1.2 sau echivalente;
* Implementare proprie pentru specificaţia Java Persistence API (JPA) sau echivalentă, cu suport pentru Enterprise Java Beans (EJB) sau echivalent;
* Cache-ul de date distribuit va oferi mecanisme de acces concurent la date si participare în tranzacţii distribuite;
* Va implementa mecanisme avansate de caching;
* Va oferi un mediu de execuţie a aplicaţiilor Java critice cu cerinţe de procesare în timp real;
* Va asigura mecanisme de grupare a serverelor în clustere de servere de aplicaţii atât în topologii de tip activ-activ cât şi activ-pasiv;
* Va permite stoparea temporară a unui nod din cluster pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale;
* Va asigura mecanisme de balansare dinamică a încărcarii sistemului între resursele administrate în cadrul aceluiaşi cluster;
* Server web integrat care sa permita inclusiv acoperirea stratului arhitectural din zona DMZ;
* Va oferi mecanisme de cache pentru optimizarea accesului la conţinutul stocat.
* Va permite rularea serverului de aplicaţii pe distribuţiile majore de sisteme de operare prezente pe piaţă (cel putin Windows şi Linux).

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de integrare a aplicatiilor

În secţiunea „Interconectarea cu sistemele existente interne şi externe” a prezentului document sunt descrise modalităţile de interconectare a platformei pentru Buletinul Electronic al Registrului Comerţului cu alte sisteme. Din punct de vedere tehnic, pentru realizarea acestei interconectări, se va utiliza o componentă de integrare ce va oferi suport pentru:

- modelarea şi execuţia proceselor de afaceri rezultate ca urmare a orchestrării de servicii standard reutilizabile;

- integrarea sistemelor informatice utilizând o soluţie de tip magistrală de mesaje (Service Bus) cu capabilităţi extinse de conectare la soluţii tehnologice eterogene;

- monitorizarea proactivă a fluxurilor în execuţie prin accesul direct, sub forma de tablouri de control, la indicatorii cheie de execuţie;

- capturarea şi tratarea de evenimente provenite din surse diferite;

- securizarea accesului la serviciile şi fluxurile modelate pe baza unor politici de acces definite şi administrate centralizat.

Din punct de vedere tehnic/tehnologic această platformă de integrare prezintă următoarele caracteristici:

- Va oferi suport complet pentru dezvoltarea, testarea, execuţia, monitorizarea, optimizarea şi administrarea proceselor de integrare;

- Va oferi suport pentru soluţii moderne şi deschise de integrare conform principiilor şi conceptelor arhitecturilor Service Oriented Architecture (SOA) şi Event Driven Architecture (EDA);

- Va fi bazată pe standardele deschide de interoperabilitate a aplicaţiilor WS-I Basic Profile, WSDL (Web Services Description Language), WS-\*, XML, SOAP sau echivalente;

- Va permite modelarea declarativă a proceselor de integrare utilizând standardul OASIS (Organization for the Advancement of Structured Information Standards) BPEL (Business Process Execution Language);

- Va permite comunicaţii sincrone şi asincrone inter-aplicaţii;

- Va oferi mecanisme transparente de persistenţă a stării proceselor şi informaţiilor de audit într-o bază de date relaţională;

- Va permite folosirea canalelor de notificare moderne (email, SMS) pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicaţii;

- Va suporta transformări şi manipulări de date complexe pentru implementarea logicii proceselor de business;

- Sistemul va include capabilităţi extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL), XPath şi XQuery sau echivalente;

- Va oferi soluţii de conectare predefinite la principalele tipuri de tehnologii: baze de date relaţionale, cozi de mesaje (JBossMQ, Oracle AQ, IBM Websphere MQ, MSMQ sau echivalente), sisteme de fişiere, etc;

- Va oferi un cadru de dezvoltare pentru noi soluţii de conectare la sisteme externe bazat pe standarde deschise;

- Va oferi servicii de transport cu suport pentru persistenţa datelor;

- Va oferi servicii de transport cu suport pentru garantarea livrării datelor;

- Va include o soluţie de tipul monitorizare a activităţii de afaceri - Business Activity Monitoring (BAM) sau echivalentă;

- Va permite monitorizarea în timp real a indicatorilor de tipul Key Performance Indicators (KPI) sau echivalentă;

- Va permite monitorizarea în timp real a SLA-urilor (Service Level Agreement) de business sau operaţionale;

- Va oferi un modul centralizat de gestiune şi aplicare a politicilor de securitate peste portofoliul de fluxuri electronice instalat;

- Va oferi servicii de securitate la nivel de aplicaţie;

- Pentru asigurarea securităţii la nivel transport, soluţia va permite utilizarea protocolul Secure Socket Layer (SSL) şi a certificatelor compatibile X.509;

- Va permite implementarea de servicii de securitate specifice lucrului cu serviciile web standard:

o autentificarea accesului la servicii;

o autorizarea accesului la servicii;

- Soluţia va fi bazată pe standardele deschise de securitate a serviciilor web, precum WS-Security, WS-Policy and WS-Security Policy, Security Assertation Markup Language (SAML) sau echivalente;

- Soluţia va putea securiza totalitatea apelurilor către serviciile existente printr-un mod de funcţionare de tip poartă de acces (gateway) fără să fie necesară modificarea proceselor instalate;

- Să ofere mecanisme de grupare a serverelor în clustere pentru toate componentele platformei de integrare atât în topologii de tip activ-activ cât şi activ-pasiv;

- Posibilitatea stopării temporare a unui nod din cluster pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale;

- Mecanisme de balansare a încărcarii sistemului între resursele administrate în cadrul aceluiaşi cluster;

- Mecanisme de scalare a sistemului pe orizontală (Scale Out).

- Va permite rularea serverului de aplicaţii pe distribuţiile majore de sisteme de operare prezente pe piaţă (cel putin Windows şi Linux);

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de integrare a datelor

Se doreşte includerea in sistemul informatic a unei componente de integrare şi consolidare oferind următoarele module de bază:

* replicare de date între surse eterogene de informaţii
* tranformare date (ETL) din surse eterogene, prin:
  + modelare declarativă a fluxurilor de integrare de date;
  + sincronizare de date între surse eterogene de informaţii.

Replicarea datelor intre Baza de date operationala existenta (baza de date de productie a sistemelor RC, RL si BPI) si baza de date a Buletinului Electronic al Registrului Comertului. Rolul acestei componente este de a capta modificările aparute in baza de date sursa si de a le transfera catre modulul de Transformare date, in vederea modificarii structurilor de date si/sau a campurilor si aplicarii acestora in baza de date destinatie.

Modulul **Replicare Date** va oferi suport tranzactional astfel incat sa nu se propage in bazele de date destinatie tranzactii incomplete, in cazul aparitiei unei erori in baza de date sursa. Captarea datelor modificate in baza de date sursa se va face prin mecanisme care nu au impact asupra performanta acesteia. Se accepta mecanisme de captare a modificărilor bazate pe log-ul tranzacțional al bazei de date. Nu se accepta mecanisme ce presupun definirea de trigger-i pe tabelele bazei de date.

Funcționalitățile majore pe care trebuie sa le asigure modulul **Replicare date** sunt:

* posibilitatea de replicare intre sistemul de gestiune a bazelor de date existent (Oracle) si Componenta de gestiune baze de date din cadrul noului sistem informatic;
* replicarea se va baza pe mecanisme ce nu impacteaza performanta bazelor de date, cum ar fi log-ul tranzactional al bazei de date;
* posibilitatea de replicare bi-directionala inte baze de date Oracle;
* soluția trebuie să permită replicare de tabele, secvente oracle, precum și comenzi DDL.
* soluția trebuie să permită replicarea întregii baze de date, sau a unui set de tabele, sau chiar a unei singure tabele. De asemenea să permită doar replicarea unui subset din coloanele, sau rândurile tabelei. Această funcționalitate este esențială având în vedere specificul replicărilor necesare în cadrul proiectului, unde se vor replica doar acele înregistrări necesare subsistemului Buletinul electronic al Registrului Comertului.
* soluția trebuie să funcționeze cu variantele de bază de date Oracle din sistemul informatic integrat existent;
* soluția trebuie să aplice în timp real modificările în baza de date destinație, întârzierea între sursă și destinație să fie minimă.
* soluția trebuie să fie capabilă să replice baze de date configurate atât în mod arhivare cât și baze de date aflate în NONARCHIVE mode.
* soluția trebuie să păstreze bazele de date destinație deschise astfel încât poată fi utilizate pentru operațiunile curente specifice aplicațiilor care rulează pe aceste baze de date.

Modulul de **Transformare date** are ca scop asigurarea instrumentelor/funcționalităților de transformare a datelor cadrul sistemului nou creat. Acesta va oferi funcționalități de extragere date (din sursa de date), transformări ale acestora și încărcare în destinație, și va fi folosit pentru transferuri programate ale datelor, spre deosebire de instrumentul de replicare care va fi folosit pentru replicarea continuă a datelor.

Modulul de **Transformare date** va răspunde următorului set de cerinţe tehnice:

* Va putea accesa şi integra date din baze de date pe tehnologii diferite: Oracle, Fox Pro, Microsoft SQL Server, MySQL, IBM DB2, etc, şi să ofere suport pentru accesarea datelor din date aflate în fişiere (.txt, .csv, etc);
* Va permite configurarea surselor de date de tip bază de date cu suport cel puțin pentru baza de date Oracle Database și pentru baza de date ofertată.
* Va avea suport pentru protocoale de transport cel puțin HTTP și dar altele precum JMS sau echivalent.
* Va avea suport pentru JSON/XML.
* Va avea suport pentru transformarea datelor folosind operatori aritmetici, condiționali, modificări șir de caractere, etc.
* Va avea suport pentru planificarea execuției unor acțiuni la momente de timp definite.
* Va avea suport pentru monitorizarea rulării instrumentului.
* Va functiona in arhitectura cluster pentru asigurarea unei disponibilitati ridicate.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de gestiune documente

Componenta va respecta urmatoarele cerinte:

* Ofera capabilităţi de management al continuţului nestructurat;
* Functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* Permite definirea securitatii (drepturilor de acces) pentru roluri, foldere si documente.
* Gestioneaza documentele, precum şi metadescriptorii asociaţi acestora;
* Va permite crearea automata de structuri de foldere in functie de valori ale metadatelor documentelor;
* Permite incarcarea de documente in depozitul de documente cel putin prin urmatoarele modalitati:
  + drag & drop,bulk upload,copy & paste in windows explorer,
  + monitorizare casuta de email si incarcare directa in depozitul de documente a tuturor fisierelor atasate care se trimit la acea casuta de email, fara nici o interventie umana
* Permite utilizatorilor adaugarea de metadate speciale in afara de cele standard ale tipului de document, metadate valabile doar pe acea instanta de document;
* Conţine un set de metadescriptori predefiniţi asociaţi unui document;
* Ofera posibilitatea de a adăuga noi metadescriptori si taguri pentru cautare pe document;
* Permite organizarea colecţiilor de documente într-o structură ierarhică în conformitate cu schemele de indexare care se vor stabili în etapa de analiza;
* Nu va impune şi nu va limita prin arhitectură sau prin implementare, numărul de documente care se pot adăuga in depozitul de documente;
* Permite gestiunea oricarui tip de documente;
* Permite accesul utilizatorilor printr-o interfata web a componentei
* Permite deschiderea, salvarea si popularea metadatelor pe fisiere direct din aplicatiile office (de ex. word, excel, powerpoint)
* Interfetele web ale componentei trebuie sa fie disponibile utilizatorilor si administratorilor in limba Romana
* Permite conversia automată a documentelor de tip MS Office sau OpenOffice în formate web (HTML, PDF), pentru o publicare facilă a acestora;
* Permite adăugarea de note, adnotări pe document;
* Permite accesarea funcţionalităţilor platformei prin intermediul unor API şi servicii web;
* Permite versionarea documentelor (fara vreo limitare privind numarul acestora);
* Permite blocarea/deblocarea documentelor (check-in/check-out);
* Include un instrument avansat de căutare care va permite efectuarea de interogări atât asupra metadatelor ce însoţesc un document cât şi asupra conţinutului documentului respectiv şi să afişeze rezultatele într-o interfaţă de tip web-browser;
* Permite căutari de tip Fuzzy Search sau echivalent, bazate pe textul introdus de utilizator;
* Asigura regăsirea documentelor de către mai mulţi utilizatori simultan;
* Va utiliza componenta de gestiune a bazelor de date oferită pentru stocarea metadatelor asociate documentelor;
* Permite ca optiuni de stocare a conţinutului nestructurat în componenta de gestiune a bazelor de date oferită si in sistemul de fisiere;
* Permite integrarea şi utilizarea de mecanisme de clustering, balansare, scalabilitate şi failover puse de dispoziţie de componenta server de aplicaţii ofertata;
* Permite integrarea cu LDAP si Active Directory pentru autentificarea utilizatorilor
* Permite expunerea de conţinut catre componenta Portal, pentru toti utilizatorii acesteia, fara a necesita costuri suplimentare pentru beneficiar;
* Permite rularea pe distribuţiile majore de sisteme de operare prezente pe piaţă (cel putin Windows si Linux).

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de procesare OCR

Componenta de procesare OCRva asigura conversia documentelor intrate in ONRC cu scopul de a fi publicate in Buletinul Electronic al Registrului Comertului, printr-un proces de recunoaștere optica a caracterelor. Serverul OCR va permite conversia automata, in bloc, a documentelor salvate in depozitele de date cu diferite formate.

Componenta de procesare OCR va respecta urmatoarele cerinte:

* Functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* Permite procesare OCR pentru toate limbile europene (inclusiv limba romana)
* Permite recunoasterea codurilor de bare, cel putin: Check Code 39, Code 128, PDF 417, Data Matrix, QR Code, Check Interleaved 2 of 5
* Suporta un numar mare de formate de fisiere de intrare, printre care: JPEG, JPEG2000, JBIG2, PDF, HTML, PNG, DOC, DOCX, XLSX, PNG, BMP, GIF, PCX, DCX, TIFF multipagina (compresie cel putin CCITT4, JPEG, LZW si ZIP)
* Suporta cel putin urmatoarele formate de iesire: PDF, PDF/A, RTF, DOC, DOCX, TXT, HTML
* Pune la dispozitie in mod nativ functionalitatile de procesare OCR prin urmatoarele modalitati: foldere de filesystem monitorizate, foldere FTP monitorizate, casute email monitorizate, servicii web sau conectori specializati pentru integrarea cu sisteme de gestiune continut.
* Are o arhitectura scalabila cu distribuirea automata a incarcarii si procesare paralela astfel incat sa foloseasca la maxim capacitatea de procesare existenta
* Dispune nativ de mecanisme de balansare a incarcarii si procesarii documentelor intre mai multe servere

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de dezvoltare aplicatii mobile

Platforma de dezvoltare aplicatii mobile va respecta urmatoarele cerinte:

* Sa permita scrierea de aplicatii o data si sa poata rula pe oricare din dispozitivele mobile importante (iOS, Android, Windows).
* Sa foloseasca tehnologii web (HTML, CSS, Javascript) in procesul de dezvoltare aplicatii mobile
* Sa detina un nivel ridicat de flexibilitate in ceea ce priveste proiectarea interfetei utilizator (paleta , liste, navigare pagini, tab-uri, larga de culori, butoane, meniuri derulante, formulare de introducere date, etc)
* Sa permita testarea aplicatilor pe baza de simulatoare incluse in platforma si cu browsere mobile (de ex. Safari pentru iOS)
* Se asigure acces la functionalitati importante din sistemul de operare in care aplicatia va rula precum: baterie, camera, localizare, acces la log-uri, etc. Sa permita dezvoltarea de plugin-uri pentru acoperirea accesului la functionalitati native.
* Sa detina o comunitate larga de dezvoltatori
* Sa detina un kit de dezvoltare software orientat catre dezvoltarea de aplicatii cu un nivel ridicat de interactivitate

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de gestiune baze de date

Sistemul de gestiune a bazelor de date va respecta următoarele cerinţe:

* Sa fie un sistem de gestiune a bazelor de date de tip relaţional;
* Sa utilizeze limbaj standard SQL pentru manipularea datelor (cel puțin SELECT, UPDATE, DELETE)
* Sa utilizeze limbaj standard pentru definire (cel puțin CREATE, ALTER, DROP, RENAME)
* Sa permita View-uri / View-uri materializate pentru tabele sau mecanisme similare
* Sa permita diverse tipuri de date printre care cel puțin: întregi, boolean, șir de caractere de mărime fixă și de mărime variabilă, numere în virgulă flotantă, date binare de mărime fixă și de mărime variabilă, JSON sau similar, dată și timp;
* Sa permita minim 250 coloane într-un tabel;
* Sa permita funcții tip fereastră (cel puțin RANK, DENSE\_RANK, LEAD, ROW\_NUMBER)
* Sa permita indecși de tip primar, coloană unică și multi-coloană;
* Sa permita partiționare pentru date și indecși
* Sa permita importul şi exportul de date în formate de date general acceptate;
* Sa permita minimizarea conflictelor de acces la date;
* Sa ofere suport pentru proceduri stocate şi triggeri;
* Sa ofere suport pentru tranzacţii autonome;
* Sa permita partiţionare logică a tabelelor mari în scopul reducerii timpului de acces la date după diverse criterii de partiţionare (list, range, hash);
* Sa ofere suport pentru Unicode UTF-8;
* Sa ofere suport de replicare bidirecţională a datelor între două instanţe ale bazei de date;
* Sistemul va asigura o disponibilitate 100% pentru utilizatori, în cazul apariţiei unei defecţiuni hardware la unul din serverele cluster-ului;
* Sistemul de gestiune a bazelor de date relaţional (SGBDR) va asigura balansarea încărcării între noduri la nivelul cererilor şi execuţiilor pe baza de date aflată în cluster;
* Sa ofere mecanisme de control şi blocare la nivel de înregistrare şi mecanisme de asigurare a consistenţei la citire, pentru a permite accesul în mod concurent al utilizatorilor la date;
* Sa permita restricţionarea accesului la nivelul obiectelor bazei de date;
* Sa permita instalarea unei singure baze de date pe mai multe noduri (arhitectură de tip cluster activ-activ) pentru a asigura toleranţă la defecte hardware sau nefuncţionare planificată, scalabilitate şi disponibilitate crescută a sistemului;
* Va oferi posibilitatea de a limita numărul de conexiuni la baza de date prin folosirea unui mecanism de tip database connection pooling;
* Va oferi un utilitar grafic pentru administrarea si monitorizarea SGBDR;
* Baza de date relaţională va avea componente pentru optimizarea interogărilor;
* Va exista posibilitatea de a cripta tot traficul de reţea dinspre şi către baza de date;
* Va permite stoparea temporară a unui nod pentru mentenanţă, suport, upgrade sistemul în acest timp să rămână disponibil;
* Stocare criptată a datelor în baza de date în mod transparent faţă de aplicaţie, fără a fi necesară scrierea de cod în aplicaţie pentru a se cripta şi decripta datele stocate în baza de date;
* Va permite rularea pe distribuţiile majore de sisteme de operare prezente pe piaţă (cel putin Windows si Linux).

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de gestiune a proiectelor

Componenta propusa va respecta următoarele cerinţe:

* Functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* permite planificarea si urmarirea proiectelor (inclusiv a celor de dezvoltare software)
* permite planificarea si urmarirea muncii membrilor echipei la nivel granular inclusiv distribuirea sarcinilor pentru acestia
* permite rularea de rapoarte predefinite si crearea de noi rapoarte.
* permite urmarirea sarcinilor
* permite atasarea de informatii conexe sarcinilor, cum ar fi comentarii, statusuri, atasamente
* permite monitorizarea performantei in cadrul unui tablou de bord
* permite gruparea sarcinilor in proiecte si crearea de sub-sarcini
* include sabloane de proiecte
* include functionalitati de cautare rapida si filtrare customizata
* ofera suport pentru REST sau Java APIs
* permite integrarea cu un serviciu director de tip LDAP
* permite afisarea informatiilor despre sarcini intr-un tablou de bord
* permite ca unui utilizator sa i se poata asigna un rol intr-un proiect sau rezolvarea unei sarcini
* permite managementul portofoliului de proiecte si al fluxurilor de lucru
* permite folosirea de formulare pentru colectarea informatiilor
* permite crearea unui colector de cerinte pentru captarea informatiilor din formularele de feedback incorporate in web site-uri
* permite integrarea cu componenta de gestiune a ciclului de viata a aplicatiilor
* include un designer de fluxuri de lucru
* permite trimiterea automata de notificari in cazul schimbarii statusului unei sarcini

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de colaborare a echipelor

Componenta propusa va respecta următoarele cerinţe:

* functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* va permite crearea de pagini diverse, pentru planuri de proiect, minutele intalnirilor, cerinte de produs etc.
* va permite alocarea de sarcini utilizatorilor
* va permite adaugarea de comentarii la nivel granular pentru pagini si fisiere atasate
* va permite versionarea automata a documentelor
* va permite accesarea folosind clienti de tip desktop sau pentru dispozitive mobile si interfata va fi adaptata in functie de tipul clientului
* va permite organizarea in spatii de lucru
* va oferi posibilitatea de creare bloguri si discutii ce pot include comentarii, mentiuni de tip @ si aprecieri
* va include sabloane de tip cele mai bune practici pentru a genera rapid pagini
* va oferi posibilitatea de abonare la continut prin notificari pe email sau de tip RSS
* va permite acordarea de permisiuni la nivel granular, pentru pagini individuale, la nivel de spatiu de lucru si la nivel global
* va permite integrarea cu Microsoft Office pentru editarea de pagini
* va include un editor de tip "rich text" cu posibilitate de "drag and drop" pentru atasamente si short-cut-uri pentru tastatura
* va include functionalitati de cautare rapida si cautare completa
* va oferi suport pentru limba romana
* va permite crearea unei baze de date de cunostinte
* va contine un spatiu de lucru pentru colectarea si organizarea cererilor si raspunsurilor pe diverse topicuri, creand astfel o baza de date de cunostinte
* va oferi suport pentru indexare si cautare, pentru gasirea cererilor si raspunsurilor cu usurinta
* va permite afisarea rezultatelor cautarii din mai multe surse (pagini, postari on bloguri, atasamente)
* va permite vizualizarea persoanelor care contribuie cel mai mult cu raspunsuri
* va avea o functie de gasire si afisare informatii similare din baza de date de cunostinte
* va propune un mecanism pentru identificarea informatiilor corecte
* va permite includerea in cereri/raspunsuri de continut media (imagini, video), text formatat, link-uri, cod sursa, etc.
* va oferi posibilitatea de informare pe e-mail in cazul aparitiei unor informatii de interes
* va permite restrictionarea accesului la nivel de grupuri
* va oferi statistici privind folosirea spatiului de lucru ce contine cereri si raspunsuri

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de gestiune a ciclului de viata al aplicatiilor

Componenta propusa va respecta următoarele cerinţe:

* functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* sa permita crearea de proiecte de dezvoltare software, planficarea si urmarirea acestora;
* sa permita inserarea de comentarii;
* sa ofere suport pentru roluri de utilizatori;
* sa permita gestionarea testarii;
* sa permita versionarea cerintelor;
* sa asigure suport pentru procesul de gestiune a calitatii software;
* sa permita integrarea cu medii de dezvoltare populare, cum ar fi: Eclipse, Visual Studio, Intelij, NetBeans;
* sa ofere suport pentru accelerarea ciclurilor de testare prin posibilitatea de planificare si rulare automata a testelor, prin integrare cu componenta de instalare si integrare continua a aplicatiilor;
* sa permita proiectarea cu usurinta a rapoartelor si a tablourilor de bord pe baza datelor proiectului;
* sa gestioneze multiple tipuri de cerinte si va permite trasabilitatea intre cerinte, teste, defecte, modificari de cod sursa si sistemele de construire a release-ului.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de instalare si integrare continua a aplicatiilor

Componenta propusa va respecta următoarele cerinţe:

* functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* va oferi suport pentru o gama larga de limbaje de programare si pentru alte tehnologii populare precum AWS CodeDeploy, Docker și Amazon S3
* va dispune de agenti dedicati pentru rezolvarea erorilor critice
* va oferi suport pentru peste 50 de agenti pentru a rula loturi de teste in paralel
* va oferi posibilitatea de alocare permisiuni per mediu de lucru
* va oferi posibilitatea de blocare in carantina a testelor care nu functioneaza corect
* va oferi un proces automat de dezvoltare si testare software care nu depinde de un mediu local specific
* va oferi suport pentru REST APIs
* va permite ca testele de integrare sa fie declanșate automat dupa ce dezvoltatorii comit codul (integrare continua)
* va suporta optimizarea performantei dezvoltarii de software prin folosirea paralelizarii
* va permite gestionarea lansarii de versiuni software
* va permite rularea de teste automate in paralel
* va permite criptarea datelor in tranzit
* va permite criptarea credentialelor in baza de date si in backup-uri
* va permite rularea pe toate distribuţiile majore de sisteme de operare prezente pe piaţă: Windows si Linux.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de testare automata a aplicatiilor

Componenta propusa va respecta următoarele cerinţe:

* functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* permite folosirea unui limbaj de programare standard (Javascript, Vbscript, Jscript, Python) pentru crearea de teste pe interfata utilizator sau imbunatatirea inregistrarilor testelor existente;
* permite convertirea facila in script-uri a testelor inregistrate in interfata grafica utilizator;
* dispune de un mediu de testare built-in;
* permite rularea de teste de tip cross-browser;
* permite rularea unui test automatizat pe mai multe editii si versiuni de browsere, suportand browserele majore existente pe piata;
* permite automatizarea testarii functionale pentru multiple tehnologii desktop (de exemplu Windows / Java / .NET / Oracle Forms);
* permite separarea datelor de comenzile de test si modificarea datelor de intrare pentru largirea ariei de testare;
* contine o platforma de testare completa si integrata, atat pentru testarea desktop cat si pentru cea a aplicatiilor mobile si web.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

* + - 1. Componenta de testare de performanta a aplicatiilor

Componenta propusa va respecta următoarele cerinţe:

* functionalitatile trebuie sa fie disponibile nativ (out-of-the-box) la nivelul componentei ofertate, fara a fi necesare dezvoltari suplimentare pentru acoperirea cerintelor.
* ofera suport pentru cele mai recente tehnologii web, cel putin pentru: HTML5, WebSocket si Oracle Forms;
* permite, pentru crearea testelor, designul acestora fara a fi necesare scripturi;
* ofera suport pentru programarea vizuala a testelor;
* permite crearea de reguli pentru extragerea datelor variabile din pagini;
* suporta cel putin SSL, Kerberos, NTLM si autentificari de tip Basic, Digest sau folosind certificate client;
* permite inregistrarea aplicatiilor mobile (cu browser de tip nativ, hibrid sau mobil) direct, de pe orice dispozitiv mobil;
* permite adaugarea/eliminarea de utilizatori virtuali in timpul executiei testelor;
* ofera suport pentru o gama larga de produse software, incluzand insa nelimitandu-se la sisteme de operare, servere de aplicații, servere web, baze de date;
* permite monitorizarea fara agenti;
* ofera suport pentru GIT;
* ofera suport pentru testarea cel putin a aplicatiilor .NET si Java;
* permite rularea de teste de incarcare la nivelul API (SOAP, REST), la nivelul componentelor sau la nivelul microservicilor;
* permite analizarea performantei sistemului dupa rularea unui test pe baza datelor colectate din straturile arhitecturale relevante;
* permite rularea de rapoarte de analiza a performantei pe diferite nivele de detaliu (de tip sumar sau la nivel de tranzactie) si rapoarte pentru determinarea incadrarii performantei intr-un SLA predefinit
* Portabilitate: va permite rularea cel putin pe urmatoarele distribuţiile de sisteme de operare prezente pe piaţă: Windows si Linux.

Avand in vedere nevoia de disponibilitate ridicata a sistemului ce va fi implementat, solutia ofertata trebuie să includă accesul la update-uri si serviciile de suport ale producatorului (inclusiv pentru fix-uri, securitate si imbunatatiri) pe durata garanției echipamentelor hardware. Nu se accepta oferte care nu includ subscripție de la producator asigurată pe toată perioada de garanție a echipamentelor hardware.

### Dimensionarea subsistemelor tehnice

Subsistemele tehnice vor fi dimensionate astfel incat sa raspunda atat cerintelor cantitative mentionate pentru fiecare in parte cat si celor calitative.

La aceşti indicatori se vor adăuga în faza de analiză o serie de indicatori de performanţă suplimentari pentru evaluarea performanţelor soluţiei şi se vor defini valorile pentru aceştia.

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, unde, prin timp de răspuns se înțelege timpul scurs între lansarea unei cereri (de scriere sau de citire din baza de date) și momentul în care sistemul răspunde cererii respective și devine din nou disponibil pentru o nouă cerere.

* + - 1. Echipamente de tip șasiu modular

În configurația preconizată, soluția hardware va include 2 seturi (câte un set pentru fiecare site), iar fiecare set va include cel puțin 2 echipamente de tip șasiu modular pentru servere de tip blade.

Fiecare șasiu va fi echipat și configurat pentru a asigura cel puțin:

* 2 module interne de I/O tip port-extender sau fabric extender;
* 8 porturi 40Gbps uplink convergent către top-of-rack în fiecare modul de I/O;
* 4 module de racire / ventilare, în configurație redundată;
* 4 surse de alimentare, în configurație redundată.

Pentru fiecare din cele două site-uri, soluția preconizată va include cel puțin 1 echipament de tip rack (19in, min. 42RU înălțime, min. 80 cm lățime și min. 100 cm adâncime), ventilat pasiv și echipat pentru montarea și interconectarea echipamentelor de tip șasiu modular, precum și a tuturor celorlalte echipamente.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack a echipamentelor de tip șasiu modular, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Echipamente de interconectare privata LAN/SAN

În configurația preconizată, soluția hardware va include 2 seturi (câte un set pentru fiecare site), iar fiecare set va include cel puțin 2 echipamente de interconectare privată (de tip port sau fabric extender) convergentă LAN/SAN.

Fiecare echipament de interconectare privată (de tip port sau fabric extender) convergentă LAN/SAN va fi echipat și configurat pentru a asigura cel puțin:

* 16 porturi 10/40Gbps Ethernet cu interfețe modulare QSFP, din care 10 echipate cu transceiver optic SR;
* 4 porturi 8/16Gbps FC cu interfețe modulare SFP+, din care 4 echipate cu transceiver optic 16Gbps SR;
* 4 1/10Gbps Ethernet cu interfețe modulare SFP+, echipate cu transceiver optic 10Gbps SR.
* 2 module de racire / ventilare, în configurație redundată;
* 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Echipamente de procesare generală

În configurația preconizată, soluția hardware va include 12 seturi (8 seturi pentru site-ul principal, respectiv 4 seturi pentru site-ul secundar), iar fiecare set va include cel puțin un echipament de procesare generală de tip server ”blade”.

Fiecare echipament de procesare generală de tip server ”blade” va fi echipat și configurat pentru a asigura cel puțin:

* 2 procesoare fizice x86\_64 (sau echivalent) 2GHz / 16-core / 20MB cache fiecare;
* 128GB RAM DDR3 sau DDR4;
* 200GB Flash, capacitate dedicată instalării hipervizorului;
* 2 porturi CNA 40Gbps pentru conectarea la rețeaua locală LAN.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în șasiu, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Componenta de virtualizare generală

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia pe ansamblul resurselor de procesare, la nivelul de echipare efectivă a echipamentelor de procesare generală.

Licențierea funcționalităților solicitate va acoperi exploatarea concurentă a tuturor unităților de tip procesor multi-core instalate în toate echipamentele de tip server ”blade”, fără a introduce alte limitări (nici în legătură cu volumul de memorie activă instalată și nici cu volumul de stocare alocată local sau în sistemele specializate), avand incluse cel putin 2 instante de platforme de management centralizat.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de platformă de operare

În configurația preconizată, componenta va include 1 set de licente, dimensionate conform cerintelor din prezenta documentatie tehnica coroborate cu specificul/necesitatile fiecarui producator, pentru sustinerea unui numar nelimitat de masini virtuale la nivel de host, respectiv echipementele de procesare generala – cu suport pentru tehnologiile Vmware si Microsoft Hyper-V.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Echipamente de integrare LAN

În configurația preconizată, soluția hardware va include 2 seturi (câte un set pentru fiecare site), iar fiecare set va include cel puțin 2 echipamente de integrare LAN.

Fiecare echipament de integrare LAN va fi echipat și configurat pentru a asigura cel puțin:

* 48 porturi 1/10/25Gbps Ethernet cu interfețe modulare SFP+, din care 16 echipate cu transceiver optic 10Gbps SR și 4 echipate pentru conexiune 1Gbps, conectorizare electrică sau optică.
* 4 porturi 40Gbps Ethernet cu interfețe modulare QSFP, echipate cu transceiver optic SR;
* 2 module de racire / ventilare, în configurație redundată;
* 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Echipament de stocare de Tip 1

În configurația preconizată, soluția hardware va include 1 set (care va fi instalat în site-ul principal), iar fiecare set va include cel puțin 1 echipament de stocare consolidată unificată (SAN/NAS).

Fiecare echipament de stocare consolidată unificată (SAN/NAS) va fi echipat și configurat pentru a asigura cel puțin:

* 2 unități de tip controller, în configuratie redundantă;
* 4 porturi de 16Gbps FC per controller;
* 4 porturi de 10Gbps Ethernet per controller;
* 40TB capacitate utilă totală (fără a lua în calcul compresia sau deduplicare), din care 16TB pe suport Flash/SSD (prin utilizarea a cel puțin 8 unitati Flash/SSD) și 24TB pe suport SAS (prin utilizarea a cel puțin 16 unitati de disc SAS cu mecanica de 10K rpm;
* 2 module de racire / ventilare, în configurație redundată;
* 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Echipament de stocare de Tip 2

În configurația preconizată, soluția hardware va include 1 set (care va fi instalat în site-ul secundar), iar fiecare set va include cel puțin 1 echipament de stocare consolidată unificată (SAN/NAS).

Fiecare echipament de stocare consolidată unificată (SAN/NAS) va fi echipat și configurat pentru a asigura cel puțin:

* 2 unități de tip controller, în configuratie redundantă;
* 4 porturi de 16Gbps FC per controller;
* 4 porturi de 10Gbps Ethernet per controller;
* 20TB capacitate utilă totală (fără a lua în calcul compresia sau deduplicare), din care 8TB pe suport Flash/SSD (prin utilizarea a cel puțin 4 unitati Flash/SSD) și 12TB pe suport SAS (prin utilizarea a cel puțin 8 unitati de disc SAS cu mecanica de 10K rpm;
* 2 module de racire / ventilare, în configurație redundată;
* 2 surse de alimentare, în configurație redundată.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Componenta de monitorizare a dezvoltării și exploatării aplicațiilor

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia în mod concurent pentru cel puțin 24 de (instanțe de) aplicații respectiv instalate si licentiate pe cel putin 160 CPU-cores. Fiecare instanță de aplicație va fi considerată la nivel de mașină virtuală (JVM) sau la nivel de instanță O/S care găzduiește mediul virtual de runtime (.Net).

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de monitorizare a accesului la date

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia în mod concurent pentru cel puțin 22 instanțe de baze de date respectiv instalate si licentiate pe cel putin 176 CPU-cores.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de monitorizare a serviciilor

În configurația preconizată, soluția integrată funcțional hardware și software va include 1 set, iar acesta va include cel puțin 1 echipament de monitorizare a serviciilor, care se va instala la nivelul site-ului principal. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia în mod concurent pentru analizarea a cel puțin 1Gbps de trafic, respectiv monitorizarea a până la cel puțin 50 de instanțe active de tip server. Monitorizarea și analiza din perspectiva accesării aplicațiilor se va putea asigura pentru până la cel puțin 5000 de utilizatori externi unici pe lună, respectiv pe cel puțin 10 milioane de vizualizări la nivel de pagină web pe an.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Componenta de analiză și testare de securitate a aplicațiilor

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia pentru:

* Analizarea statică (SAST) fără restricții de număr de aplicații, în limita a 100,000 linii de cod, respectiv cel puțin pentru cod Java și .Net (C#);
* Analizarea dinamică (IAST/DAST) pentru cel puțin un serviciu de aplicație în tehnologie web targetat, la orice moment dat, inclusiv la nivel de modelare și evaluare de formulare interactive, autentificare și autorizare a accesului și logică de business implementată;
* Minim 2 utilizatori concurenti pentru analiza si raportare.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de analiză și remediere a vulnerabilităților de securitate

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea va acoperi utilizarea acesteia pentru minimum de 500 echipamente sau noduri si servicii active, identificabile în rețea prin adresa IP, scanate simultan într-o singură sesiune.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de analiză a accesării și utilizării resurselor

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea funcționalităților solicitate va acoperi utilizarea acestora pentru cel puțin 500 de utilizatori, respectiv pe un număr de 500 de echipamente de post lucru individual, fără a introduce alte limitări.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de redistributia a accesului la serviciile de aplicatie

În configurația preconizată, soluția integrată funcțional hardware și software va include 2 seturi cu funcționalități și echipare identice, iar fiecare set va include cel puțin 1 echipament de redistributie a accesului la serviciile de aplicație.

Atat in site-ul principal cat si in site-ul secundar se va instala cate 1 set, car vor forma un cluster la nivel global. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

Fiecare echipament redistributie a accesului la serviciile de aplicație va fi echipat și configurat pentru a asigura cel puțin:

* 10Gbps throughput, în regim de procesare generală L4/L7;
* 5Gbps procesare criptografică hardware internă integrată;
* 3Gbps compresie software internă integrată;
* 2000 tranzacții pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
* Procesarea de trafic până la cel puțin 500000 noi cereri L4 HTTP deschise pe secundă;
* Procesarea de trafic până la cel puțin 300000 noi conexiuni L7 deschise pe secundă;
* 4 porturi 1Gbps Ethernet SFP SX;
* 2 porturi 10Gbps Ethernet SFP+ SR;
* 1x 400GB SSD sau HDD;
* 2 module de răcire / ventilare, în configurație redundată;
* 2 surse de alimentare, în configurație redundată.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Componenta de protecție a serviciilor de aplicație

În configurația preconizată, soluția integrată funcțional hardware și software va include 4 seturi cu funcționalități și echipare identice, iar fiecare set va include cel puțin 1 echipament gateway de protecție a serviciilor de aplicație.

Atat in site-ul principal cat si in cel secundar se vor instala cate 2 seturi, în configurație de tip cluster. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

Fiecare echipament gateway de protecție a serviciilor de aplicație va fi echipat și configurat pentru a asigura cel puțin:

* Suport intern asigurat pentru autentificarea concurentă a cel puțin 500 utilizatori;
* 10Gbps throughput, în regim de procesare generală L4/L7;
* 8Gbps procesare criptografică hardware internă integrată;
* 5Gbps compresie hardware internă integrată;
* 4000 tranzacții pe secundă procesare SSL hardware internă integrată (cu chei 2048bit);
* Procesarea de trafic până la cel puțin 1000000 noi cereri L4 HTTP deschise pe secundă;
* Procesarea de trafic până la cel puțin 600000 noi conexiuni L7 deschise pe secundă;
* 4 porturi 1Gbps Ethernet SFP SX;
* 2 porturi 10Gbps Ethernet SFP+ SR;
* 1x 400GB SSD sau HDD;
* 2 module de răcire / ventilare, în configurație redundată;
* 2 surse de alimentare, în configurație redundată.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Componenta centrală de protecție avansată antimalware

În configurația preconizată, soluția integrată funcțional hardware și software va include 2 seturi cu funcționalități și echipare identice, iar fiecare set va include cel puțin 1 echipament de protecție avansată antimalware.

Atat in site-ul principal cat si in site-ul secundar se va instala cate 1 set. Se vor cota separat sub-componenta hardware și, respectiv, sub-componenta software a soluției.

Fiecare echipament de protecție avansată antimalware va fi echipat și configurat pentru a asigura procesarea a cel puțin 500Mbps de trafic.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

Vor fi incluse toate reperele și subansamblurile necesare pentru montarea în rack, racordarea la sistemul de alimentare cu energie electrică, precum și pentru interconectarea în mediile LAN și/sau SAN (acolo unde este cazul).

* + - 1. Componenta de protecție a resurselor la nivel de post de lucru

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea funcționalităților solicitate va acoperi utilizarea acestora pentru cel puțin 500 de utilizatori, respectiv pe un număr de 500 de echipamente de post lucru individual și pentru un număr de cel puțin 25 de instanțe de tip server, fără a introduce alte limitări.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta de management al datelor de audit

În configurația preconizată, soluția software va include 1 set de licențe, iar licențierea funcționalităților solicitate va acoperi utilizarea acestora pentru procesarea unui volum de informație martor de audit (de tip log, sau asimilat) generată susținut de cel puțin 10GB/zi, fără a introduce alte limitări.

Configurația va include garantarea dreptului de utilizare software, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe durata de viață a produsului, dar nu mai puțin de 3 ani de la darea în funcțiune a sistemului.

* + - 1. Componenta portal

Acest subsistem tehnic va sustine componenta functionala de Consultare Online a Buletinului Electronic al Registrului Comertului si va fi dimensionata pentru 5000 de utilizatori externi care vor avea acces la serviciile electronice publicate în componenta Portal, dintre care 1000 concurenţi.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta server de aplicatie

Acest subsistem tehnic va sustine cel putin urmatoarele componente functionale:

* + Componenta de consultare online a Bulentinului Electronic al Registrului Comertului
  + Componenta de Colectare si Elaborare a Buletinului Electronic al Registrului Comertului
  + Componenta de integrare aplicatii

Următoarele elemente cantitative vor fi avute în vedere la dimensionarea acestui subsistem:

1. Minim 500 de utilizatori interni care vor avea acces la funcţionalităţile subsistemului, dintre care 250 concurenţi;
2. Minim 5000 de utilizatori externi care vor avea acces la serviciile electronice publicate în componenta Portal, dintre care minim 1000 concurenţi
3. Incarcarea a minim 10.000 acte in programul de lucru al unei zile, totalizand un volum de date de minim 2 GB.
4. Licentierea trebuie sa acopere cel putin o capacitate de procesare de 48 core-uri de procesor.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de integrare a aplicatiilor

Licentierea trebuie sa acopere cel putin 8 core-uri de procesor.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de integrare a datelor

Licentierea pentru componenta de Replicare a datelor trebuie sa acopere nivelul de licentiere al componentei de gestiune a bazei de date cat si al serverelor de baza de date ce va fi implicat in replicarea datelor (clusterul de Oracle RAC existent in Sistemul Informatic Integrat al ONRC).

Licentierea trebuie sa acopere cel putin 8 core-uri de procesor pentru componenta de Transformare a datelor la nivelul fiecarui centru de date.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de gestiune documente

Acest subsistem tehnic trebuie sa asigure capacitatea de incarcare, stocare, procesare si consultare a documentelor indiferent de componenta prin care acestea ajung in cadrul sistemului informatic, cu respectarea parametrilor de perfomanta solicitati pentru fiecare componenta in parte.

Suplimentar fata de sustinerea componentelor cu care se integreaza pentru stocarea, procesarea si consultarea documentelor, următoarele elemente cantitative vor fi avute în vedere la dimensionarea acestui subsistem:

1. Minim 40 de utilizatori interni care vor avea acces la toate funcţionalităţile subsistemului;
2. stocarea a minim 7.000.000 acte care vor fi publicate în Buletinul Electronic al Registrului Comerţului din care aproximativ 4.500.000 documente existente in prezent; fiecare act are una sau mai multe pagini, în medie 2 pagini pe act.
3. incarcarea anuala a minim 300.000 acte ce totalizeaza aproximativ 20 GB;
4. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de procesare OCR

Licentierea acestei componente va fi dimensionata pentru minim 8 core-uri de procesor la nivelul fiecarui centru de date dar care sa permita o capacitate de procesare totala de minim 145 pagini A4 / minut.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de dezvoltare aplicatii mobile

Acest subsistem tehnic trebuie sa permita modificarea/depanarea de aplicatii existente sau dezvoltarea de noi aplicatii pentru cel putin 5 dezvoltatori.

Dimensionarea acestei componente se va realiza astfel incat fiecare centru de date sa poata sustine aplicatiile dezvoltate in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de gestiune baze de date

Următoarele elemente cantitative vor fi luate în considerare în dimensionarea acestui subsistem tehnic:

* 1. Licentiere pentru cel putin 16 core;
  2. Instrumentele de administrare incluse trebuie sa acopere toate masinile pe care vor fi instalate servere de baze de date si sa fie licentiate pentru cel putin 5 administratori.
  3. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de gestiune a proiectelor

Următoarele elemente cantitative vor fi luate în considerare în dimensionarea acestui subsistem tehnic:

* 1. 500 de utilizatori interni care vor avea acces la funcţionalităţile subsistemului, dintre care 100 manageri (manageri de proiect, manageri de departamente); estimam ca maxim 250 utilizatori pot fi concurenti;
  2. Minim 10 utilizatori interni vor avea acces pentru testarea subsistemului;
  3. pentru asigurarea unei disponibilități sporite, serverele trebuie grupate în cluster activ-activ pentru distribuţia cererilor;
  4. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de colaborare a echipelor

Următoarele elemente cantitative vor fi luate în considerare în dimensionarea acestui subsistem tehnic:

1. 500 de utilizatori interni care vor avea acces la funcţionalităţile subsistemului, dintre care 250 concurenţi;
2. Minim 10 utilizatori interni vor avea acces pentru testarea subsistemului;
3. pentru asigurarea unei disponibilități sporite, serverele trebuie grupate în cluster activ-activ pentru distribuţia cererilor;
4. pentru asigurarea continuității funcționării în caz de dezastru, subsistemul va fi distribuit in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de gestiune a ciclului de viata al aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. 50 de utilizatori interni care vor avea acces la funcţionalităţile componentei, din care maxim 20 concurenti;
2. folosirea a doua instante de servere distribuite in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini si de disponibilitate inalta la nivelul fiecarui centru de date.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de instalare si integrare continua a aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. folosirea unui numar de minim 50 de agenti ;
2. folosirea a doua instante de servere distribuite in 2 centre de date (centru primar si centru secundar).

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de testare automata a aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. o echipa IT de 50 de persoane va avea acces la testarea sistemului, dintre care 5 persoane vor avea acces in mod concurent;
2. solutia trebuie sa permita testarea sistemului pentru aplicatii de tip desktop, web si mobile;
3. trebuie sa poata fi rulate teste concurente, pe masini fizice si virtuale;
4. trebuie sa poata fi rulate un numar nelimitat de teste;
5. trebuie sa fie permisa rularea testelor pe browsere multiple.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

* + - 1. Componenta de testare de performanta a aplicatiilor

Următoarele elemente cantitative vor fi luate în considerare pentru dimensionarea acestui subsistem tehnic:

1. testele de performanta trebuie sa permita asigurarea unei incarcari de cel putin 1000 de utilizatori virtuali
2. echipa IT ce va fi desemnata de catre ONRC pentru gestiunea si rularea cazurilor de test va fi de minim 5 persoane care pot lucra concurent;
3. trebuie sa poata fi create un numat nelimitat de teste;
4. solutia trebuie sa permita testarea sistemului pentru incarcarea maxima a sa.

Dimensionarea se va realiza astfel incat fiecare centru de date sa poata sustine incarcarea mai sus mentionata in conditiile de performanta ale prezentului caiet de sarcini.

Totodata se va avea in vedere si licentierea componentei pentru mediul de testare/dezvoltare.

Configurația va include garantarea dreptului de utilizare software nelimitat in timp, precum și de acces al beneficiarului la actualizările și pachetele corective publicate de producător, fără costuri suplimementare, pe o perioada de cel puțin 3 ani de la furnizarea licentelor.

## Cerințe de livrare și implementare

Ofertantul declarat castigator (Prestatorul) va fi responsabil atât cu livrarea, instalarea și configurarea echipamentelor hardware și a sistemelor software de bază în site-urile autoritatii contractante (centrele de date), cât și cu dezvoltarea noilor componente.

Prestatorul va fi responsabil de toate activitățile necesare pentru punerea în producție a sistemului incluzând, fără a se limita la: analiză detaliată, proiectare detaliată, dezvoltare de cod, testare unitară, testare de integrare, testare pentru punerea în producție, instalarea și configurarea pentru punerea în producție, sprijin pentru Beneficiar în vederea punerii în producție, garanție, management de proiect.

Codul sursă pentru componentele noi dezvoltate în cadrul proiectului va deveni proprietatea Beneficiarului.

În cazul în care echipamentele componente ale soluției tehnice vor fi furnizate de mai mulți producatori, va fi asigurată integritatea și funcționalitatea întregului sistem. Funcționalitatea componentelor sistemului nu va fi in nici un fel afectată de integrarea în ansamblul soluției oferite.

Echipamentele, componentele și produsele software care fac obiectul prezentului caiet de sarcini vor fi instalate la sediul principal al autoritatii contractante sau la centrul de date secundar.

Instalarea echipamentelor, componentelor și a produselor software care fac obiectul prezentului caiet de sarcini va fi efectuată de catre personalul de specialitate al Prestatorului. Acestea vor fi instalate, configurate, parametrizate, testate și integrate în sistemul informatic existent de catre personalul de specialitate al Prestatorului.

Echipamentele hardware livrate trebuie să fie noi și să beneficieze de suport din partea producatorului (nu se accepta echipamente uzate moral, ce nu se mai află în linia de fabricație).

## Organizarea şi coordonarea proiectului

### Servicii de management de proiect

În vederea implementării cu succes a sistemului, Prestatorul va asigura servicii de management de proiect prin alocarea unui Manager de Proiect dedicat pentru executia acestui proiect, pe toată durata implementării.

Durata de implementare a achiziţiei (semnarea acceptanţei finale) va fi de maxim 15 luni de la data semnării contractului. Această perioadă include livrarea, instalarea și punerea în functiune a echipamentelor precum si proiectarea, dezvoltarea, testarea, instruirea și acceptanța sistemului.

Ofertantii vor avea in vedere urmatoarele termene maximale pentru finalizarea activitatilor de implementare:

* Livrare infrastructura HW si SW standard – 2 luni de la semnarea contractului
* Instalare infrastructura HW si SW standard – 4 luni de la semnarea contractului
* Analiza – 4 luni de la semnarea contractului
* Proiectare – 5 luni de la semnarea contractului
* Dezvoltare / testare prestator – 10 luni de la semnarea contractului
* Instalarea si configurarea paticulara a solutiei – 12 luni de la semnarea contractului
* Testare functionala si de integrare – 13 luni de la semnarea contractului
* Instruire administratori si utilizatori – 15 luni de la semnarea contractului
* Punere in functiune sistem (inclusiv datele migrate/incarcate) si obtinere acceptanta finala – 15 luni de la semnarea contractului

Totodata, in planul de proiect se va avea in vedere realizarea urmatoarelor receptii:

* 1. Cantitative – prin intermediul carora se livreaza produsele HW, pachetele SW standard si livrabilele serviciilor prestate din punct de vedere cantitativ.
  2. Calitative – prin intermediul carora Beneficiarul verifica parametrii de calitate ai livrarilor cantitative. Acestea pot fi:
     1. Receptii calitative partiale – sunt receptii calitative ce privesc anumite componente si/sau servicii ce fac obiectul contractului de achizitie. In baza acestor receptii calitative intermediare, beneficiarul poate realiza plati partiale aferente produselor / serviciilor receptionate. Sunt acceptate receptii calitative partiale pentru:
        + Livrarea si instalarea produselor HW - in urma testelor de acceptanta a instalarii produselor HW
        + Livrarea si instalare pachetelor SW de baza – in urma testelor de acceptanta a instalarii pachetelor SW de baza
        + Serviciile de analiza – in urma aprobarii documentului de analiza
        + Serviciile de proiectare – in urma aprobarii documentului de proiectare
        + Servicii de dezvoltare si testare – in urma testarii functionale si de performanta a sistemului
        + Serviciile de instruire – in urma acceptarii serviciilor de instruire prestate
     2. Receptie finala – care este realizata dupa finalizarea tuturor activitatilor proiectului si punerea in functiune a intregului sistem informatic.

Ofertantul are obligatia sa respecte urmatoarele termene maxime pentru realizarea receptiilor calitative in cadrul proiectului:

|  |  |  |  |
| --- | --- | --- | --- |
| **Denumire produs/serviciu** | **Livrabile** | **Document receptie calitativa** | **Termen receptie calitativa (luni de la semnarea contractului)** |
| Infrastructura HW | Infrasructura HW  Raport instalare si configurare infrastructura HW si produse SW standard  Scenarii de testare a infrastructurii HW si produse SW standard | Proces verbal receptie calitativa infrastructura HW si produse SW standard | 5 |
| Produse SW standard | Produse SW standard  Raport instalare si configurare infrastructura HW si produse SW standard  Scenarii de testare a infrastructurii HW si produse SW standard | Proces verbal receptie calitativa infrastructura HW si produse SW standard | 5 |
| Livrarea si instalarea infrastructurii HW | Raport instalare si configurare infrastructura HW si produse SW standard  Scenarii de testare a infrastructurii HW si produse SW standard | Proces verbal receptie calitativa infrastructura HW si produse SW standard | 5 |
| Livrarea si instalarea produselor SW standard | Raport instalare si configurare infrastructura HW si produse SW standard  Scenarii de testare a infrastructurii HW si produse SW standard | Proces verbal receptie calitativa infrastructura HW si produse SW standard | 5 |
| Servicii de analiza | Document analiza de business  Scenarii de testare functionala si de testare integrare | Proces verbal receptie calitativa servicii analiza | 5 |
| Servicii de proiectare | Document proiectare detaliata  Scenarii de testare non-functionala | Proces verbal receptie calitativa servicii proiectare | 6 |
| Servicii de dezvoltare si testare | Kit de instalare  Procedura de instalare  Manuale de utilizare si instalare  Ghid de testare functionala si de testare integrare | Proces verbal receptie calitativa servicii dezvoltare si testare | 14 |
| Servicii de instalare si configurare particulara a solutiei | Raport instalare si configurare particulara a solutiei | Proces verbal receptie calitativa servicii de instalare si configurare particulara a solutiei | 14 |
| Servicii de instruire | Materiale instruire utilizatori  Materiale instruire administratori  Rapoarte privind participarea la cursurile de instruire | Proces verbal receptie calitativa servicii instruire | 15 |
| Sistem informatic integrat | Raport de punere in functiune a sistemului informatic (GOLIVE)  Codul sursa al aplicatiilor dezvoltate  Procedura de compilare a codului sursa  Rapoartele de monitorizare si control al proiectului  Certificat de garantie pentru sistemul informatic | Proces verbal de receptie calitativa finala | 15 |

Librabilele se predau beneficiarului pe baza de procese verbale de receptie cantitativa. Receptiile calitative se realizeaza pe baza proceselor verbale de receptie cantitativa aferente livrabilelor mentionate in tabelul de mai sus si a inspectiilor / verificarilor realizate de catre beneficiar in conformitate cu prevederile prezentului document.

Ofertantii vor evidentia toate milestone-urile si activitatile importante, duratele acestora si resursele ce vor fi alocate, in cadrul graficului de proiect ce va fi inclus in oferta tehnica.

* + - 1. Planificare, monitorizare si control / Planul de proiect

Ofertantul va prezenta împreună cu oferta un plan de proiect în care se vor detalia toate activitățile planificate în cadrul proiectului, milestone-urile aferente furnizarii livrabilelor si ale acceptarii acestora de catre Autoritatea Contractanta, responsabilitățile cu privire la fiecare activitate în parte și persoanele responsabile din cadrul echipei de proiect pentru realizarea fiecărei activități.

Planul de proiect va include, după caz, livrarea unui pilot pentru solutia implementata, care va fi pus in productie, astfel incat la finalizarea fazei pilot, solutia sa fie ajustata pentru o functionare optima si conforma cu cerintele. Durata fazei pilot va fi agreata de catre parti la fiecare solutie implementata.

Controlul proiectului se va realiza cu ajutorul unei structuri de evaluare care va include:

* sedinta lunara de evaluare a stadiului intregului proiect
* sedinte regulate de evaluare a diferitelor zone functionale ale proiectului
* sedinte de evaluare la finalizarea unor etape de proiect
* sedinte de evaluare a riscului
* sedinte ad-hoc de rezolvare a unor probleme specifice

Aceste sedinte vor fi conduse de catre expertul Manager de Proiect, iar rezultatele sedintelor vor fi documentate in Minute de Sedinta care vor fi pastrate in cadrul Dosarului de Proiect.

* + - 1. Raportarea

Se vor întocmi rapoarte de progres pe întreaga perioadă de derulare a proiectului.

Prestatorul trebuie sa transmita Beneficiarului cel putin urmatoarele rapoarte:

* Rapoarte periodice prezentate de catre Managerul de Proiect catre Comitetul de Conducere al proiectului
* Rapoarte de Exceptie (rapoarte ad-hoc care vor fi elaborate ori de cate ori vor apare exceptii de la activitatile planificate, exceptii care necesita o decizie din partea Comitetului de Conducere al proiectului)
* Raport Final (la finalizarea contractului)
* Rapoarte ad-hoc elaborate de către Managerul de Proiect, ori de câte ori acest lucru este necesar, la solicitarea Comitetului de Conducere al proiectului.
  + - 1. Metodologia de proiect

Ofertantul va descrie metodologia de abordare şi conducere a proiectului, precum şi fiecare fază a proiectului în conformitate cu metodologia de proiect propusă.

Ofertantul va detalia metodele şi instrumentele folosite pentru:

* managementul proiectului
* monitorizarea evolutiei proiectului
* managementul calitatii
* managementul riscurilor
* managementul schimbarii

##### Managementul calitatii

Calitatea in mediul de proiect se defineste ca fiind totalitatea cerintelor de ordin tehnic, functional, a obiectivelor cantitative si calitative ale proiectului, precum si metodologia si procedurile de management de proiect stabilite la nivelul proiectului, care trebuie atinse și respectate pentru finalizarea cu succes a proiectului.

Ofertantul va avea in vedere cel putin furnizarea urmatoarelor livrabile pe durata implementarii:

* Livrabile de management (planuri, proceduri, rapoarte):
* Echipa de proiect şi Comitetul de conducere al proiectului;
* Planul proiectului;
* Rapoarte de monitorizare şi control al proiectului:
* Livrabile tehnice ale proiectului:
* Documentul de analiză de business – a proceselor existente şi a celor care vor fi implementate;
* Documentul de proiectare detaliată HW/SW – ce include arhitectura sistemului si aspectele non-functionale;
* Scenarii de testare functionala si non-functionala;
* Echipamentele hardware şi software standard contractate şi livrate;
* Documentul care certifică instalarea şi configurarea echipamentelor hardware;
* Documentul care certifică corectitudinea funcţionalităţilor dezvoltate în cadrul sistemului informatic;
* Documentul care certifică instalarea şi configurarea finală a sistemului informatic;
* Documentul care certifică instruirea utilizatorilor sistemului informatic;
* Documentul care certifică instruirea personalului care va utiliza/administra echipamentele hardware şi software;
* Kitul de instalare a aplicatiei dezvoltate (include release note si instructiuni de instalare)
* Codul sursa al aplicatiei dezvoltate
* Materiale de instruire
* Manuale de utilizare/administrare/configurare ale sistemului informatic;
* Manuale de instalare şi configurare a echipamentelor şi software-ului de bază;
* Manuale de administrare a sistemului/soluţiei;
* Manuale de utilizare a componentelor sistemului/soluţiei;
* Documentaţia funcţională a componentelor sistemului/soluţiei;
* Documentaţia tehnică a componentelor sistemului/soluţiei;
* Documentaţiile tehnice ale echipamentelor şi software-ului de bază, furnizate de producători;
* Alte manuale/documentaţii stabilite în urma perioadei de analiză, proiectare, dezvoltare sau urmare derulării proiectului.
* Proceduri de lucru cu / administrare a sistemul(ui) informatic;
* Certificate de garantie.

Implementatorul va furniza toate manualele şi documentaţiile în limba română, cu excepţia documentaţiilor tehnice ale echipamentelor şi software-ului de bază, furnizate de producători, care pot fi în limba engleză.

Manualele şi documentaţiile, cu excepţia celor elaborate de producător, vor fi livrate pe suport electronic (CD, DVD) şi vor fi revizuite la fiecare schimbare de versiune software.

Odată cu predarea sistemului împreună cu toate documentaţiile aferente, Ofertantul cedează şi drepturile de proprietate intelectuală/drepturile de autor asupra aplicaţiilor dezvoltate care constituie componente ale sistemului.

Cerinte de calitate pentru fiecare livrabil:

* pentru echipamente:
* tip
* cerinte tehnice
* standarde
* dimensiuni
* consum energetic etc.
* pentru software:
* cerinte functionale
* cerinte tehnice
* cerinte de capacitate, timp de raspuns
* pentru servicii
* cerinte, specialisti, activitati
* specificatiile livrabilelor rezultante

Procedura de management al calității va prevedea metodele concrete prin care se va monitoriza și controla evoluția calității livrabilelor, pe întreaga durată a proiectului. În mod concret, se va realiza la nivelul proiectului o strategie de testare și acceptanță care va indica, pentru fiecare tip de livrabil în parte, etapele procesului de verificare a calității (testare), criteriile de acceptanță și modalitatea de documentare a acestui proces.

Pentru monitorizarea aspectelor legate de calitate, se va întreține la nivelul proiectului un Registru de Calitate și se vor organiza ședinte periodice de management al calității, în cadrul cărora se vor discuta aspecte legate de calitate, se vor stabili acțiuni și se va actualiza Registrul de calitate. În Registrul de calitate se vor înregistra toate testele și acceptanțele din cadrul proiectului, data și rezultatele obținute. Orice disfuncționalitate sau neconformitate va fi ulterior tratată, până la rezolvare. Concluzia finală se va înregistra, de asemenea, în Registrul de Calitate al proiectului.

##### Managementul riscurilor

Riscurile la adresa obiectivelor proiectului vor fi identificate si documentate in Registrul Riscurilor, impreuna cu modul in care acestea pot fi tinute sub control. De asemenea, se vor prevedea masuri de rezerva pentru situatia in care riscul devine activ. Registrul Riscurilor si planurile asociate pentru controlul acestor riscuri vor fi revazute in mod regulat in timpul sedintelor de evaluare a riscurilor.

Pe durata derulării proiectului, în momentul identificării unui nou risc sau al manifestării unui risc planificat, persoana din echipa de proiect care a identificat riscul îl comunică Managerului de Proiect. Acesta realizează o analiză preliminară și, dacă riscul este real, întocmește un Raport de Risc pe care îl transmite Comitetului de Conducere al proiectului în vederea aprobării măsurilor propuse în cadrul Raportului.

Prestatorul va fi responsabil pentru livrarea unui sistem informatic perfect integrat, care să includă toate funcționalitățile prevăzute în proiectul tehnic și care să permită atingerea tuturor obiectivelor specifice ale proiectului, conform cerintelor din Caietul de Sarcini.

Ofertantul va include în echipa sa de proiect doi specialiști în securitate, care vor defini/monitoriza/verifica cerințele de implementare din perspectiva asigurării securității datelor și a sistemelor. De asemenea, la finalizarea implementării tehnice a proiectului și înainte de testarea finală a soluției, Prestatorul va trebui să realizeze teste de securitate și să prezinte un raport cu privire la problemele identificate. Acestea vor fi analizate, se vor stabili acțiuni de remediere care vor fi implementate și ulterior se va face o nouă verificare a securității.

##### Managementul schimbarii

In cadrul oricarui proiect care are un ciclu mai lung de viață (peste 1 an) între momentul inițializării și cel al finalizării implementării, este posibil ca pe durata derularii sale anumite procese de lucru, cerinte tehnice si functionale sau prioritati sa se modifice. Este esential ca in astfel de situatii proiectul sa se poata adapta acestor schimbari, iar aceasta poate insemna modificarea diferitelor planuri, specificatii si livrabile ale proiectului pe durata implementarii proiectului.

Toate aceste schimbari vor fi gestionate prin intermediul Procedurii de Management al Schimbarii.

Schimbarile survenite sau propuse vor fi analizate din punct de vedere al implicațiilor asupra diferitelor elemente ale proiectului (obiective, cerințe, buget, resurse, termene de implementare, riscuri etc.) si se vor stabili cele mai bune strategii pentru gestionarea lor. Schimbarile care au implicatii asupra livrabilelor proiectului vor fi documentate si supuse aprobarii Comitetului de Conducere al proiectului.

### Servicii de implementare

* + - 1. Analiza

Echipa de analiza a Prestatorului trebuie sa analizeze cerintele impreuna cu expertii Beneficiarului pentru a intelege corect modificarile legislative/nevoile utilizatorilor inainte de proiectarea şi dezvoltarea noilor functionalitati.

Livrabilele de analiza includ descrierea componentelor care trebuie dezvoltate/adaptate. Livrabilele acestei etape sunt urmatoarele:

* Document de analiza de business - cu specificatiile functionale pentru componentele dezvoltate/adaptate
* Cazuri si scenarii de testare functionale si respectiv de integrare, pentru componentele dezvoltate/adaptate conform cerintelor din prezentul document

In vederea derularii etapei de proiectare si dezvoltare software, livrabilele mai sus mentionate vor fi aprobate de catre persoanele responsabile din cadrul ONRC.

* + - 1. Proiectare si dezvoltare software

Ofertantul va descrie metodologia de dezvoltare software folosita in cadrul proiectului.

Serviciile de proiectare si dezvoltare software se vor realiza pe baza documentelor rezultate si aprobate in faza de analiza software. Aceste servicii includ: proiectarea, dezvoltarea si integrarea efectiva a functionalitatilor, conform specificatiilor aprobate in faza de analiza. Etapa de proiectare si dezvoltare se va incheia cu testarea interna realizata de Prestator, in vederea livrarii catre ONRC a functionalitatilor dezvoltate in cadrul prezentului contract.

Livrabilele acestei etape sunt urmatoarele:

* Codul sursa al aplicatiei comentat la nivel de clasa (Java), functie (PL/SQL) si proceduri (PL/SQL), codul XML, codul fisierelor de configurare
* Rezultatele testelor Prestatorului
* Procedura de compilare a codului sursa
* Document de proiectare detaliata – include Modelul functional si de date (UML 2.0) si aspectele non-functionale specifice componentelor ce asigura monitorizarea si securitatea sistemului
* Manuale de utilizare
* Orice alte informatii relevante, la cerinta ONRC

Inainte de predarea unui release nou (sau a unui patch) spre testare catre ONRC, Prestatorul va realiza propria etapa de testare interna, ca parte a procedurilor sale de asigurare a calitatii.

Echipa Prestatorului alocata pentru realizarea acestor servicii va fi responsabila pentru intretinerea permanenta pe durata acestui acord cadru a codului sursa al tuturor dezvoltarilor realizate in cadrul sistemului informatic al carui proprietar este ONRC. Orice dezvoltare noua a sistemului informatic ONRC, realizata ca urmare a acestui acord cadru, va deveni proprietatea exclusiva a ONRC.

Echipa Prestatorului va avea sarcina de a actualiza codul sursa al aplicatiilor, precum si procedurile necesare pentru compilarea si utilizarea acestui cod sursa. Procedura de compilare a codului sursa va fi astfel documentata incat sa permita restaurarea aplicatiilor din cadrul sistemului informatic in caz de dezastru si de indisponibilitate a copiilor de siguranta. Procedura va prezenta pas cu pas activitatile necesare pentru restaurarea aplicatiilor plecand de la codul sursa al acestora.

* + - 1. Instalare şi configurare soluție

Ofertantul va fi responsabil pentru realizarea soluţiei ofertate asigurând:

* compatibilitate maximă cu soluția existentă;
* valorificarea infrastructurii existente;
* garantarea unei maxime disponibilităţi.

Ofertantul va asigura următoarele servicii:

##### Implementarea soluţiei

Implementarea subsistemelor/soluţiilor va cuprinde cel putin urmatoarele faze/activitati:

* transportul şi manipularea până la sediul beneficiarului, dupa caz;
* furnizarea cerințelor necesar a fi asigurate de beneficiar pentru instalarea în bune condiții;
* realizarea planului detaliat al activităților ce vor fi realizate şi agrearea acestuia cu beneficiarul, în vederea evitării oricărei întreruperi în funcționarea aplicațiilor din producție;
* analiza cerintelor, pregatirea specificatiilor functionale si validare de catre beneficiar;
* proiectarea detaliata a soluțiilor solicitate si validare de catre beneficiar. După validarea acestui document de către Beneficiar se va trece la executarea serviciilor necesare aferente;
* instalarea şi configurarea tuturor produselor software, dupa caz;
* instalarea şi configurarea tuturor echipamentelor în scopul implementării soluției, dupa caz;
* reaizarea tuturor configurărilor necesare pentru asigurarea tuturor serviciilor solicitate;
* dezvoltarea solutiei software;
* realizarea testării funcționale a solutiei pe mediul de dezvoltare/testare;
* instalarea şi configurarea produselor software, dupa caz;
* configurarea produselor software existente în scopul implementării soluțiilor, dupa caz;
* realizarea tuturor configurărilor necesare pentru asigurarea tuturor serviciilor solicitate;
* actualizarea configurațiilor ca urmare a unor modificări survenite pe cel putin unul din sistemele din locaţiile implementate;
* realizarea testării funcționale a sistemului implementat pe mediul de dezvoltare/testare la fiecare modificare de configurație;
* livrarea documentelor cu specificațiile pentru soluţiile implementate;
* livrarea procedurilor de lucru detaliate pentru serviciile implementate;
* livrarea procedurilor de back-up şi restore, dupa caz.

Prestatorul va asigura serviciile de instalare / configurare în afara orelor programului de lucru ale ONRC, cel puțin pentru serviciile care implica centrul principal (productiv, la nivel central si teritorial), reconfigurările aferente testării şi orice alte configurării care implica sistemul aflat în producție.

Metodologia de implementare propusa trebuie sa fie de tip iterativ.

##### Instalare / configurare subsisteme/soluţii

Ofertantul va fi responsabil pentru realizarea subsistemelor/soluţiilor asigurând:

* compatibilitate cu soluția existentă;
* valorificarea infrastructurii existente;
* garantarea unei maxime disponibilităţi.

Serviciile de instalare/configurare vor cuprinde:

* instalare software aplicativ la nivel central si teritorial dupa caz;
* configurare şi monitorizare.
  + - 1. Testarea și testele de acceptanță

Realizarea cu succes a testelor este condiție pentru obținerea acceptantei finale asupra soluţiilor livrate. Testele se consideră a fi încheiate cu succes dacă este posibilă furnizarea serviciilor solicitate in conditii optime conform cerintelor.

Planul de testare va fi propus de Prestator şi agreat de Beneficiar.

Testele vor include dar nu se vor limita la următoarele:

* Testare funcţională pe date relevante
* Testare de performanţă (timp de răspuns corespunzător profilului de utilizator)
* Teste de stres (volum de date, număr de utilizatori concurenţi)
* Teste de identificare a problemelor cu menţionarea zonei de cod care trebuie optimizată (clasă, funcţie, procedură, instrucţiune)
* Testare pentru acceptanţa finală.

Ofertantul trebuie sa prezinte in cadrul propunerii tehnice metodologia de testare după care se vor realiza activitățile de testare în timpul desfășurării proiectului.

Planul detaliat de testare, însoțit de scenariile de testare, va fi realizat de către Prestator și aprobat de Beneficiar înainte de fiecare etapă de testare agreată prin planul de proiect.

Beneficiarul (cu asistența Prestatorului) va rula toate scenariile pentru testele de acceptanță ale componentei livrate. Testele de acceptanţă se vor derula în conformitate cu Planul de Testare.

* + - 1. Intrarea in productie

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 şi cu impact minim asupra activităţilor zilnice ale angajaţilor Beneficiarului.

### Servicii de garantie si suport

**Cerinţele de garanție și suport exprimate în continuare sunt cerinţe minime obligatorii.**

Perioada de garanţie şi suport pentru sistemul informatic va fi asigurata pentru:

***Minim 3 ani pentru hardware*** ***de la data semnării procesului verbal de recepţie cantitativa.***

*Garanţia produselor hardware asigură înlocuirea oricărei componente defecte, costurile înlocuirii fiind suportate de către furnizorul echipamentului.*

*În perioada de garanţie, Prestatorul se obligă să asigure constatarea defecţiunilor hardware și remedierea defectelor on-site.*

*Remedierea defectelor se va face la sediul ONRC, iar în cazul unor defecte mai grave, echipamentele se vor transporta de către furnizor la sediul acestuia, asigurându-se însă continuitatea serviciilor informatice ale ONRC.*

* *În situaţia în care este necesară transportarea echipamentelor în afara sediului ONRC, toate mijloacele de stocare a datelor vor fi reţinute de către beneficiar (hard-discurile vor fi scoase din echipamente și păstrate la sediul ONRC).*
* *La finalizarea fiecărei intervenţii în cadrul perioadei de garanţie se va întocmi o fişă de intervenţie care va conţine următoarele detalii: data intervenţiei, descrierea intervenţiei, modalitatea de rezolvare a intervenţiei (reparaţie/înlocuire), durata de intervenţie şi confirmarea recepţiei prin semnăturile Prestatorului şi beneficiarului.*

***Minim 2 ani pentru produse software standard (inclusiv SO, software de cluster, dacă este cazul) de la data semnării procesului verbal de recepţie cantitativa****.* Garantia produselor software va cuprinde:

* *Acces la ultima versiune, patch-uri, fix-uri publicate de producator;*
* *Acces la documentaţia tehnica;*
* *Analiza problemelor;*
* *Prioritizarea problemelor după severitatea acestora;*
* *Comunicarea cererilor de asistenţă către un centru de suport tehnic;*

***Minim 2 ani garantie pentru aplicaţiile dezvoltate de la data punerii in functiune a sistemului informatic cu toate functionalitatile acestuia.***

*Aceste servicii obligă ofertantul/furnizorul noului sistem să rezolve orice neconformitate a sistemului informatic, în concordanţă cu specificatiile acestuia.*

*În cazul in care sunt necesare modificari, implementatorul este obligat:*

* *să modifice/actualizeze aplicaţiile componente ale sistemului;*
* *să modifice/actualizeze şi documentaţia acestor aplicaţii;*
* *să predea codul sursă, executabilele şi kit-urile de instalare ale aplicaţiilor modificate.*

*Aplicaţiile vor respecta specificaţiile funcţionale, vor fi fără erori şi vor rula fără întreruperi sau probleme de funcţionare, în caz contrar Ofertantul având obligaţia de a remedia erorile în cauză.*

*În perioada de garantie, Ofertantul va remedia erorile de funcţionare ale sistemului livrat. Aplicaţiile implementate nu vor avea vulnerabilităţi privitoare la atacuri sau intruziuni în sistem. Aceste aspecte vor fi detaliate de către Ofertant în documentul de specificaţii tehnice ale aplicaţiilor informatice;*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Nivel Criticitate*** | ***Timp de raspuns*** | ***Timp solutionare temporara*** | ***Timp solutionare finala*** |
| ***Critic*** | *1 oră lucratoare* | *4 ore lucratoare* | *2 zile lucratoare* |
| ***Mediu*** | *4 ore lucratoare* | *2 zile lucratoare* | *4 zile lucratoare* |
| ***Minor*** | *2 zile lucratoare* | *4 zile lucratoare* | *8 zile lucratoare* |

* + 1. *Fereastra de suport tehnic / garanție:* 
       1. *L-V/ zile de lucru nelucrătoare declarate ca fiind lucrătoare în sistemul administrației publice/ 08:00 – 18:00*
    2. *Tipurile incidentelor:*
       1. ***Critic****: una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate iar impactul acestui incident duce la imposibilitatea utilizării sistemului*
       2. ***Mediu****: impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor functionalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.*
       3. ***Minor****: impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.*

***Prestatorul va asigura o garanţie de minim 2 ani după finalizarea implementării proiectului si punerea in functiune a sistemului pentru toate funcţionalităţile acestuia, care trebuie să rămână nealterate pe întreaga perioadă de garanţie****.*

Depășirile timpilor de răspuns/solutionare asumați prin propunerea tehnică pentru perioada de garanție și suport dau dreptul achizitorului de a calcula și aplica penalizări. Acestea sunt cuantificate prin puncte de penalizare, astfel:

- Pentru depasirea termenului de raspuns si a termenului de solutionare temporară/finală aferente defectelor critice, se vor aplica 3 puncte de penalizare pentru fiecare oră de depășire a termenului;

- Pentru depășirea termenului de raspuns si a termenului de solutionare temporară/finală a defectelor medii se vor aplica 2 puncte de penalizare pentru fiecare oră de depășire a termenului

- Pentru depășirea termenului de raspuns si a termenului de solutionare temporară/finală a defectelor minore se va aplica 1 punct de penalizare pentru fiecare oră de depășire a termenului

Un punct de penalizare valorează 0,001% din valoarea contractului.

*Garanţia se va asigura fără costuri slimentare din partea ONRC.*

*Perioada de garanţie se va majora cu timpul de nefuncţionare al echipamentelor/subsistemelor informatice în intervalul de reparare a acestora.*

*Toate serviciile mentionate vor fi prestate in baza metodologiei de asistenta, suport tehnic si garantie ce va fi descrisa de catre ofertanti in cadrul propunerii lor.*

Înştiinţarea cu privire la o disfuncţionalitate a sistemului informatic implementat va fi realizată de către beneficiar prin următoarele metode (care vor fi puse la dispoziţie de către furnizor odata cu punerea in functiune a sistemului):

* Aplicatie informatica de gestiune a incidentelor in perioada de garantie
* Utilizând sistemul de poștă electronică (la o adresa de poştă electronică dedicată pusă la dispoziţie de către furnizor).
* Printr-un apel telefonic al ONRC la un număr dedicat pus la dispoziţie de către furnizor.
* Prin transmiterea unui fax de către ONRC la un număr de fax dedicat pus la dispoziţie de către furnizor.

Remedierea defectelor se va face la sediul ONRC, iar în cazul unor defecte mai grave, echipamentele se vor transporta de către furnizor la sediul acestuia, asigurându-se însă continuitatea serviciilor informatice ale ONRC.

* În situaţia în care este necesară transportarea echipamentelor în afara sediului ONRC, toate mijloacele de stocare a datelor vor fi reţinute de către beneficiar (Hard-discurile vor fi scoase din echipamente și păstrate la sediul ONRC).
* La finalizarea fiecărei intervenţii în cadrul perioadei de garanţie se va întocmi o fişă de intervenţie care va conţine următoarele detalii: data intervenţiei, descrierea intervenţiei, modalitatea de rezolvare a intervenţiei (reparaţie/înlocuire), durata de intervenţie şi confirmarea recepţiei prin semnăturile Prestatorului şi beneficiarului.
* Perioada de garanţie se va majora cu timpul de nefuncţionare al echipamentelor/subsistemelor informatice în intervalul de reparare a acestora.

### Instruire

**Instruirea utilizatorilor, administratorilor de sistem, reţea, comunicaţii şi securitate şi administratorilor de aplicaţii joacă un rol esenţial în garantarea acceptanţei sistemului livrat precum şi în întreţinerea şi dezvoltarea acestuia.**

**În cadrul proiectului, activităţile de instruire au în vedere** **instruirea/cursarea a 50 utilizatori, angajaţi ai ONRC, atât de la nivel central cât şi teritorial (ORCT), 5 administratori de sistem, reţea, comunicaţii şi securitate si 5 administratori de aplicatii.**

**Cerinţele de instruire exprimate în continuare sunt cerinţe minime obligatorii.**

Procesul de instruire este adresat utilizatorilor finali, administratorilor de reţea, comunicaţii şi securitate precum şi administratori de aplicaţii şi va include tematici cu privire la utilizarea, administrarea şi dezvoltarea noului sistem implementat.

Prestatorul va organiza mai multe tipuri de cursuri de instruire, în funcţie de audienţa vizată şi anume:

* 1. ***Cursuri destinate utilizatorilor finali*** care includ tematici cu privire la utilizarea, in conditii de siguranta, a noului sistem implementat de către personalul de la nivel central şi teritorial:

A.1. Instruire personal implicat în colectarea, analiza datelor şi actelor persoanelor supuse obligaţiei de înregistrare în registrul comerţului, raportarea către ONRC, publicarea în Buletinul Electronic al Registrului Comerţului si utilizarea datelor din Buletinul Electronic al Registrului Comerţului:

- 50 persoane (1 persoana de la fiecare ORCT, 5 persoane de la ORCTB si 4 persoane de la ONRC), organizate în 3 grupe;

- instruirea va fi organizată în 3 grupe;

- cursurile vor avea loc la Bucureşti, într-o locație asigurată de Prestator dotată corespunzător necesar susținerii cursurilor;

- Prestatorul va asigura cazarea (într-o unitate hotelieră de minim 3 stele sau similar, în regim de camera single), transportul și masa (mic dejun, prânz și cină);

- durata cursurilor va fi de 4 zile/ 4 nopți pentru fiecare grupa

- pentru serviciile de cazare va fi decontată contravaloarea serviciilor efectiv prestate, pe baza documentelor justificative privind numărul de participanţi efectiv cazaţi şi a listei cu participanţii semnată în original

- în vederea bunei desfășurări a cursului prestatorul va asigura pentru fiecare sesiune 1 formator

- formatorul va presta un număr de 32 ore de pregătire/sesiune de formare (care vor include și orele aferente evaluării)

- Orele de pregătire şi evaluare vor fi evidenţiate în cadrul fişei de pontaj pentru fiecare categorie de activitate.

**Serviciile de transport vor fi asigurate de operatorul economic** (dus/întors) pentru **numărul de participanti** care provin din toate zonele țării, ținând seama de organizarea instituției registrului comerțului la nivelul țării, prin **decontarea cheltuielilor aferente transportului dus/întors pentru numărul de participanți, în limita a 400 lei, fără TVA/participant, in pretul ofertei**.

**Decontarea transportului se va face de către prestator individual către aceste persoane, pe baza documentelor justificative prezentate. Decontarea transportului se va efectua pentru deplasare dus–întors, la data prezentării participantului la locul desfășurării cursului. Prestatorul va asigura participanţilor decontarea acestui tip de cheltuială de transport din fonduri proprii, pe baza documentelor justificative, cu respectarea dispozițiilor** H.G. 1860/2006 cu modificările și completările ulterioare, luând în considerarare distanța disponibilă pe website-ul [www.distanța.ro](http://www.distanța.ro) și în raport de prevederile cuprinse în Ghidul Beneficiarului astfel:

**Pentru transport cu autoturismul personal**:

* Decontul se va realiza pe baza bonurilor fiscale de combustibil cu menţionarea numărului de înmatriculare al maşinii pe verso şi numele participantului. Bonurile fiscale vor reflecta cantitatea de combustibil cu care s-a făcut alimentarea mijlocului de transport personal şi trebuie să fie emis într-o perioadă apropiată deplasării;
* Se decontează contravaloarea 7,5 l combustibil/100 km cu documente justificative şi ordin de deplasare/delegaţie înregistrat la angajator, completat cu perioada deplasării şi scopul acesteia, semnat şi ştampilat de angajator, cu număr şi dată, cu precizarea "Se deplasează cu auto personal". Valoarea bonului fiscal de combustibil trebuie să fie cel mult egală cu valoarea efectiv calculată pentru decont. În cazul în care valoarea bonului fiscal este mai mare decât valoarea calculată, se va deconta suma calculată conform H.G. 1860/2006 cu modificările și completările ulterioare, luând în considerarare distanța disponibilă pe website-ul [www.distanța.ro](http://www.distanța.ro).
* Distanţa luată în calcul la decontarea carburantului reprezintă suma distanţelor de la localitatea din care provine instituția la locul de desfăşurare a sesiunilor de instruire şi retur. Se va lua în calcul distanţa cea mai scurtă conform datelor disponibile pe website-ul [www.distanța.ro](http://www.distanța.ro)

**Pentru transport cu tren/autobuz/microbuz:**

* Biletele de tren/autobuz/microbuz sau alte documente relevante corespunzătoare perioadei de desfășurare a cursului, astfel încât să se asigure participarea;
* Decontul se va face pe baza biletului de tren/autobuz/microbuz dus – întors în original. Pentru tren, în cazul în care deplasarea, pe timp de noapte peste 300 km, se face cu vagon de dormit, ordinul de deplasare va include precizarea "Se deplasează cu vagon de dormit.“ Transportul cu trenul se decontează clasa a-II a pentru distanţe mai mici de 300 km şi clasa I pentru distanţe mai mari de 300 km, conform H.G. 1860/2006 cu modificările și completările ulterioare.

Ordinele de deplasare trebuie să fie semnate şi ştampilate de către instituţia de la care provine participantul, precum şi de către unitatea de cazare la care a fost cazat acesta, şi să nu depăşească perioada de desfăşurare a sesiunii respective;

**Ofertantul va propune un program de cursare** ce va fi agreat de către Autoritatea Contractantă pentru cursurile menţionate mai sus, cu precizarea următoarelor informaţii:

* descrierea programului de curs, a tematicii şi a conţinutului acestuia;
* detalii de organizare a cursului (săli folosite, unități de cazare, durată, număr de sesiuni, număr de formatori şi calificarea acestora, număr participanţi etc);
* descrierea rezultatelor aşteptate;
* resurse puse la dispoziţie de Prestator;
* resurse necesare din partea ONRC.

Ofertantul va prezenta în oferta care va fi depusă descrierea detaliată a procedurilor de sustinere a cursurilor pe care le propune în cadrul proiectului care vor evidenţia în mod obligatoriu următoarele:

* modalitatea de planificare a cursurilor;
* modalitatea de desfăşurare a cursurilor;
* modalitatea de evaluare a rezultatelor cursurilor;
* modalitatea de evaluare a performanţelor instructorilor.

ONRC, împreună cu Prestatorul, vor stabili de comun acord modalitatea de prestare a serviciilor pe baza planificării proiectului şi disponibilităţii cursanţilor.

Prestatorul va elabora un plan de instruire cuprinzând numărul de zile alocate pentru fiecare curs din cele menţionate mai sus şi, eventual, cursuri suplimentare pe care le consideră necesare pentru implementarea şi acceptanţa noului sistem. Fiecare curs va trata una sau mai multe componente ale sistemului, grupate de obicei după funcţionalitate.

ONRC va stabili, la nivel intern, lista participanţilor la cursurile de instruire şi va comunica Managerului de Proiect din partea Prestatorului lista de cursanţi.

**Desfăşurarea cursurilor**

Cursurile se vor desfăşura conform planului de instruire stabilit şi agreat contractual. Cursurile se vor tine în limba română, utilizând metode interactive combinate cu metode clasice de către formatori din partea Prestatorului. Acesta va asigura infrastructura hardware, software şi suportul de curs în limba română.

Cursurile se vor face pe baza suportului de curs, livrat de Prestator fiecărui participant. Acest suport de curs va conţine exemple practice pentru o mai bună înţelegere a modului de funcţionare şi administrare a sistemului, precum şi alte detalii legate de acesta.

Încheierea cursurilor se va efectua prin testarea participanţilor. În urma acestei testări se va efectua certificarea/atestarea participanţilor. Testarea se va face pe formulare tipizate, cu întrebări de tip grilă şi/sau răspuns liber.

Pentru instruirea utilizatorilor finali vor fi utilizate suporturi de curs, create special în acest sens.

Şedinţele de instruire constau din:

* prezentarea conceptelor de către formator;
* şedinţe practice, pentru mai buna înţelegere şi utilizare a sistemului / produselor software (sisteme de operare, sisteme de gestiune a bazelor de date etc.) / echipamentelor hardware;

La sfârşitul cursului, formatorul va cere cursanţilor să completeze un Chestionar de Evaluare a Cursului.

În cadrul fiecărei sesiuni de cursare va fi inclusă o prezentare a temei orizontale „Dezvoltare durabilă, egalitate de şanse şi protecţia mediului” pentru a conștientiza participanţii de importanţa acestor subiecte în activitatea lor curentă. Astfel, prezentarea va include:

- o secțiune cu privire la importanța protecției mediului și dezvoltării durabile, problemele de mediu și tema schimbărilor climatice;

- o secțiune de promovare a egalității de șanse între femei și bărbați, a egalității de șanse pentru toți, fără discriminare în funcție de gen, rasă, origine etnică, religie, handicap, vârstă, orientare sexuală.

B. ***Servicii de instruire a administratorilor:***

a) ***de sistem, reţea, comunicaţii şi securitate*** care cuprind tematici privind administrarea sistemului, administrarea bazelor de date, administrarea utilizatorilor şi a drepturilor de acces, administrarea comunicaţiilor, asigurarea securitatii, monitorizarea performanţelor, asistenţă acordată utilizatorilor etc:

- 5 persoane

- instruirea va fi organizată pe o perioada de 25 zile

- instruirea va avea loc la sediul Autoritatii contractante, intr-o sala dotată corespunzător serviciilor de instruire.

b) ***de aplicaţii*** care au ca obiect prezentarea aplicaţiilor sistemului, a instrumentelor de dezvoltare şi tehnicilor de programare utilizate în cadrul proiectului:

- 5 persoane

- instruirea va fi organizată pe o perioada de 10 zile

- instruirea va avea loc la sediul Autoritatii contractante, intr-o sala dotată corespunzător serviciilor de instruire.

Administratorii de sistem, reţea, comunicaţii şi securitate vor fi astfel instruiţi de către Prestator astfel încât să poată asigura funcţionarea sistemului cu o asistenţă minimă din partea Prestatorului sau independent de acesta, începând cu perioada post-implementare.

În plus, ofertantul va trebui să includă în propunerea tehnică şi instruire din mers (on-the-job-training) pentru utilizatorii cheie ai ONRC, prin implicarea lor în diferite etape ale proiectului. În acest sens, ofertantul va trebui să prezinte în propunerea tehnică **metodologia prin care va asigura implicarea utilizatorilor cheie ai ONRC în derularea proiectului.**

**Ofertantul va propune un program de instruire** ce va fi agreat de către Autoritatea Contractantă pentru toate serviciile de instruire menţionate mai sus, cu precizarea următoarelor informaţii:

* descrierea programului de instruire, a tematicii şi a conţinutului acestora;
* detalii de organizare a programului de instruire
* descrierea rezultatelor aşteptate;
* resurse puse la dispoziţie de Prestator;
* resurse necesare din partea ONRC.

Ofertantul va prezenta în oferta care va fi depusă descrierea detaliată a procedurilor de instruire pe care le propune în cadrul proiectului care vor evidenţia în mod obligatoriu următoarele:

* modalitatea de planificare a instruirii;
* modalitatea de desfăşurare a instruirii;
* modalitatea de evaluare a rezultatelor instruirii;
* modalitatea de evaluare a performanţelor instructorilor.

ONRC, împreună cu Prestatorul, vor stabili de comun acord modalitatea de instruire pe baza planificării proiectului şi disponibilităţii cursanţilor.

Prestatorul va elabora un plan de instruire cuprinzând numărul de zile alocate pentru fiecare program de instruire din cele menţionate mai sus şi, eventual, programe de instruire suplimentare pe care le consideră necesare pentru implementarea şi acceptanţa noului sistem. Fiecare program de instruire va trata una sau mai multe componente ale sistemului, grupate de obicei după funcţionalitate.

ONRC va stabili, la nivel intern, lista participanţilor la cursurile de instruire şi va comunica Managerului de Proiect din partea Prestatorului lista de cursanţi.

**Desfăşurarea instruirii**

Instruirea se va desfăşura on-site, la sediul central al ONRC, precum şi off-site, conform planului de instruire stabilit şi agreat contractual. Instruirea se va tine în limba română/engleză, utilizând metode interactive combinate cu metode clasice de către instructori din partea Prestatorului. Acesta va asigura infrastructura hardware, software şi suportul de curs în limba română/engleză.

Instruirea se va face pe baza suportului de curs, livrat de Prestator fiecărui participant. Acest suport de curs va conţine, după caz, exemple practice pentru o mai bună înţelegere a modului de funcţionare şi administrare a sistemului, precum şi alte detalii legate de acesta.

Încheierea instruirii se va efectua prin testarea participanţilor. În urma acestei testări se va efectua certificarea/atestarea participanţilor. Testarea se va face pe formulare tipizate, cu întrebări de tip grilă şi/sau răspuns liber.

Pentru instruire vor fi utilizate suporturi de curs, create special în acest sens.

Şedinţele de instruire constau din:

* prezentarea conceptelor de către formator;
* şedinţe practice, pentru mai buna înţelegere şi utilizare a sistemului / produselor software (sisteme de operare, sisteme de gestiune a bazelor de date etc.) / echipamentelor hardware;

La sfârşitul programului de instruire, formatorul va cere participanților să completeze un Chestionar de Evaluare a Cursului.

În cadrul fiecărei sesiuni instruire va fi inclusă o prezentare a temei orizontale „Dezvoltare durabilă, egalitate de şanse şi protecţia mediului” pentru a conștientiza participanţii de importanţa acestor subiecte în activitatea lor curentă. Astfel, prezentarea va include:

- o secțiune cu privire la importanța protecției mediului și dezvoltării durabile, problemele de mediu și tema schimbărilor climatice;

- o secțiune de promovare a egalității de șanse între femei și bărbați, a egalității de șanse pentru toți, fără discriminare în funcție de gen, rasă, origine etnică, religie, handicap, vârstă, orientare sexuală.

## Riscuri identificate

În elaborarea ofertelor tehnice, operatorii economici trebuie să ia în calcul următoarele riscuri, care pot interveni în derularea contractului:

* Surse de ordin instituțional – factori care aparțin organizației ONRC;
* Surse de mediu legislativ – factori care provin din contextul legislativ național (legislația actuală aplicabilă);
* Surse de ordin tehnic – factori care provin din constrângeri (limitări) de tip tehnic.

Prin urmare, prezentăm o analiză calitativă a riscurilor aferente proiectului, în care s-a identificat riscul, precum și măsurile de atenuare a riscului, având în vedere impactul estimat (mic, mediu, semnificativ) și consecințele materializării riscului.

În ceea ce privește riscurile de mediu și legate de schimbările climatice, precizăm că nu există o vulnerabilitate a proiectului referitor la aceste aspecte.

| Nr. crt. | Risc identificat | Masuri de atenuare ale riscului |
| --- | --- | --- |
| 1. | Se schimba Managerul de Proiect al Ofertantului sau Autorității Contractante pe durata derularii proiectului  Probabilitate: mică | Impact: semnificativ  Consecinte: aparitia unor disfunctionalitati in gestionarea proiectului si in coordonarea echipei de proiect.  Actiuni preventive: Desemnarea unui adjunct de manager de proiect care sa cunoasca toate aspectele operationale ale proiectului si care sa poata prelua aceasta functie in cazul indisponibilitatii Managerului de Proiect desemnat initial.  Responsabili: Director General ONRC / Manager de Proiect Ofertant |
| 2. | Descompletarea echipelor pe durata ciclului de viaţa al proiectului  Probabilitate: medie | Impact: mediu  Consecinţe: un posibil impact asupra activităţilor proiectului, livrabilelor cheie, finalizării etapelor proiectului. Pierderea unor abilitaţi cheie în momente critice.  Acţiuni corective: Înlocuirea personalului/experților cât mai curând posibil sau alocarea unei perioade de tranziţie, atunci când este posibil.  Acţiuni preventive: Pregătirea şi derularea unui program intern de instruire.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 3. | Rezistenta personalului beneficiarului la schimbare  Probabilitate: medie | Impact: mediu  Consecinţe: Probleme operaţionale. Beneficiile sistemului nu pot fi valorificate complet din cauza folosirii practicilor vechi de lucru.  Acţiuni corective: problema va fi escaladată către Comitetul Director al Proiectului. Ar putea fi necesare programe de instruire suplimentare.  Acţiuni preventive: obţinerea angajamentului conducerii beneficiarului că personalul său va fi informat despre importanţa proiectului.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 4. | Modificări în aria de cuprindere a proiectului  Probabilitate: medie | Impact: mediu  Consecinţe: Posibile reevaluări ale obiectivului, costurilor si/sau etapelor proiectului.  Acţiuni corective: Reprogramarea componentelor non-critice ale proiectului pentru etapa ulterioara. Acest proces va fi desfăşurat în concordanta cu procedura de control a modificărilor.  Acţiuni preventive: Asigurarea acordului tuturor factorilor decizionali importanţi în privinţa acoperirii sistemului din faza iniţială a proiectului.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 5. | Lipsa cooperării din partea utilizatorilor  Probabilitate: mica | Nivelul de implicare a utilizatorilor este esenţial atât pentru succesul sistemului cât şi pentru acceptanţa finală.  Impact: mediu  Consecinţe: costuri suplimentare pentru proiect, cauzate de eventuala apariţie a unor noi cerinţe. Definirea eronată a unor cerinţe funcţionale.  Acţiuni corective: Escaladarea către nivelurile conducerii superioare şi obţinerea unui angajament puternic din partea Comitetului Director.  Acţiuni preventive: Utilizatorii trebuie implicaţi în activităţile proiectului. Dacă este necesar se vor efectua analize ale proiectului.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 6. | Nu se respecta termenul de implementare tehnică al proiectului.  Probabilitate: medie | Impact: mediu  Consecinte: imposibilitatea respectarii termenului de implementare specificat in Contractul de finantare  Actiuni preventive: Respectarea perioadei de analiza pentru stabilirea tuturor detaliilor pentru desfasurarea dezvoltarii in parametri stabiliti. Verificarea periodica a taskurilor in derulare.  Actiuni corective: stabilirea masurilor pentru recuperarea timpului pierdut in etapele anterioare. Incheierea de acte aditionale la contractul de finantare.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 7. | Soluția finală nu respecta intocmai cerintele clientului  Probabilitate: medie | Riscul apare atunci cand Prestatorul nu a inteles exact ce doreste clientul sau cand nu sunt respectate specificatiile functionale ale proiectului.  Impact: Semnificativ  Actiuni preventive: Validarea tuturor etapelor intermediare, astfel incat sa se poata observa cat mai rapid orice deviatie si pentru a se putea lua masurile necesare pentru corectarea deviatiilor.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 8. | Soluția finală nu funcționează corespunzător  Probabilitate: medie | Impact: Mediu  Actiuni preventive: stabilirea unei etape de testare interna a fiecarei componente livrate, apoi a unei testari integrate.  Actiuni corective: Asigurarea unei marje de timp pentru rezolvarea bugurilor sau problemelor apărute, existența unei echipe de testare care sa descopere toate bugurile/problemele existente.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 9. | Neagrearea unui plan formal pentru testarea functionala a sistemului informatic, bazat pe scenarii clare de testare, ceea ce poate duce la prelungirea excesiva a perioadei de testare, sau la aparitia unor noi cerinţe introduse sub formă de observatii de testare. Prelungirea perioadelor de testare afecteaza si planificarea activitatilor expertilor pentru managementul proiectului.  Probabilitate: medie | Impact: Mediu  Actiuni preventive: Urmărirea strategiei de testare si acceptanta pentru sistemul informatic prezentată de către Prestator. Intocmirea unor scenarii de testare si acceptanta agreate de ambele parti, care sa usureze activitatea de testare.  Stabilirea unei strategii de testare si acceptanta imediat dupa demararea proiectului de implementare a solutiei informatice.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |
| 10. | Existenta unor divegente de opinie de natura tehnica între expertii ONRC si expertii tehnici ai Prestatorului, care sa determine intarzierea finalizarii unor activitati din proiect.  Probabilitate: medie | Impact: Mediu  Actiuni preventive: Stabilirea exacta a responsabilitatilor si a nivelului de autoritate pentru fiecare din expertii / specialistii celor doua organizatii. Derularea unor intalniri in care sa fie prezentate si discutate opiniile expertilor si specialistilor celor doua organizatii. Derularea unei sesiuni de instruire preliminare pentru prezentarea tehnologiilor utilizate în proiect.  Actiuni corective: Implicarea Managerului de Proiect al ONRC si a Managerului de Proiect al Ofertantului pentru medierea eventualelor dispute.  Responsabili: Manager de Proiect ONRC, Manager de Proiect Ofertant |

Ofertantul va identifica și alte riscuri față de cele principale, relevate mai sus. În oferta se vor prezenta recomandări/propuneri de reducere sau eliminare a riscurilor menționate și a celor identificate de către Ofertant și care ar putea afecta implementarea proiectului.

## Cerințe specifice

Pentru toate componentele software dezvoltate si/sau pentru toate aplicatiile software propuse pentru desfasurarea contractului, Prestatorul va respecta urmatoarele cerinte:

* Toate licentele software necesare implementarii sistemului vor fi perpetue, in proprietatea ONRC pentru totdeauna de la momentul platii, respectiv orice componenta software furnizata va putea sa fie folosita in mod legal pentru o perioada nedefinita de timp, in care cerintele/functionalitatile minimale din prezentul document trebuie sa ramana active, pentru sistemele ofertate si pentru un numar nelimitat de utilizatori. Nu se accepta alte tipuri de licentiere software, inclusiv nu se accepta urmatoarele: leasing, inchiriere, licentiere temporara indiferent de perioada de timp ofertata, licentiere cloud, etc.
* Toate componentele software se vor instala pe echipamentele prezentate in caietul de sarcini, fara a exista nici o componenta in afara sistemului prezentat in cadrul acestui caiet de sarcini. Nu se vor accepta aplicatii sau sisteme care interactioneaza cu entitati din afara retelei ONRC, inclusiv nu se accepta sisteme care sa interactioneze cu sistemele producatorilor, sisteme de tip cloud public (extern ONRC), etc. Exceptie fac cazurile in care pentru buna functionare si mentenanta aplicatiilor si componentelor ofertate si pentru buna indeplinire a cerintelor tehnice, este nevoie de interactiunea cu site-urile producatorilor sau alte site-uri (de exemplu: site-uri de update-uri pentru sistemul de operare sau aplicatii, site-uri de unde este nevoie de componente sau versiuni noi ale aplicatiilor furnizate, site-uri de firmware, BIOS, drivere, knowledge base ale producatorilor de echipamente – in orice situatie este obligatoriu ca aceste site-uri sa fie cele oficiale indicate de producatori). De asemenea, la exceptii se incadreaza si conectivitatea specifica sistemului, asa cum este prezentata in acest document.

Pe parcursul desfasurarii contractului, cat si in timpul perioadei de garantie si a asigurarii suportului pentru platforma software, ONRC isi rezerva dreptul sa verifice oricand orice livrabil realizat de Prestator, inclusiv cod sursa, proceduri de instalare, modificari in sisteme, documentatie, etc. Pentru orice neconcordanta, Prestatorul este obligat sa remedieze problema semnalata si eventual sa updateze documentele aferente.

Criteriile de acceptanţă de la fiecare nivel de testare vor fi stabilite în acord cu Autoritatea Contractantă intr-un plan de testare care va fi propus de prestator si validat de Autoritatea Contractanta, astfel încât să se asigure conformitatea implementarii solutiei cu specificaţiile functionale stabilite.

Receptii si teste de acceptanta:

* Receptii cantitative a componentelor sistemului informatic (echipamente hardware, produse software, alte componente software, instruire)
* Punerea in functiune a infrastructurii hardware si a platformei de virtualizare si receptia calitativa prin teste de baza a functionarii acestora
* Receptie finala a sistemului informatic prin testarea intregului sistem integrat pe baza unui plan de testare agreat;

## Evaluarea performantei Contractantului

Performanta Contractantului va fi evaluata pe durata implementarii proiectului pe baza urmatorilor indicatori de performanta. Aceste informații vor fi utilizate inclusiv pentru eliberarea documentului constatator la finalul prestării serviciilor.

Contractantul va ține evidența valorilor asociate indicatorilor de performanță și va include informații referitoare la nivelul de performanță înregistrat în toate rapoartele și documentele întocmite pentru realizarea întâlnirilor de pe durata derulării Contractului, așa cum sunt acestea descrise în Caietul de Sarcini.

Astfel, Autoritatea Contractantă va utiliza indicatori de performanță mentionati in Anexa 2 a prezentului caiet de sarcini. Performanta finala a Contractantului va fi calculata ca medie aritmetica a indicatorilor.

# Cerinte experti cheie

## Structura echipei de proiect

Prestatorul va asigura o echipa formata din expertii solicitati, care vor fi responsabili de realizarea activităţilor din cadrul contractului, in conformitate cu cerintele beneficiarului.

Prestatorul poate suplimenta numărul de resurse alocat activităților pe perioada derulării proiectului, fără însă a solicita modificarea valorii contractului.

Echipa de proiect a Prestatorului va trebui să conțină cel puțin experți care să acopere următoarele roluri:

1. **Manager de proiect** – pentru gestionarea şi controlul proiectului, urmărirea dezvoltării şi rezultatelor proiectului, măsuri corective, dacă şi unde este necesar – rol acoperit de un expert certificat;
2. **Manager de proiect adjunct** – pentru suplinirea managerului de proiect când acesta nu este disponibil sau în situațiile in care este necesară prezența acestuia în activități importante desfăsurate în paralel – rol acoperit de un expert certificat;
3. **Arhitect soluție** – pentru designul soluţiei, inclusiv generarea şi aprobarea specificaţiilor de design – rol acoperit de un expert certificat;
4. **Coordonator analiza** – pentru coordonarea tehnică a echipei de analiza – rol acoperit de un expert certificat;
5. **Analist de business** – care să înțeleagă sistemul, tipul de informații existente in el și structura acestora, să extragă cerintele detaliate și să elaboreze specificatiile functionale – rol acoperit de experți certificați;
6. **Expert integrare** – pentru analiza sistemelor existente, elaborarea specificatiilor si riscurilor specifice, instalarea si configurarea produselor aferente subsistemelor – rol acoperit de un expert certificat;
7. **Expert implementare software** – pentru implementarea soluțiilor software ofertate – rol acoperit de un expert certificat;
8. **Expert baze de date** – pentru managementul bazelor de date folosite pentru proiect, inclusiv al structurii acestora – rol acoperit de un expert certificat;
9. **Coordonator dezvoltare software** – pentru coordonarea tehnica a echipei care va realiza dezvoltarea componentelor funcționale care nu pot fi implementate utilizând produse comerciale existente – rol acoperit de un expert certificat;
10. **Expert dezvoltare aplicatii software** – pentru dezvoltarea componentelor software – rol acoperit de experți certificați;
11. **Expert dezvoltare aplicatii mobile** – pentru dezvoltarea componentelor software aferente aplicatiilor mobile – rol acoperit de un expert certificat;
12. **Coordonator testare** – pentru coordonarea tehnica a echipei care va realiza testarea – rol acoperit de un expert certificat;
13. **Expert testare software** – pentru testarea componentelor dezvoltate și asigurarea calității componentelor – rol acoperit de experți certificați;
14. **Expert infrastructura / virtualizare** – pentru instalarea, configurarea si managementul sistemului de virtualizare ofertat si al componentelor de infrastructura – rol acoperit de un expert certificat;
15. **Expert comunicatii** – pentru prestarea de activitati specifice proiectarii si implementarii din punct de vedere securitate a comunicatiilor sistemului informatic – rol acoperit de un expert certificat;
16. **Expert testare de securitate** – pentru testarea de securitate a componentelor dezvoltate si a sistemului in ansamblul sau si identificarea vulnerabilitatilor – rol acoperit de un expert certificat;
17. **Expert securitatea informatiei** – pentru crearea, configurarea si implementarea solutiilor de securitate a datelor și a sistemelor informatice – rol acoperit de experți certificați;
18. **Expert instruire** – pentru organizarea structurii instruirii, crearea materialelor de instruire și a cursurilor, sustinerea cursurilor – rol acoperit de un expert certificat;
19. **Coordonator suport tehnic** – pentru gestionarea serviciilor de suport tehnic pe perioada de garantie a sistemului informatic ce va fi implementat – rol acoperit de un expert certificat;
20. **Expert suport** **tehnic** – pentru activitati de suport si asistenta tehnica – rol acoperit de experți certificați;

ONRC va oferi suport tehnic pentru implementare prin intermediul personalului propriu, punând la dispoziţia Prestatorului informaţiile necesare despre infrastructura existentă şi, de asemenea, cu privire la sursele și specificul datelor existente în cadrul organizației.

Echipa de proiect din partea ONRC se va implica în întregul proces de implementare, pentru a acumula experiența practică necesară pentru operarea și administrarea ulterioară a sistemului informatic.

## Responsabilitatile expertilor cheie

### Manager de proiect – 1 persoana

Responsabilitati:

* Activitati specifice de management de proiect (legat de obiectul contractului)
* Punct principal de contact in relaţia cu beneficiarul
* Managementul contractului
* Managementul proiectului in ansamblul sau, managementul ariei de cuprindere, managementul schimbarilor, planificarea generala a proiectului, managementul riscurilor, managementul problemelor, managementul comunicarii
* Asigurarea resurselor proiectului
* Managementul, organizarea, alocarea si planificarea echipei de proiect
* Identificarea riscurilor si propunere de solutii pentru diminuarea/evitarea riscurilor
* Rezolvarea problemelor in scopul evitarii situaţiilor de criza
* Urmarirea respectarii tuturor termenelor conform planului de proiect
* Analiza modalitatii prin care livrabilele proiectului corespund cerintelor de business
* Realizarea rapoartelor periodice / ad-hoc ale proiectului.
* Elaborarea planurile de calitate
* Verificarea si asigurarea calitatii livrabilelor

### Manager de proiect adjunct – 1 persoana

Responsabilitati:

* Activitati specifice de management de proiect (legat de obiectul contractului), atunci cand managerul de proiect nu este disponibil
* Punct secundar de contact in relaţia cu beneficiarul
* Rezolvarea problemelor in scopul evitarii situaţiilor de criza
* Urmarirea respectarii tuturor termenelor conform planului de proiect
* Analiza modalitatii prin care livrabilele proiectului corespund cerintelor de business
* Verificarea si asigurarea calitatii livrabilelor

### Arhitect solutie – 1 persoana

Responsabilitati:

* Definirea arhitecturii generale a solutiei
* Definirea, impreuna cu coordonatorul tehnic, a solutiilor detaliate pentru componentele sistemului
* Definirea arhitecturii de integrare a componentelor
* Definirea modelului de date al subsistemului și pentru procesele de extragere, transformare și încărcare în noile structuri de date
* Identificarea riscurilor si problemelor tehnice si a solutiilor de rezolvare

### Coordonator analiza – 1 persoana

Responsabilitati:

* Coordoneaza activitatile de analiza a cerintelor de business, elaborare a documentelor de specificatii functionale si a scenariilor de testare
* Activitati de implementare, asistenta si suport tehnic
* Suport acordat utilizatorilor cheie pentru testarea de acceptanta a sistemului

### Analist de business – 3 persoane

Responsabilitati:

* Analiza cerintele de business
* Realizarea documentelor de specificatii functionale si a scenariilor de testare
* Activitati de implementare, asistenta si suport tehnic
* Suport acordat utilizatorilor cheie pentru testarea de acceptanta a sistemului

### Expert integrare – 1 persoana

Responsabilitati:

* activitati specifice integrarii noului sistem in cadrul sistemului actual ONRC;
* activitati specifice implementarii bazelor de date aferente noului sistem;
* asistenta si suport tehnic;
* adaptări/actualizări/îmbunătăţiri/extinderi ale interfetelor existente sau dezvoltate intre componentele sistemului;
* testarea interfetelor, testarea sistemului;
* crearea/ actualizarea documentatiilor de administrare;

### Expert implementare software – 1 persoana

Responsabilitati:

* Activitati specifice de instalare si configurare a produselor software ofertate
* Crearea si actualizarea documentatiilor de administrare a produselor software
* Activitati de implementare, asistenta si suport tehnic

### Expert baze de date – 1 persoana

Responsabilitati:

* Activitati specifice de instalare si administrare baze de date in arhitecturi redundante
* Activitati specifice replicarii datelor din baza de date
* Asistenta si suport tehnic
* Testare
* Crearea/ actualizarea documentatiilor de administrare

### Coordonator dezvoltare software – 1 persoana

Responsabilitati:

* Coordonarea echipei si a activitatilor de dezvoltare de aplicatii software
* Asigura suport tehnic in activitatile de implementare
* Rezolva disfunctionalitati software (bug-uri)
* Asigura suport tehnic in perioada de garantie
* crearea/ actualizarea documentatiilor

### Expert dezvoltare aplicatii software – 6 persoane

Responsabilitati:

* Activitati specifice privind dezvoltarea de aplicatii software, pe baza documentelor de analiza, specificatii functionale, specificatii tehnice, arhitectura sistem
* Testare unitara (interna)
* Suport in activitatile de implementare
* Rezolvarea disfunctionalitatilor software (bug-uri)
* Asigurarea suportului tehnic in perioada de garantie
* Crearea/ actualizarea documentatiilor

### Expert dezvoltare aplicatii mobile – 1 persoana

Responsabilitati:

* Activitati specifice privind dezvoltarea de aplicatii mobile
* Rezolvarea disfunctionalitatilor software (bug-uri)
* Asigurarea suportului tehnic in perioada de garantie
* Crearea/ actualizarea documentatiilor

### Coordonator testare – 1 persoana

Responsabilitati:

* Coordonarea echipei si activitatilor de testare
* Activitati specifice testarii de aplicatii software
* Implementarea planurilor, scenariilor si cazurilor de test
* Activitati de testare componente si testare functionala
* Intocmirea si livrarea rapoartelor de testare si implementare

### Expert testare software – 2 persoane

Responsabilitati:

* Prestarea de activitati specifice testarii de aplicatii software
* Implementarea planurilor, scenariilor si cazurilor de test
* Activitati de testare componente si testare functionala
* Intocmirea si livrarea rapoartelor de testare si implementare

### Expert infrastructura / virtualizare – 1 persoana

Responsabilitati:

* activitati specifice implementarii infrastructurii / sistemului de virtualizare aferente sistemului;
* asistenta si suport tehnic;
* adaptări/actualizări/îmbunătăţiri/extinderi/ configurari ale sistemului de virtualizare;
* testarea sistemului de virtualizare;
* crearea/ actualizarea documentatiilor de administrare;

### Expert comunicatii – 1 persoana

Responsabilitati:

* Activitati specifice proiectarii si implementarii din punct de vedere securitate a comunicatiilor sistemului informatic implementat, atat din punct de vedere software, cat si hardware
* Activitati de proiectare, instalare si configurare retele de comunicatie redundante
* Asistenta si suport tehnic
* Crearea/ actualizarea/ verificarea documentatiilor

### Expert testare de securitate – 1 persoana

Responsabilitati:

* Prestarea activitatilor specifice testarii de securitate a sistemelor informatice
* Testarea eficientei controalelor de securitate implementate in proiect
* Identificarea vulnerabilitatilor existente la nivelul sistemului
* Implementarea planurilor, scenariilor si cazurilor de test
* Activitati de testare componente si testare functionala
* Intocmirea si livrarea rapoartelor de testare si implementare

### Expert securitatea informatiei – 1 persoana

Responsabilitati:

* Definirea solutiei de securitate in etapa de analiza
* Configurarea din punct de vedere al securitatii a sistemelor informatice
* Consultanta de specialitate pentru echipa de proiect in timpul derularii proiectului
* Realizarea planului de securitate a sistemului informatic
* Realizarea planurilor de continuitate si recuperare in caz de dezastru
* Instructaj pentru administratorii sistemului informatic
* Instructaj privind constientizarea securitatii pentru utilizatorii sistemului informatic
* Intocmirea si livrarea rapoartelor de testare si implementare

### Expert instruire – 1 persoana

Responsabilitati:

* Organizarea structurii de instruire
* Derularea activitati de instruire utilizatori;
* Pregatirea materialelor de curs si a testelor;
* Pregatirea raportului de curs.

## Cerinte minime obligatorii ale expertilor cheie

Numarul minim de persoane necesar pentru fiecare expert este mentionat in dreptul acestuia. Fiecare dintre persoanele propuse trebuie sa indeplineasca integral toate cerintele minime aferente expertului (profilului de persoana) pentru care au fost nominalizate. Nu se accepta indeplinirea cerintelor minime aferente unui expert prin cumul de catre mai multe persoane.

### Manager de proiect – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind managementul de proiect dovedite prin certificare recunoscuta la nivel national / international
* Experiența specifica in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Manager de proiect adjunct – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind managementul de proiect dovedite prin certificare recunoscuta la nivel national / international
* Experiența specifica in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Arhitect solutie – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente in domeniul arhitecturilor de tip Enterprise dovedite prin certificare recunoscuta la nivel national / international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Coordonator analiza – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind analiza de business dovedite prin certificare in domeniu
* Competente privind managementul si modelarea proceselor de business dovedite prin certificare in domeniu
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Analist de business – 3 persoane

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind analiza de business dovedite prin certificare in domeniu
* Experiența specifica in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert integrare – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Compentente in domeniul arhitecturilor de tip Enterprise, dovedite prin certificare recunoscuta la nivel national/ international
* Competente privind platforma de gestiune a arhivei utilizata in cadrul SAE dovedite prin certificare/diploma recunoscuta la nivel national/ international
* Competente privind administrarea bazelor de date dovedite prin certificare/diploma recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert implementare software – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente in domeniul IT pentru cel putin 2 din urmatoarele domenii: sisteme de operare / aplicatii software / portal / servere de aplicatie, dovedite prin certificari recunoscute la nivel national / international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert baze de date – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta;
* Competente privind administrarea bazelor de date in configuratie cluster dovedite prin certificare in domeniu recunoscuta la nivel national/ international
* Competente privind optimizarea performantei bazelor de date dovedite prin certificare in domeniu recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Coordonator dezvoltare software – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind o metodologie de dezvoltare software, recunoscuta la nivel national/ international, dovedite prin certificare in domeniu
* Competente privind dezvoltarea de software dovedite prin certificare in domeniu obtinute la nivel national sau international (pentru absolvenții de studii superioare la facultăți cu profil informatic/calculatoare, este suficientă diploma de absolvire).
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert dezvoltare aplicatii software – 6 persoane

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind dezvoltarea de software dovedite prin certificare in domeniu obtinute la nivel national sau international (pentru absolvenții de studii superioare la facultăți cu profil informatic/calculatoare, este suficientă diploma de absolvire)
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert dezvoltare aplicatii mobile – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind dezvoltarea de aplicatii mobile pentru iOS / Android dovedite prin certificare in domeniu
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Coordonator testare – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert testare software – 2 persoane

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind testarea sistemelor informatice, dovedite prin certificare in domeniu recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert infrastructura / virtualizare - 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta;
* Compentente in domeniul sistemelor de operare de tip Enterprise, dovedite prin certificare recunoscuta la nivel national/ international
* Competente in domeniul IT pentru cel putin unul din urmatoarele domenii: servere / sisteme de stocare , dovedite prin certificari recunoscute la nivel national / international
* Competente privind sisteme de virtualizare, dovedite prin certificare recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert comunicatii – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta;
* Competente privind implementarea, administrarea si depanarea tehnologiilor avansate de rutare si switching, dovedite prin certificare recunoscuta la nivel national/ international
* Compentente privind administrarea si gestiunea securitatea retelelor dovedite prin certificare recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert testare de securitate – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente privind testarea de securitate a sistemelor informatice, dovedite prin certificare recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert securitatea informatiei – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta;
* Competente privind securitatea datelor si a sistemelor informatice, dovedite prin certificare recunoscuta la nivel national/ international
* Experiența specifica in cel putin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

### Expert instruire – 1 persoana

* Absolvent studii superioare finalizate cu diploma de licenta
* Competente de instruire, dovedite prin diploma de formator
* Experiența specifica in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

Ofertantii trebuie sa prezinte in oferta tehnica, pentru fiecare expert solicitat urmatoarele informatii/documente:

* Numele persoanei propuse pentru fiecare pozitie (de exemplu pentru dezvoltator software sunt cerute minim 2 pozitii si pentru fiecare dintre acestea trebuie nominalizata cate o persoana),
* Declaratia de disponibilitate semnata de persoana propusa (in cazul în care aceasta nu este angajat al Prestatorului)
* CV
* Documente justificative relevante care demonstreaza indeplinirea cerintelor:
* copiile documentelor relevante care demonstreaza indeplinirea cerintelor referitoare la studiile, expertiza si experienta specifica relevanta solicitata si prezentata in CV, cum ar fi:
  + copii diplome de studii, certificari, alte diplome relevante,
  + copii ale recomandarilor emise de beneficiarii finali ai proiectelor, semnate sau contrasemnate de catre Autoritatea Contractanta/beneficiarul privat in calitate de beneficiar final, sau alte documente edificatoare, din care sa reiasa activitatile desfasurate si care sa evidentieze experienta profesionala specifica similara

Copiile documentelor trebuie sa fie confirmate pentru conformitate cu originalul documentelor respective. Certificatele/ diplomele/ documentele justificative emise in alta limba decat limba română vor fi prezentate in limba de origine, insotite de traducerea autorizata in limba română.

Ofertantul are obligatia ca in cadrul ofertei depuse, sa mentioneze cel putin urmatoarele elemente pentru a demonstra experienta minima in proiecte a personalului propus:

* Denumirea proiectului, beneficiarul și perioada de realizare a proiectelor în care a acumulat experiența solicitată, precum și obiectivele proiectului respectiv.
* Date de contact ale unei persoane de la beneficiarul final al proiectului care poate confirma experienta similara
* Activitatile prestate de catre persoana propusa
* Perioada de timp in care persoana propusa a desfasurat activitatile mentionate in cadrul proiectului propus

Autoritatea Contractantă are dreptul de a verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți si de a solicita și alte documente/ informații care să clarifice experiența similara respectiva.

In urma verificarii exactitatii informațiilor și a dovezilor furnizate de catre ofertanți, Autoritatea Contractantă poate solicita și alte documente/informații care să clarifice experiența profesionala solicitata. De asemenea, Autoritatea Contractantă isi rezerva dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experienta profesionala, in vedere confirmarii celor prezentate de catre ofertanti.

Persoanele propuse vor fi de preferat vorbitori de limba romana la un nivel avansat. In cazul persoanelor care nu sunt vorbitori de limba română, prestatorul va pune la dispoziție interpreți/ traducători autorizați in domeniul IT în vederea comunicării cu personalul autorității contractante și în vederea traducerii livrabilelor ce trebuie predate autorității contractante în limba română. Ofertantul declarat castigator este responsabil de acoperirea tuturor cheltuielilor referitoare la interpreți/ traducători/ traduceri.

Pentru persoanele propuse care au calitatea de salariati ai ofertantului, se va prezenta în mod obligatoriu orice document prin care sa se demonstreze relatia contractuala dintre persoanele nominalizate si ofertant (extras Revisal/ contract de munca, etc.). În cazul în care se propune personal care nu este salariat al Prestatorului, fiecare astfel de persoana va completa si va semna o declarație de disponibilitate semnata de aceasta, cu referire stricta la obiectul contractului ce face obiectul prezentei proceduri.

# Modalitatea de întocmire a ofertei

*Pentru fiecare componentă, hardware sau software, se va preciza în mod clar denumirea, producătorul, cantități, capacități, referințe la materiale din care să reiasă în mod clar soluția ofertată.*

*Pentru toate echipamentele hardware, ofertanții vor include în ofertă configurațiile propuse astfel încât să poată fi verificat fiecare subsistem (exemplu tipul de procesor propus sau tipul de memorie propus).*

*Nicio componentă software din cele ofertate nu trebuie să aibă vreo limitare de timp de licențiere care să prevină folosirea acesteia după o anumită perioadă de timp sau să condiționeze continuarea folosirii acesteia de achiziționarea de suport sau servicii suplimentare.*

*Soluția propusă nu trebuie să aibă alte limitări de licențiere sau de altă natură care să prevină folosirea acesteia în scopul în care a fost achiziționată.*

*Oferta se va prezenta într-un format în care să permită copierea textului cu formatare.*

*Oferta va cuprinde obligatoriu fisele tehnice, manualele sau/şi ghidurile de prezentare sau orice alte documente relevante pentru toate echipamentele, componentele și produsele software prezentate, astfel încat să rezulte faptul că acestea respecta cerințele minime din prezentul caiet de sarcini.*

*Propunerea tehnică va fi elaborată astfel încât să rezulte că sunt îndeplinite în totalitate cerinţele aferente Caietului de sarcini. Propunerea tehnică trebuie să reflecte asumarea de către ofertant a tuturor cerinţelor si obligaţiilor prevăzute în Caietul de sarcini.*

*Propunerea tehnică va respecta obligatoriu următoarele cerințe:*

1. *Ofertantul va prezenta o singură ofertă cu respectarea cerinţelor Caietului de Sarcini.*
2. *Propunerea tehnica va fi întocmita în conformitate cu solicitarile din caietul de sarcini, acestea fiind considerate minime si obligatorii.*
3. Ofertantul va detalia modul in care echipamentele, componentele si produsele software oferite raspund la fiecare dintre cerintele enumerate in parte, specificând în clar identificatorul unic producător asociat fiecărui echipament, numărul de echipamente ofertate pentru fiecare tip de echipament, configurația, functionalitatile si optiunile acestora. Separat, vor fi prezentate de asemenea si functionalitatile suplimentare, dacă este cazul. Nu se acceptă echipamente scoase din fabricație sau la finalul ciclului de vânzare. Se acceptă livrarea doar de echipamente noi.
4. Ofertantul va detalia lista licențelor propuse în propunerea tehnică, specificând în clar numele licenței de la producător, ediția, producătorul, cantitatea și unitățile de licențiere specifice producătorului, precum și corelarea acestora cu cerințele caietului de sarcini.
5. *Prezentarea modului de indeplinire a cerintelor functionale si tehnice solicitate in caietul de sarcini: ofertantul va prezenta sub forma tabelara, explicatiile, valorile si documentele doveditoare pentru toate caracteristicile solicitate in caietul de sarcini (matrice de complianta), raspunzand punct cu punct la toate cerințele prezentei documentații si detaliind soluția ofertată într-un mod care sa permita verificarea cu ușurință a conformității.*
6. *Propunerea tehnica va contine descrierea metodologiei de implementare ce va fi aplicată pe durata proiectului, care trebuie sa fie de tip iterativ si bazata pe o metodologie recunoscuta la nivel international. Daca este cazul se va prezenta contribuitia fiecarui membru al grupului de operatori economici/subcontractant, precum si distribuirea si interactiunea sarcinilor si responsabilitatilor dintre acestia.*
7. *Propunerea tehnica va contine descrierea procedurii de gestiune a schimbării.*
8. *În cadrul propunerii tehnice, se va prezenta obligatoriu un grafic de execuţie, în format Gantt în care trebuie să includă cel puțin toate activitățile necesare pentru implementarea cu succes a proiectului, inclusiv dependențele dintre acestea, respectiv rezultatele acestora, pentru fiecare activitate a proiectului, se vor menţiona resursele umane alocate, precum şi nivelul de implicare al fiecărei resurse în activităţile proiectului (pentru fiecare activitate în parte), precizând fazele/subfazele de bază de realizare a activităților, evidențiindu-se reperele de referință, succesiunea activităţilor şi numărul de zile/om de implicare în proiect pentru experţi.*
9. *Descrierea părților de contract subcontractate, a interacţiunii dintre ofertant şi subcontractor/i, precum şi o descriere detaliată a serviciilor ce vor fi subcontractate.*
10. *Oferta financiara va fi prezentata detaliat si va contine preturile unitare pentru fiecare echipament, produs software sau serviciu inclus in propunerea tehnica.*
11. *Propunerea tehnica va contine si alte informaţii considerate semnificative de ofertant sau orice alte constrângeri, pentru evaluarea corespunzătoare a propunerii tehnice.*
12. *Ofertantul are obligatia de a detalia modul de abordare si gestionare a relatiei cu subcontractorii, in raport cu activitatile subcontractate (daca este cazul).*

**Notă - condiții generale și particulare:**

1. Prin depunerea unei oferte, ofertantul acceptă în prealabil condiţiile generale şi particulare care guvernează acest contract, după cum sunt acestea prezentate în Documentaţia de atribuire, ca singură bază a acestei proceduri de atribuire, indiferent care sunt condiţiile proprii de vânzare ale ofertantului.
2. Ofertanţii au obligaţia de a analiza cu atentie documentaţia de atribuire si să pregătească oferta conform tuturor instrucţiunilor, formularelor, prevederilor contractuale şi Caietului de sarcini conţinute în această documentaţie.
3. Niciun cost suportat de operatorul economic pentru pregătirea şi depunerea ofertei nu va fi rambursat. Toate aceste costuri vor fi suportate de către operatorul economic ofertant, indiferent de rezultatul procedurii.
4. Prezumţia de legalitate şi autenticitate a documentelor prezentate: ofertantul îşi asumă răspunderea exclusivă pentru legalitatea şi autenticitatea tuturor documentelor prezentate în original şi/sau copie în vederea participării la procedură.
5. Analizarea de către comisia de evaluare a documentelor prezentate de ofertanţi nu angajează din partea acesteia nicio răspundere sau obligaţie faţă de acceptarea acestora ca fiind autentice sau legale şi nu înlătură răspunderea exclusivă a ofertantului sub acest aspect.

# Criterii de atribuire

Criteriul de atribuire este cel mai bun raport calitate-pret.

**ALGORITM DE CALCUL**

Evaluarea ofertelor se va face în ordinea descrescătoare a punctajului total obtinut din punctajul tehnic şi financiar, pe baza ponderilor prezentate în fişa de date a achiziţiei, pentru fiecare dintre criteriile respective.

Oferta care obtine cel mai mare număr de puncte va fi declarată câştigătoare.

Evaluarea ofertelor se va realiza pe baza urmatoarelor criterii si a punctajul aferent obtinut de fiecare oferta evaluata.

Punctajul total acordat pentru fiecare ofertă se calculează pe baza formulei:

**Punctaj Total Ofertant A = Punctaj „Pretul ofertei” Ofertant A + Punctaj „Propunerea tehnica - Experiența profesionala a personalului” Ofertant A + Punctaj “Propunerea tehnică – Capabilitati solutie tehnica” Ofertant A + Punctaj „Propunerea tehnica - Demonstrarea unei metodologii adecvate de implementare a contractului” Ofertant A**

Criteriile de evaluare propuse sunt:

|  |  |  |
| --- | --- | --- |
| **Nr. crt.** | **Factori de evaluare** | **Pondere %** |
| 1. | Pretul ofertei | 50 |
| 2. | Propunere tehnică – Capabilitati solutie tehnica | 30 |
| 3. | Propunerea tehnica – Experiența profesionala a personalului | 15 |
| 4. | Propunerea tehnică – Demonstrarea unei metodologii adecvate de implementare a contractului | 5 |
| Total | | 100 |

Notă: toate calculele se vor face cu 4 zecimale, iar rotunjirile se vor face la 2 zecimale, conform functiei ROUND din Microsoft Excel – ROUND(formula, 2) – pentru fiecare din calculele aferente evaluarii ofertelor. Functia ROUND se va aplica pentru intreaga formula de calcul, pentru fiecare etapa a calculului.

Pentru criteriile de evaluare 3 si 4, fiecare subfactor va fi apreciat in functie de calificativul foarte bine/bine, acceptabil. Comisia de evaluare va acorda calificativul luand in considerare liniile directorare prezentate in tabele aferente. Punctajul tehnic total al ofertei se calculeaza prin insumarea punctajelor tehnice obtinute in urma aplicarii fiecaraui subfactor de evaluare. Punctajul aferent unui subfactor de evaluare va fi obtinut prin acordarea notei corespunzatoare calificativului obtinuit de oferta respectiva la evaluarea acelui subfactor.

În cazul în care mai multe oferte eligibile obțin același punctaj total (tehnic + financiar), atunci se va solicita o nouă ofertă financiară ofertanților clasați pe primul loc.

## Descrierea modalitatii de punctare a factorului de evaluare “Pretul ofertei”

|  |  |  |
| --- | --- | --- |
| **Factor de evaluare** | **Modalitate de punctare** | **Punctaj maxim** |
| **1. Pretul ofertei** | Punctajul financiar se acordă astfel:  a. Pentru cel mai mic dintre prețurile ofertate se acordă 50 de puncte;  b. Pentru alt preț decât cel prevăzut la litera a) se acordă punctaj astfel:  **Punctaj Financiar Ofertant A = Pret minim ofertat ÷ Pret Ofertant A × 50**  Se vor compara preturile fara TVA prezentate in propunerea financiara. | **50 puncte** |

## Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnică – Capabilitati solutie tehnica”

Numar maxim de puncte: 30 puncte.

Acordare punctajului „Capabilitati solutie tehnica” se va face in felul urmator:

|  |  |
| --- | --- |
| **Element evaluat** | **Punctaj** |
| Componenta de replicare captureaza si replica modificarile la sursa in momentul in care acestea au loc, fara sa astepte finalizarea tranzactiei. Acest procedeu este utilizat si de baza de date Oracle (procesul dbwriter) pentru a reduce semnificativ necesarul de banda utilizat, memoria consumata de procesul de replicare (deoarece nu se pastreaza tranzactia la sursa pana la finalizarea acestea) si din acelasi motiv, pentru a reduce semnificativ intarzierea aplicarii datelor la destinatie. | 1.5 |
| Componenta de replicare include funcționalități de comparare și reparare ale datelor, astfel încât să fie facila introducerea de noi tabele în replicare si repararea sincronizarii tabelelor existente în replicare. | 1.5 |
| Componenta de gestiune a documentelor permite stocarea compresata si criptata a fisierelor in depozitul de documente vor sta in forma compresata pentru economisirea spatiului si criptat cu standard AES256 sau echivalent | 1.5 |
| Componenta de gestiune a documentelor include la nivelul de depozitului de documente functii de realizare a conformitatii cu standardul GDPR cum ar fi dar fara a se limita la: pseudonimizare, anonimizare, scopul preluarii datelor, nivel de securitate, categorii de date din punct de vedere GDPR, audit la nivel de inregistrare | 1.5 |
| Interfata web a componentei de gestiune a documentelor utilizatorului rezultatele căutării sub forma unei liste care cuprinde documente corespunzatoare criteriului selectat si permite cautari specifice in subsetul rezultat din cautare | 1.5 |
| Componenta de dezvoltare aplicatii mobile sa permita actualizarea in timp real a aplicatiilor instalate pe dispozitive (inclusiv corectii rapide ale aplicatiei) fara a fi necesara actualizarea in magazinul de aplicatii (app store) | 1.5 |
| Componenta de dezvoltare aplicatii mobile sa permita monitorizarea in timp real a problemelor / erorilor aparute la nivelul aplicatiilor instalate pe dispozitivele mobile cu corelarea erorii cu codul sursa al aplicatiei dezvoltate si notificarea dezvoltatorului in cazul aparitiei de erori neasteptate. | 1.5 |
| Componenta gestiune a ciclului de viata a aplicatiilor permite integrarea cu componenta testare performanta pentru gestiunea testelor de performanta | 1.5 |
| Componenta gestiune a ciclului de viata a aplicatiilor permite integrarea cu componenta testare automata pentru gestiunea si automatizarea testelor functionale | 1.5 |
| Componenta de testare automata permite reducerea timpului de testare prin executia simultana de teste distribuite; | 1.5 |
| Componenta de testare de performanta permite rularea testelor definite la nivel de API in componenta de testare automata a aplicatiilor (pentru testarea incarcarii); | 1.5 |
| Componenta de testare de performanta permite obtinerea de analize comparative intre mai multe rulari de teste cu scopul de dimensionare a capacitatii sistemului sau de testare intre versiuni diferite de software. | 1.5 |
| Componenta de testare de performanta permite localizarea, extragerea si inlocuirea valorilor dinamice din cadrul paginilor web precum id-ul de sesiune, authentication token, customer id, etc asigurand astfel acceptarea cererilor de catre serverele web supuse testarii | 1.5 |
| Componenta centrala de protectie avansata antimalware permite compararea comportamentului manifestat de rularea software-ului malițios pe diferite configurații ale mașinilor virtuale de analiză (de exemplu: versiuni diferite ale sistemului de operare, ale aplicațiilor uzuale, configurări diferite ale sistemelor de operare, actualizări aplicate sistemelor de operare, patch-uri sau service pack-uri), in vederea evaluarii cat mai exacte a impactului acestora la nivelul sistemelor aflate in exploatare | 1.5 |
| Componenta centrala de protectie avansata antimalware permite personalizarea facila a mecanismului de sandbox-ing prin operatiuni de import/export a sistemelor de operare/setului de aplicatii disponibil in mediul de tip sandbox, inclusiv prin incarcarea integrala a unor imagini de sistem de operare standard (gold image), in scopul reflectarii realitatii relevante din mediul productiv al Autoritatii Contractante la un moment dat. | 1.5 |
| Componenta de protectie a resurselor la nivel de post de lucru permite asigurarea protectiei impotriva amenintarilor de tip ransomware cu recuperarea datelor din backup. Astfel solutia trebuie sa ofere mecanisme automatizate de salvare a datelor in momentul detectiei unui element de tip ransomware, respectiv sa blocheze procesul de criptare initiat de elementul de tip ransomware si sa recupereze datele in eventualitatea in care procesul de criptare a fost declansat | 1.5 |
| Componenta de redistributie a accesului la serviciile de aplicatie permite extinderea functionalitatilor native prin limbaj de scripting care sa ofere suport pentru :   * folosirea declaratiilor conditionale (if/then) si a buclelor (for, while); * generarea de alerte si executia de script-uri pe baza diferitelor tipuri de evenimente; * alterarerea cererii sau a raspunsului pe baza de: origine, tip, semnatura sau datele continute in cerere/raspuns   in scopul personalizarii solutiei pentru nevoi punctuale ce vor fi identificate in dreularea proiectului | 1.5 |
| Componenta de management a datelor de audit ofera mecanisme integrate de anonimizare si mascare a datelor confidentiale din afisarea rezultatelor de cautare asupra seturilor de date de audit, in scopul respectarii reglementarilor legale in vigoare, inclusiv a conformitatii cu GDPR | 1.5 |
| Componenta de management a datelor de audit include mecanisme de analiza bazata pe algoritmi matematici (Machine Learning), respectiv permite definirea propriilor modele algoritmice de analiza plecand de la modelele componentei si/sau prin integrarea de limbaje Opensource dedicate (unelte de tip SDK, Toolkit, etc integrate), in scopul minimizarii efortului de valorificare a informatiei si a asigurarii unei flexibilitati sporite in gestiunea datelor de audit | 1.5 |
| Componenta de management al datelor de audit permite colectarea, analiza si corelarea datelor de la toate sistemele, aplicatiile si serviciile din infrastructura, fara a se baza pe un sistem de baza de date suport, depasind astfel limitarile de performanta generate de structurarea datelor intr-un sistem relational de baza de date | 1.5 |
| **Total** | **30** |

Ofertantii vor descrie in detaliu in cadrul ofertei modul de functionare a componentelor sistemului cu referire la aspectele supuse evaluarii acestui criteriu de atribuire. In cazul in care descrierea tehnica este incompleta (adica nu acopera aspectele ce vor fi evaluate sau nu sunt punctate functionalitatile utilizate in acest sens de la nivelul componentelor software de baza), Achizitorul isi rezerva dreptul de a nu acorda punctajul aferent in cadrul acestui criteriu de atribuire. Doar simpla mentiune, nejustificata in detaliu din punct de vedere tehnic in cadrul ofertei, ca solutia indeplineste cerintele nu va fi luata in considerare de catre Achizitor.

## Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnica - Experiența profesionala a personalului”

Prin acest factor se va realiza evaluarea experientei profesionale a persoanelor propuse pentru anumite pozitii de experti solicitate in Caietul de sarcini. Persoanele pentru care se va face evaluarea vor avea responsabilitatea realizarii efective a activitatilor si proceselor de executie aferente derularii contractului. Factorul de evaluare este experienta profesionala a personalului ofertantului concretizata in numarul de proiecte in care personalul a indeplinit acelasi tip activitati ca cele pe care urmeaza sa le indeplineasca in viitorul contract.

Numar maxim de puncte: 15.

Acordarea punctajului „Experiența profesionala a personalului” se va face in felul urmator:

|  |  |
| --- | --- |
| **Expert cheie** | **Numar maxim de puncte** |
| Manager de proiect | 2 |
| Arhitect solutie | 1 |
| Coordonator analiza | 2 |
| Expert integrare | 1 |
| Expert baza de date | 1 |
| Coordonator dezvoltare software | 2 |
| Coordonator testare | 2 |
| Expert infrastructura/virtualizare | 1 |
| Expert testare de securitate | 1 |
| Expert securitatea informatiei | 1 |
| Expert instruire | 1 |
| **Total** | **15** |

Punctajul aferent experienței persoanelor propuse ca experți-cheie pentru pozitiile Arhitect solutie, Coordonator analiza, Expert integrare, Expert baza de date, Coordonator dezvoltare software, Coordonator testare, Expert infrastructura/virtualizare și Expert securitatea informatiei se va acorda pentru fiecare în parte, astfel:

a) pentru experiența constând în implicarea între 2 și 4 proiecte sau contracte dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/4 din punctajul maxim alocat poziției respective în caietul de sarcini;

b) pentru experiența constând în implicarea între 5 și 7 proiecte sau contracte dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/2 din punctajul maxim alocat poziției respective în caietul de sarcini;

c) pentru experiența constând în implicarea în minim 8 proiecte sau contracte dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă punctajul maxim alocat poziției respective în caietul de sarcini;

Punctajul aferent experienţei persoanei propuse pentru pozițiile de Manager de proiect, Expert testare de securitate și Expert instruire se va acorda astfel:

1. pentru experienţa constând în implicarea între 2 şi 4 proiecte in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/4 din punctajul maxim alocat pozitiei respective în caietul de sarcini;
2. pentru experienţa constând în implicarea între 5 şi 7 proiecte in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă 1/2 din punctajul maxim alocat pozitiei respective în caietul de sarcini;
3. pentru experienţa constând în implicarea în minim 8 proiecte in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract a persoanei propuse se acordă punctajul maxim alocat pozitiei respective în caietul de sarcini;

Nu se accepta persoane propuse pe pozitii de experti fara nici un fel de experienta, respectiv fara demonstrarea implicarii in cel putin un proiect sau contract in care a indeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

Nu va fi punctata experienta profesionala a unor persoane propuse pe pozitii de experti suplimentare fata de cele mentionate in tabelul de mai sus, chiar daca acestea indeplinesc cerintele minimale si dovedesc experienta similara asa cum este descrisa in acest caiet de sarcini.

Pentru demonstrarea experientei profesionale solicitate, Ofertantii trebuie sa prezinte in cadrul ofertei tehnice documente relevante cum ar fi: recomandări emise de beneficiarul final al proiectului, semnate sau contrasemnate de către Autoritatea Contractantă/beneficiarul privat in calitate de beneficiar final al proiectului sau alte documente edificatoare semnate de acesta. Pentru fiecare document propus, se va prezenta o persoana de contact din partea beneficiarului final al proiectului (nume, pozitie, adresa de mail, numar de telefon), in masura sa confirme cele prezentate in recomandari (sau alte documente).

In urma verificarii exactitatii informațiilor și a dovezilor furnizate de catre ofertanți, Autoritatea Contractantă poate solicita și alte documente/informații care să clarifice experiența profesionala solicitata. De asemenea, Autoritatea Contractantă isi rezerva dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experienta profesionala, in vedere confirmarii celor prezentate de catre ofertanti.

Punctajul va fi acordat numai pentru proiectele sau contractele pentru care documentele prezentate dovedesc experienta solicitata pentru fiecare persoana propusa pentru o anumita pozitie de expert.

## Descrierea modalitatii de punctare a factorului de evaluare “Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului”

Prin acest criteriu se va realiza evaluarea masurii in care ofertantii inteleg specificul proiectului si a maturitatii metodologiei de implementare propuse de acestia (a proceselor si procedurilor specifice).

Numar maxim de puncte: 5 puncte.

Acordare punctajului „Demonstrarea unei metodologii adecvate de implementare a contractului” se va face in felul urmator:

|  |  |  |
| --- | --- | --- |
| **Element evaluat** | **Calificativ** | **Punctaj** |
| Abordarea propusă se bazează în mare măsură pe o serie de metodologii, metode şi/sau instrumente testate anterior de ofertant, recunoscute la nivel national / international şi care demonstrează o foarte bună înţelegere a contextului, respectiv a particularităţii sarcinilor stabilite în caietul de sarcini, în corelaţie cu aspectele-cheie, precum şi cu riscurile şi ipotezele identificate | Foarte bine | 5 |
| Abordarea propusă se bazează parţial pe metodologii,metode şi/sau instrumente testate anterior de ofertant, recunoscute la nivel national / international şi care demonstrează parţial înţelegerea contextului, respectiv a particularităţii sarcinilor stabilite în caietul de sarcini, în corelaţie cu aspectele-cheie, precum şi cu riscurile şi ipotezele identificate. | Bine | 3 |
| Abordarea propusă nu are la bază metodologii, metode şi/sau instrumente testate anterior de ofertant, recunoscute la nivel national/international şi arată o înţelegere limitată a contextului, respectiv a particularităţii sarcinilor stabilite în caietul de sarcini. | Acceptabil | 1 |

Ofertantul va prezenta organizarea și metodologia pentru realizarea sistemului informatic conform Anexa 5 – Formular propunere tehnică.

# Cerinte pentru sesiunea demonstrativa

Avand in vedere complexitatea sistemului ce trebuie implementat si importanta respectarii termenului de implementare mentionat in prezentul document, asumat si prin contractul de finantare, Autoritatea Contractanta va solicita ofertantilor prezentarea capabilitatii solutiei tehnice propuse in cadrul unei sesiuni demonstrative, demonstrand modalitatea in care produsele software incluse in solutia tehnica propusa raspund nativ, fara a fi necesare dezvoltari suplimentare, la unele cerinte minime din caietul de sarcini si la functionalitatile suplimentare ce vor fi punctate de autoritatea contractanta in cadrul factorului de evaluare „Propunere tehnica – Capabilitati solutie tehnica”.

Astfel, in timpul sesiunii demonstrative vor fi prezentate urmatoarele capabilitati ale solutiei ofertate:

1. Va fi prezentata interfata web de management pentru componenta de gestiune a documentelor, evidentiind urmatoarele functionalitati disponibile in platforma:
   1. Permite definirea securitatii (drepturilor de acces) pentru roluri, foldere si documente.
   2. Permite incarcarea de documente in depozitul de documente cel putin prin urmatoarele modalitati:
      1. drag & drop,bulk upload,copy & paste in windows explorer,
      2. monitorizare casuta de email si incarcare directa in depozitul de documente a tuturor fisierelor atasate care se trimit la acea casuta de email, fara nici o interventie umana
   3. Permite utilizatorilor adaugarea de medatate speciale in afara de cele standard ale tipului de document, metadate valabile doar pe acea instanta de document;
   4. Permite conversia automată a documentelor de tip MS Office sau OpenOffice în formate web (HTML, PDF), pentru o publicare facilă a acestora;
   5. Va permite crearea automata de structuri de foldere in functie de valori ale metadatelor documentelor;
2. Vor fi prezentate urmatoarele functionalitati cheie ale componentei de dezvoltare aplicatii mobile:
   1. Sa permita scrierea de aplicatii o data si sa poata rula pe oricare din dispozitivele mobile importante (iOS, Android, Windows).
   2. Sa foloseasca tehnologii web (HTML, CSS, Javascript) in procesul de dezvoltare aplicatii mobile
   3. Sa asigure acces la functionalitati importante din sistemul de operare in care aplicatia va rula precum: baterie, camera si localizare
3. Vor fi prezentate urmatoarele functionalitati cheie ale componentei de testare performanta:
   1. permite adaugarea/eliminarea de utilizatori virtuali in timpul executiei testelor;
   2. permite monitorizarea fara agenti;
   3. permite rularea de teste de incarcare la nivelul API (SOAP, REST), la nivelul componentelor sau la nivelul microservicilor;
   4. permite analizarea performantei sistemului dupa rularea unui test pe baza datelor colectate din straturile arhitecturale relevante;
   5. permite rularea de rapoarte de analiza a performantei pe diferite nivele de detaliu (de tip sumar sau la nivel de tranzactie) si rapoarte pentru determinarea incadrarii performantei intr-un SLA predefinit
   6. permite localizarea, extragerea si inlocuirea valorilor dinamice din cadrul paginilor web precum id-ul de sesiune, authentication token, customer id, etc asigurand astfel acceptarea cererilor de catre serverele web supuse testarii
4. Vor fi prezentate urmatoarele functionalitati cheie ale componentei de testare automata
   1. permite convertirea facila in script-uri a testelor inregistrate in interfata grafica utilizator;
   2. permite folosirea unui limbaj de programare standard (Javascript, Vbscript, Jscript, Python) pentru crearea de teste pe interfata utilizator sau imbunatatirea inregistrarilor testelor existente;
   3. permite automatizarea testarii functionale pentru multiple tehnologii desktop (de exemplu Windows / Java / .NET / Oracle Forms);
   4. permite separarea datelor de comenzile de test si modificarea datelor de intrare pentru largirea ariei de testare;
   5. permite rularea de teste de tip cross-browser;
5. Vor fi prezentate toate functionalitatile pentru care ofertantul considera ca propunerea tehnica trebuie punctata in cadrul factorului de evaluare “Propunere tehnica – Capabilitati solutie tehnica” cu exceptia functionalitatilor aferente componentelor din categoria infrastructura de securitate si anume: componenta de redistributie a accesului la servicii, componenta de protectie avansata antimalware, componenta de protectie a resurselor la nivel de post de lucru si componenta de management a datelor de audit. Functionalitatile aferente componentelor din categoria infrastructura de securitate vor fi validate in etapa de evaluare tehnica a ofertelor doar pe baza documentelor justificative prezentate ca parte a ofertei tehnice (documentatii tehnice, datasheet-uri, screenshot-uri ale interfetelor aplicatilor, etc), urmand ca Ofertantul castigator sa le prezinte practic Autoritatii Contractante in perioada de implementare a proiectului, in urma instalarii acestora pe mediile Autoritatii Contractante (test sau productiv).

Prezentarea capabilitatilor solutiei propuse in cadrul sesiunii demonstrative se va baza pe prezentarea practica a produselor software ofertate (de ex. a interfetelor expuse de acetea, a fisierelor de configurare ale acestora, etc) in cadrul unor medii demonstrative si nu doar pe descrieri ale producatorilor (de ex. datasheet-uri, manuale de administrare, alte documentatii tehnice).

In cazul in care un Ofertant nu poate demonstra in cadrul sesiunii demonstrative indeplinirea unei cerinte minimale din caietul de sarcini, va duce la respingerea ofertei acestuia ca neconforma.

In cazul in care un Ofertant nu poate demonstra in cadrul sesiunii demonstrative functionalitatile declarate ca fiind disponibile out-of-the-box in cadrul solutiei pentru a fi punctate in cadrul factorului de evaluare “Propunere tehnica – Capabilitati solutie tehnica”, functionalitati ce intra in scopul declarat al sesiunii demonstrative, Autoritatea Contractanta va acorda punctajul minim (0 puncte) pentru functionalitatile respective chiar daca in oferta tehnica au fost prezentate ca fiind incluse in solutie.

Personalul nominalizat de catre Ofertanti pentru participare la sesiunea demonstrativa va fi desemnat din echipa propusa in propunerea tehnica pentru implementarea proiectului.

Sesiunea demonstrativa va fi sustinuta de catre fiecare Ofertant la sediul Autoritatii Contractante in urma invitatiei de participare din partea acesteia.

Cu minim 2 zile lucratoare inainte de data planificata pentru sesiunea demonstrativa, Ofertantul are obligatia sa transmita Autoritatii Contractante lista participantilor la sesiunea demonstrativa in care se mentioneaza rolul in timpul sesiunii si relatia pe care acestia o au cu Ofertanul – participantii vor fi dintre cei expertii propusi in oferta tehnica. Autoritatea Contractanta nu va accepta in sesiunea demonstrativa decat persoanele nominalizate de ofertant in lista participantilor si care figureaza in lista de experti cheie mentionati in oferta depusa.

Ofertantul va pune la dispozitia expertilor sai resursele necesare (de ex. laptop-uri, modem-uri de date, servere pentru sustinerea demonstratiei, etc) pentru derularea in bune conditii a sesiunii demonstrative.

Pe durata sesiunii demonstrative, Autoritatea Contractanta va solicita realizarea de screenshot-uri cu interfetele aplicatiilor utilizate in demonstrarea fiecarei functionalitati ce intra in scopul sesiunii demonstrative. Aceste screenshot-uri vor fi incluse in anexa procesului verbal aferent sesiunii demonstrative ce va fi incheiat de catre Autoritatea Contractanta si Ofertant la finalul sesiunii demonstrative.

Refuzul de a semna procesul verbal aferent sesiunii demonstrative, consemnandu-se astfel in scris rezultatele obtinute in cadrul sesiunii demonstrative, va duce la respingerea ofertei ca neconforma.

# Drepturi de proprietate intelectuală

Orice documente sau materiale elaborate ori compilate de către executant sau de către personalul său salariat ori contractat în executarea prezentului contract, vor deveni proprietatea exclusivă a achizitorului. După încetarea prezentului contract, executantul nu va păstra copii ale documentelor şi/sau materialelor realizate şi nu le va utiliza în scopuri care nu au legătură cu prezentul contract fără acordul scris prealabil al achizitorului.

Prestatorul nu va publica articole referitoare la obiectul prezentului contract, nu va face referire la aceste lucrari în cursul executării altor lucrari pentru terţi şi nu va divulga nicio informaţie furnizată de achizitor, fără acordul scris prealabil al acestuia.

Orice rezultate ori drepturi, inclusiv drepturi de autor sau alte drepturi de proprietate intelectuală ori industrială, dobândite în executarea prezentului contract vor fi proprietatea exclusivă a achizitorului, care le va putea utiliza, publica, cesiona ori transfera aşa cum va considera de cuviinţă, fără limitare geografică ori de altă natură, cu excepţia situaţiilor în care există deja asemenea drepturi de proprietate intelectuală ori industrială.

# Modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului.

1. Prestatorul se obligă să pună la dispoziție numărul de experți necesari în realizarea contractului.

2. În cazul în care pe parcursul derulării contractului apar situații care impun înlocuirea unui membru din echipa de proiect atunci această înlocuire trebuie notificată și aprobată de achizitor, prin act adițional.

3. Prestatorul poate să propună din proprie inițiativă înlocuirea unui membru al personalului – expert cheie, numai în următoarele condiții:

a) în cazul decesului, în cazul îmbolnăvirii sau în cazul accidentării unui membru al personalului

b) dacă se impune înlocuirea unui membru al personalului pentru orice alt motiv care nu este sub controlul prestatorului ( ex. demisia, etc.)

4. Înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează numai cu acceptul autorităţii contractante, şi nu reprezintă o modificare substanţială, aşa cum este aceasta definită în art. 221 din Lege, decât în următoarele situaţii:

a) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu îndeplineşte cel puţin cerințele din cadrul documentaţiei de atribuire;

b) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu obţine cel puţin acelaşi punctaj ca personalul propus la momentul aplicării factorilor de evaluare.

5. Contractantul are obligaţia de a transmite pentru noul personal documentele solicitate prin documentaţia de atribuire fie în vederea demonstrării îndeplinirii cerințelor, fie în vederea calculării punctajului aferent factorilor de evaluare.

6. Achizitorul nu va purta nicio răspundere față de eventualele pretenții ale persoanei înlocuite, singurul responsabil de legalitatea înlocuirii fiind prestatorul. Costurile suplimentare generate de înlocuirea personalului revin în mod obligatoriu prestatorului.

# Modalitatea de plată

Plata se va efectua în 3 tranșe, după cum urmează:

- Prima tranșă reprezentând 60% din valoarea aferentă livrării, instalării și configurării infrastructurii hardware și software prevăzută la alin. (1) lit. a) se va efectua după aprobarea raportului de progres intermediar care va avea ca anexă procesele-verbale de recepție cantitativă și calitativă care atestă livrarea, instalarea și configurarea infrastructurii hardware și livrarea, instalarea și configurarea infrastructurii software de bază.

- A doua tranșă reprezentând 40% din valoarea aferentă serviciilor de analiză, proiectare, dezvoltare și testare software prevăzută la alin. (1) lit. b) se va efectua după aprobarea raportului de progres intermediar care va avea ca anexă procesele-verbale de recepție cantitativă și calitativă a serviciilor de analiză, proiectare dezvoltare, testare software

- A treia tranșă însumând 40 % din valoarea aferentă livrării, instalării și configurării infrastructurii hardware și software prevăzută la alin. (1) lit. a) și 60 % din valoarea aferentă serviciilor de analiză, proiectare, dezvoltare și testare software prevăzută la alin. (1) lit. b) se va efectua după aprobarea raportului final care va avea ca anexă procesul-verbal de acceptanță finală a tuturor activităților proiectului și punerea în funcțiune a întregului sistem informatic, inclusiv plata în procent de 100% pentru serviciile de instruire/cursare utilizatorilor/administratorilor.

Plățile se vor face numai după aprobarea rapoartelor/semnarea proceselor-verbale de livrare și punere în funcțiune a produselor/serviciilor, însoțite de rapoartele financiare aferente/livrabile/fișe tehnice/licențe/certificate de garanție, etc..

Facturile vor fi emise numai după aprobarea rapoartelor/semnarea proceselor verbale de livrare și punere în funcțiune a produselor/serviciilor.

Plata facturilor emise de prestator se efectuează în termen de 30 de zile de la înregistrarea acestora la beneficiar, însoțite de documentele justificative aprobate de beneficiar.

Documentele care necesită a fi aprobate de beneficiar, în vederea efectuării plăților în funcție de etapele de implementare, sunt:

1. **Raport de progres intermediar nr. 1** care va va cuprinde descrierea etapelor de recepție cantitativă și calitativă a a produselor livrate, instalare și configurare infrastructură harware și livrare, instalare și configurare infrastructură software de bază, care include și raport financiar. Acesta va fi transmis oficial în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maxim 8 luni de la data semnării contractului.
2. **Raport de progres intermediar nr. 2** care va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de analiză, proiectare, dezvoltare și testare software aplicativ, care include și raport financiar. Acesta va fi transmis oficial în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de 15 luni de la data semnării contractului.
3. **Raport final -** document elaborat de prestator la finalul contractului care va descrie modul în care s-a desfășurat implementarea contractului din punct de vedere tehnic/financiar, inclusiv acceptanța finală prin care se vor recepționa toate activitățile proiectului și punerea în funcțiune a întregului sistem informatic, inclusiv instruirea utilizatorilor/administratorilor.

Aprobarea documentelor sau notificarea cu privire la neconformitățile identificate de beneficiar se va efectua în maxim 10 zile lucratoare de la primirea acestora. Prestatorul va revizui și retransmite documentele în maxim 5 zile lucratoare de la notificare.

Plățile pentru serviciile efectuate/bunurile livrate se vor efectua cu încadrarea în creditele bugetare aprobate.

Executarea contractului nu trebuie să genereze alte servicii/produse decât cele cuprinse în contract și/sau cheltuieli comerciale neuzuale în afara celor înscrise în bugetul contractului și menționate în caietul de sarcini. Dacă totuși apar astfel de cheltuieli, achizitorul nu va fi răspunzător și nu va suporta cheltuielile comerciale în afara celor înscrise în bugetul contractului.

# Informatii finale

În situaţia în care comisia de evaluare constată că elemente de preţ ale unei oferte sunt aparent neobişnuit de scăzute, prin raportare la preţurile pieţei, comisia de evaluare va solicita ofertantului care a depus oferta în cauză explicaţii cu privire la posibilitate îndeplinirii contractului în condiţiile de calitate impuse prin documentaţia de atribuire. Explicaţiile aduse de ofertant vor fi însoţite de dovezi concludente privind elementele prevăzute la art. 210 alin. (2) din Legea 98/ 2016, precum şi, după caz, documente privind preţurile ce pot fi obţinute de la furnizori, modul de organizare şi metodele utilizate în cadrul procesului de lucru, nivelul de salarizare al personalului ofertantului, performanţele şi costurile implicate de anumite utilaje sau echipamente de lucru.

În cazul în care ofertantul nu prezintă comisiei de evaluare informaţiile şi/sau documentele solicitate sau acestea nu justifică în mod corespunzător nivelul scăzut al preţului sau al costurilor propuse, oferta va fi considerată inacceptabilă.

Ofertanții trebuie sa întocmeasca propunerea tehnică și financiară cu respectarea prevederilor stabilite în cadrul prezentului caiet de sarcini.

Ofertantul trebuie să răspundă punctual la toate cerințele cuprinse în prezentul caiet de sarcini și să detalieze în cadrul propunerii tehnice metodologia de lucru și mijloacele concrete prin care sistemul informatic ofertat îndeplineste aceste cerințe, planul de lucru, personalul utilizat si organizarea acestuia, astfel încât comisia de evaluare să aibă posibilitatea evaluării acesteia în mod obiectiv.

***Simpla copiere a conţinutului caietului de sarcini în Propunerea Tehnica nu reprezintă îndeplinirea cerinţelor de conformitate anterior enunţate.***

Propunerea tehnică se va întocmi într-o manieră organizată, astfel încât procesul de evaluare a ofertelor să permită identificarea facilă a corespondenței informațiilor cuprinse în ofertă cu specificațiile tehnice din prezentul caiet de sarcini. Oferta tehnica trebuie sa fie prezentata si intr-un format editabil care sa permita selectarea textului, copierea acestuia, precum si cu toate referintele (link-urile) către site-uri in format hyperlink, „gata de click” (in acest sens solicitam prezentarea ofertei tehnice si in format Microsoft Word sau intr-un format care sa permita copierea textului catre Microsoft Word cu pastrarea formatarii acestuia).

Ofertantii au obligativitatea prezentarii pentru fiecare dintre membrii personalului care va face parte din echipa de proiect, conform pozitiei de expert pe care este alocat, toate documentele necesare evaluarii, in mod ordonat, pentru a facilita procesul de evaluare.

Omisiunea sau neîndeplinirea corespunzătoare a oricărei dintre cerințele prezentului caiet de sarcini va duce la respingerea ofertei ca neconformă. De asemenea, un simplu răspuns (afirmație) de confirmare din partea operatorului economic cu privire la respectarea cerințelor din caietul de sarcini, fără precizarea exactă a modalității de îndeplinire, va conduce la respingerea ofertei. În acest sens se solicită din partea ofertantilor și intră în răspunderea acestora prezentarea dovezilor concrete în sprijinul oricăror afirmații care se pot încadra în categoria exemplului anterior menționat.

Toate livrabilele furnizate in cadrul proiectului de catre Prestator vor fi in limba romana.

Specificatiile tehnice definite in cadrul prezentului caiet de sarcini corespund necesitatilor si exigentelor autoritatii contractante. Avand in vedere specificitatea acestui proiect, Autoritatea Contractanta a descris sistemul informatic ce va fi achizitionat la nivelul de detaliu necesar operatorilor economici interesati, permitand identificarea obiectului acestui contract de achizitie publica.

Orice referire la producători / mărci comerciale / denumiri de produse sau parti componente / tipuri / standarde / procedee / tehnologii / proceduri / producţii si elemente specifice / origini / certificări prezentate în caietul de sarcini sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si vor fi considerate ca purtând menţiunea “**sau echivalent**", chiar daca nu este efectiv precizata in cadrul respectivei cerinte.

**AUTORITATEA CONTRACTANTĂ**

# Anexa 1 - Lista locaţiilor semnificative la nivelul proiectului – ONRC, ORCT București şi ale ORCT Brașov

**Lista locaţiilor – ONRC şi ale ORCT semnificative la nivelul proiectului, reprezentanţi autorizaţi din partea ONRC**

| **Nr. crt.** | **Locaţie** | **Adresă** | **Telefon fix, mobil** | **Fax** | **E-mail** | **Persoane de contact personal tehnic** |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | Oficiul Naţional al Registrului Comerţului (ONRC) | Bucureşti, Bd. Unirii nr. 74, sector 3 | 021-316.08.04 | 021-316.08.03 | [onrc@onrc.ro](mailto:onrc@onrc.ro) | Stefan CRETIOIU  021-316.08.17/123  E-mail: [stefan.cretioiu@onrc.ro](mailto:stefan.cretioiu@onrc.ro)  Dan TĂNASE  021-316.08.17/123  Mobil: 0752 011 492  E-mail: [dan.tanase@onrc.ro](mailto:dan.tanase@onrc.ro) |
| 2. | Oficiul Registrului Comerţului de pe lângă Tribunalul (ORCT) BUCUREŞTI | Bucureşti, Intrarea Sectorului nr. 1, sector 3 | 021-316.08.28 | 021-316.08.23  021-316.08.25 | [orcb@b.onrc.ro](mailto:orcb@b.onrc.ro) | Maria Tănase  [maria.tanase@b.onrc.ro](mailto:maria.tanase@b.onrc.ro)  0752-011469  Adrian Cărăşel  [adrian.carasel@b.onrc.ro](mailto:adrian.carasel@b.onrc.ro)  0756-067 145 |
| 3. | ORC de pe lângă Tribunalul BRAŞOV | Braşov,  str. Zizinului, nr. 106A | 0268-311.992, 0268-319.027 | 0268-318.616 | [orcbv@bv.onrc.ro](mailto:orcbv@bv.onrc.ro) | Rodica Tatiana TOMA – Director  orcbv@bv.onrc.ro,  0752-011 328  Florin Razvan Lupsa Tataru  florin.lupsa@bv.onrc.ro,  0752-011 330 |

# Anexa 2 – Indicatori de performanta pentru realizarea activitatilor din contract

| **Indicator de performanță** | **Referința în Contract / Caiet de Sarcini -** | **Nivelul de performanță așteptat (conform Contract / Caiet de Sarcini)** | **Ce se măsoară** | **Modalitate de evaluare** | **Scop** |
| --- | --- | --- | --- | --- | --- |
| Documentie de analiza adecvata pentru scopul utilizării | Analiza – Document analiza de business | Documentația de analiza este livrată conform cerințelor stabilite în Caietul de Sarcini | Nivelul de acuratețe al documentației livrate după “peer review” (pondere informații inexacte / sub nivelul de calitate agreat în informațiile furnizate) | **Foarte satisfăcător (5 puncte)** – Documentația livrată include îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini în special prin luarea în considerare a noilor tendințe din industrie și respectarea aspectelor de mediu și sociale. Documentația a fost folosită pentru realizarea achiziției și pentru construcțieașa cum a fost prezentată.  **Satisfăcător (4 puncte)** – Documentația livrată include unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreat. Documentația a fost folosită pentru realizarea achiziției și pentru construcțieașa cum a fost prezentată. Au fost necesare doar ajustări nemateriale.  **Acceptabil (3 puncte)** - Documentația livrată nu include neconformități/inexactități față de nivelul agreat însă nu include nici elemente suplimentare care **să** aducă o valoare adăugată semnificativă proiectului sau nu a fost acordată o atenție specială aspectelor de mediu sau sociale.  Documentația a putut fi folosită pentru realizarea achiziției și/sau construcției după ce a fost corectată de câteva ori de Consultant.  Nu au existat întârzieri semnificative ca urmare a corecturilor.  **Nesatisfăcător (2 puncte)** - Documentația transmisă a inclus neconformități / inexactități față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate de către Consultant, fără costuri suplimentare pentru Autoritatea Contractantă.  **Foarte nesatisfăcător (1 punct)** – Documentația livrată a inclus neconformități / inexactități majore față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau, în principal, abandonate de industrie, iar aceste aspecte nu au putut fi corectate de către Consultant. Autoritatea Contractantă a trebuit **să** mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului. | Evaluarea aplicabilității și relevantei documentației de analiza |
| Documentie de proiectare adecvata pentru scopul utilizării | Proiectare si dezvoltare software – Document proiectare detaliata | Documentația de proeictare este livrată conform cerințelor stabilite în Caietul de Sarcini | Nivelul de acuratețe al documentației livrate după “peer review” (pondere informații inexacte / sub nivelul de calitate agreat în informațiile furnizate) | **Foarte satisfăcător (5 puncte)** – Documentația livrată include îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini în special prin luarea în considerare a noilor tendințe din industrie și respectarea aspectelor de mediu și sociale. Documentația a fost folosită pentru realizarea achiziției și pentru construcțieașa cum a fost prezentată.  **Satisfăcător (4 puncte)** – Documentația livrată include unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreat. Documentația a fost folosită pentru realizarea achiziției și pentru construcțieașa cum a fost prezentată. Au fost necesare doar ajustări nemateriale.  **Acceptabil (3 puncte)** - Documentația livrată nu include neconformități/inexactități față de nivelul agreat însă nu include nici elemente suplimentare care **să** aducă o valoare adăugată semnificativă proiectului sau nu a fost acordată o atenție specială aspectelor de mediu sau sociale.  Documentația a putut fi folosită pentru realizarea achiziției și/sau construcției după ce a fost corectată de câteva ori de Consultant.  Nu au existat întârzieri semnificative ca urmare a corecturilor.  **Nesatisfăcător (2 puncte)** - Documentația transmisă a inclus neconformități / inexactități față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate de către Consultant, fără costuri suplimentare pentru Autoritatea Contractantă.  **Foarte nesatisfăcător (1 punct)** – Documentația livrată a inclus neconformități / inexactități majore față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau, în principal, abandonate de industrie, iar aceste aspecte nu au putut fi corectate de către Consultant. Autoritatea Contractantă a trebuit **să** mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului. | Evaluarea aplicabilității și relevantei documentației de proiectare |
| Livrabil final predat în termenul agreat | Servicii de management de proiect | Sistemul infornatic a fost pus in functiune conform termenului agreat în contract | Livrarea la timp a rezultatelor | **Foarte satisfăcător (5 puncte)** – livrate în termenele convenite în contract,  **Satisfăcător (4 puncte)** – livrate imediat după încheierea termenelor convenite în Contract însăfărăîntârzierea activităților din calendarul general al proiectului  **Acceptabil (3 puncte)** – livrate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate.  **Nesatisfăcător (2 puncte)** – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului, ex. mai mult de 60 de zile.  **Foarte nesatisfăcător (1 puncte)** – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului, ex. mai mult de 120 de zile | Evaluarea finalizării la timp punerii in functiune a sistemului informatic |

**AUTORITATEA CONTRACTANTĂ**