

3.5.4 Cerințe tehnice

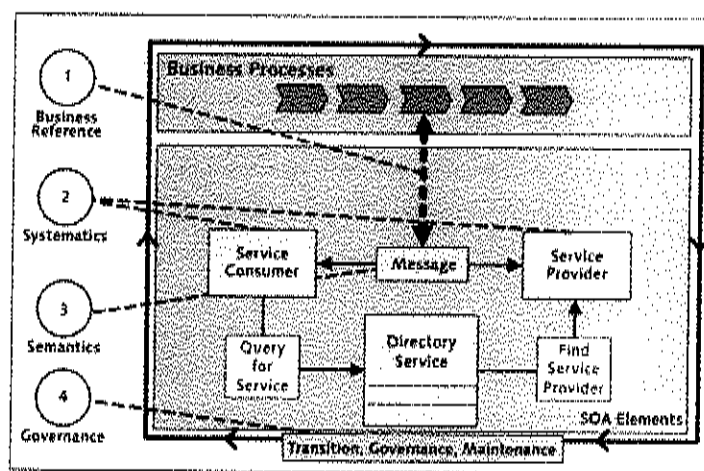
3.5.4.1 Arhitectura funcțională a noului sistem

Noul sistem informatic integrat va fi implementat conform bunelor practici din domeniul IT și va utiliza standarde deschise pentru eficientizarea schimbului de informații între componentele funcționale, asigurând totodată:

- O abordare unitară, etapizată, folosind metodologii și tehnologii adecvate;
- Componente pre-integrate - pe cât posibil de la același producător;
- O arhitectură modulară și deschisă, bazată pe standarde larg răspândite;
- Un sistem centralizat cu punct de administrare și monitorizare unic;

Arhitectura orientată pe microservicii (SOA) oferă o flexibilitate mai bună în construirea aplicațiilor și a proceselor de business, asigurând o manieră de management agilă și se poate folosi de infrastructura aplicațiilor existente pentru a compune noi servicii. Dezvoltarea, asumarea costurilor și riscurile de implementare sunt scăzute. SOA este și o arhitectură și un model de programare, o nouă modalitate de a construi un software de bună calitate.

SOA asigură crearea unor componente reutilizabile, o încapsulare totală a serviciilor, o cuplare mică a acestora (serviciile nu depind unele de altele), se pot atinge diverse niveluri de granularitate a serviciilor și datorită independenței platformei folosite se pot integra numeroase servicii folosind limbaje de programare diferite.



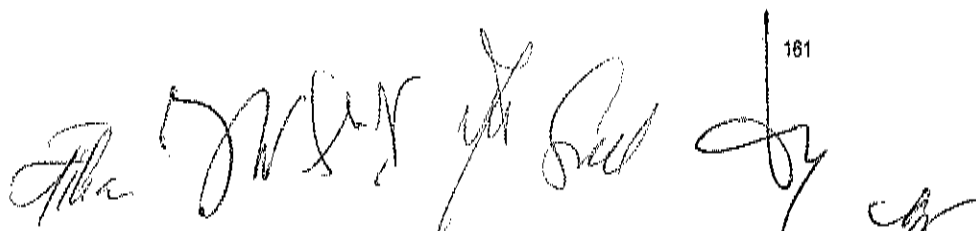
Figură – Principiile SOA

În cazul de față, luând în considerare faptul că actualul SII este implementat în tehnologia Java, pentru extinderea acestuia se va avea în vedere faptul că implementarea viitorului sistem va trebui la rândul ei să utilizeze tehnologia Java pentru a avea un cadru uniformizat la nivelul limbajului de programare de bază și totodată pentru a putea îmbunătăți serviciile deja implementate.

[Handwritten signature]

În consecință, noul sistem informatic trebuie să aibă la bază o arhitectură orientată pe servicii, urmând principiile SOA pentru design-ul soluției dorite:

- **interoperabilitate** - capacitatea aplicațiilor de a interacționa într-un mod standardizat în vederea realizării unui serviciu IT. Interoperabilitatea, promovată în mod special prin aplicarea consecventă asupra proiectelor diferite, ce pot fi în mod repetat asamblate împreună într-o varietate de configurații pentru a ajuta la automatizarea proceselor;
- **abstractizarea serviciilor** - presupune că informațiile publicate într-un serviciu să fie limitate la ceea ce este necesar pentru a utiliza în mod eficient serviciile. La nivel fundamental, acest principiu subliniază necesitatea de a ascunde cât mai mult detaliile care stau la baza unui serviciu precum detaliile tehnice ale platformei sau detalii neesențiale despre serviciul în sine;
- **autonomia serviciilor** - este un principiu de design care presupune furnizarea de servicii independente față de mediile lor de execuție. Aplicând autonomia la nivel de serviciu, limitele serviciilor pot fi deosebite, chiar dacă acestea partajează unele resurse. Compunerea Serviciilor - încurajează proiectarea de servicii care pot fi refolosite în soluții multiple care la rândul lor sunt alcătuite din servicii compuse. Acest principiu este direct responsabil pentru agilitatea promisă de SOA, deoarece promovează compunerea de noi soluții prin reutilizarea serviciilor existente;
- **detectarea serviciilor** - completarea serviciilor cu metadate, prin care ele pot fi descoperite și interpretate în mod eficient. Pentru a face un serviciu detectabil este necesar ca informațiile despre serviciu să fie documentate în mod consecvent și totodată să fie stocate într-un registru pentru a se permite căutarea informațiilor într-un mod eficient;
- **servicii cuplate independent** - promovează designul independent și evoluția implementării unui serviciu, în același timp garantând interoperabilitatea;
- **reutilizarea serviciilor** - crearea de servicii, care au potențialul de a fi reutilizate la nivel Enterprise. Aceste servicii reutilizabile sunt concepute într-un mod, astfel încât soluția lor logică este independentă de orice proces particular sau tehnologie;
- **servicii statelessness** - minimizarea consumului de resurse prin amânarea gestionării informațiilor de stare atunci când este necesar. Managementul excesiv al informațiilor de stare poate compromite disponibilitatea unui serviciu și submina potențialul său de scalabilitate;
- **orientarea pe servicii și Interoperabilitatea** - într-o arhitectură orientată spre servicii, "Interoperabilitatea" se referă la capacitatea serviciului de a fi invocat de către orice client potențial al serviciului respectiv. Interoperabilitatea semantică depinde de modul în care interfețele unui serviciu sunt descrise și de modul în care informațiile sunt împărtășite cu potențialii clienți ai serviciului. Din punct de vedere sintactic, o arhitectură orientată pe servicii este opțiunea de viitor, iar provocarea constă în determinarea numărului de adaptoare de implementare și determinarea granularității interfețelor de servicii, deoarece nu este întotdeauna cunoscut modul în care sistemele vor utiliza serviciile;
- **servicii standardizate** - asigură faptul că serviciile care sunt în același inventar de servicii sunt păstrate în conformitate cu standardele de proiectare. Serviciul standardizat impune practic considerente specifice ce trebuie luate în calcul atunci când interfața tehnică publică a unui serviciu este în curs de

 181

proiectare. Acesta evaluează simultan natura și cantitatea de conținut care va fi publicat ca parte oficială a serviciului.

Arhitectura noului sistem va respecta principiul esențial de separare în straturi:

1. Nivelul aplicațiilor principale de back-office;
2. Nivelul intermediar de integrare (middleware - business logic) care să asigure comutarea mesajelor și gestiunea canalelor de distribuție a acestora;
3. Nivelul de prezentare al canalelor de distribuție, de front-office către client, prin intermediul canalelor de distribuție. Clienții pot fi atât externi (persoane fizice sau juridice, instituții), cât și interni, lucrătorii ONRC/ORCT.

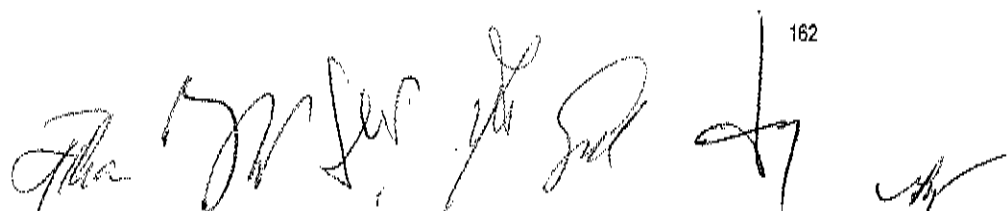
Această arhitectură ar permite o segregare, un nivel de abstractizare practică cu trei componente:

1. Operațiuni - tranzacții care determină una sau mai multe înregistrări de date, de citire sau de actualizare;
2. Servicii - o grupare logică de operațiuni (de exemplu, "înființarea unei afaceri", "desființarea unei afaceri", "obținere informații de la Registrul Comerțului", "obținere informații din Buletinul Procedurilor de Insolvență" etc.);
3. Procese de business - o serie de operațiuni sunt executate într-o ordine secvențială în conformitate cu un set de reguli de business. Selecția, secvențierea și execuția operațiunilor, inclusiv rutarea acestora prin nivelul middleware, sunt orchestrate omogen și unitar.

Din punct de vedere al modelului de date, descrierea acestuia se va face utilizând standardul de modelare UML 2.0. Din punct de vedere tehnologic, pentru implementarea cu succes a arhitecturii de tip SOA dorite, sunt necesare următoarele componente de bază:

- Componentă de integrare:
 - o Suport pentru integrare cu alte sisteme utilizând conectori existenți sau oferind suport pentru dezvoltarea de noi conectori;
 - o Suport pentru dezvoltare, publicare și expunere de servicii în vederea consumării de către clienți;
 - o Suport pentru rutare, mediere și transformări de date;
 - o Suport pentru transmiterea consistentă de informații între aplicații sub formă de mesaje.
- Componentă de proces:
 - o Suport pentru definirea și execuția de procese de business;
 - o Suport pentru modelarea grafică de procese prin intermediul unor instrumente;
 - o Suport pentru interacțiunea cu procesele utilizând REST API;
 - o Suport pentru definirea de indicatori de performanță (KPI) și monitorizarea lor la nivelul de execuție procese;
 - o Suport pentru raportarea la nivel de proces și publicarea de informații în mod grafic (dashboards-uri).

Acestea vor fi descrise în secțiunea următoare, alături de celelalte componente ale sistemului.

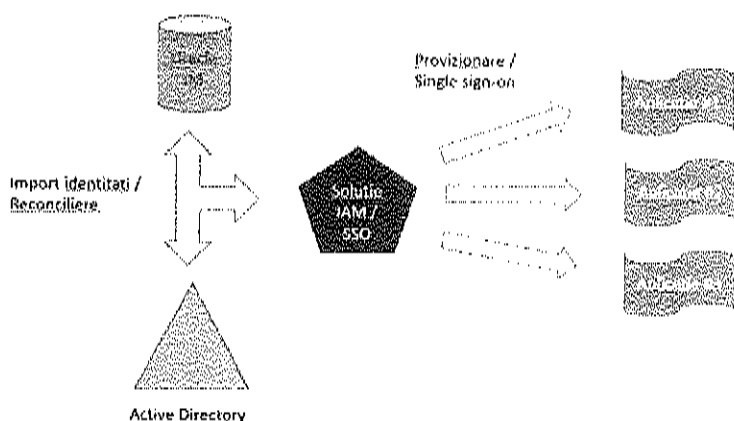
A series of handwritten signatures and initials in black ink, located at the bottom of the page. The signatures are stylized and appear to be of various individuals.

3.5.4.2 Management identități

Importul inițial al identităților se va efectua din depozitul existent la nivelul sursei Oracle. Vor fi implementate mecanisme minimale de validare și uniformizare a atributelor pentru aceste identități, folosind un set de reguli de bază definite în soluția de administrare a identităților. În momentul importului inițial, identitățile existente vor fi asociate unui set de roluri ce va trebui definit în repository-ul acestei soluții.

Odată importate, conturile utilizator vor trebui sincronizate cu serviciul director parte a platformei.

Provizionarea ulterioară a identităților se va putea realiza fie manual, direct în soluția de administrare a identităților, fie vor fi create / modificate / șterse în serviciul director sau platforma Oracle, iar modificările preluate pe bază de flux din aceste surse.



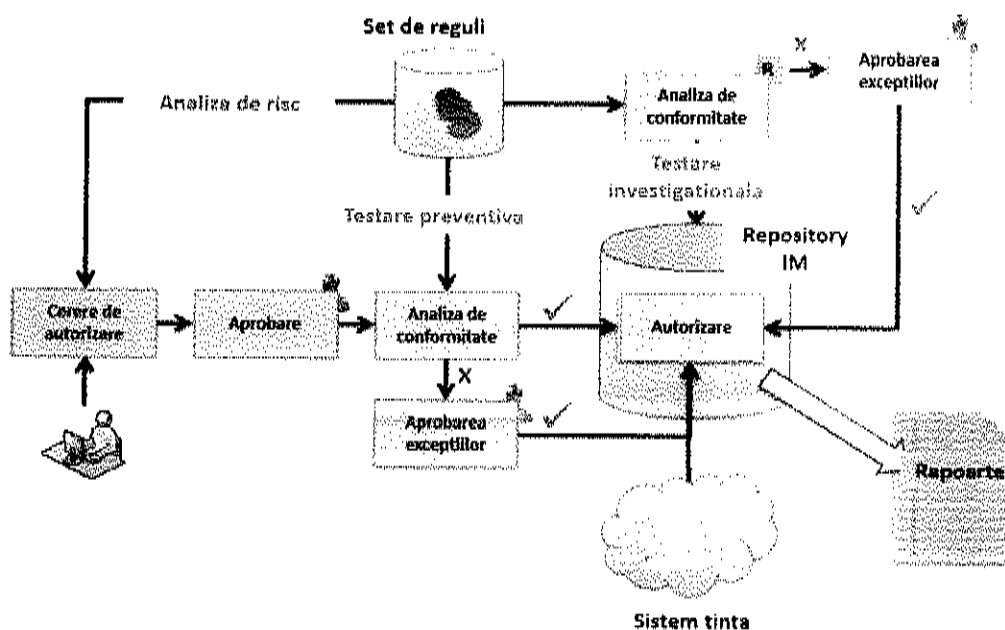
Implementarea va include mecanisme de control și reconciliere a sincronizărilor, folosind ca sursă primară serviciul director sau sistemul Oracle, iar ca sursă de reconciliere sistemul secundar. Soluția va trebui să poată preveni automat duplicarea conturilor existente în oricare dintre cele două surse, și va trata conturile duplicate nou create ca modificări a celor existente – operând corecțiile necesare în sistemul sursă Microsoft existent.

În continuare, modificările vor fi sincronizate în sistemele țintă (aplicațiile suportate).

În scopul implementării este inclusă conectarea a până la cinci aplicații Enterprise pentru necesitățile de sincronizare a identităților și single sign-on.

Scopul implementării va fi dimensionat pentru crearea unui număr estimat de două până la 10 fluxuri de provizionare și sincronizare bidirecțională de identități, în funcție de modul în care soluția oferită poate gestiona cerințele de reconciliere și atestare (recertificare), conform modelului de mai jos:

163



3.5.4.3 Cerințele componentelor sistemului informatic

3.5.4.3.1 Componenta virtualizare servere

Cerinte:

Componenta de virtualizare a serverelor oferă toate pârghiile necesare implementării unei arhitecturi scalabile în care se pot gestiona eficient resursele existente, atât alocate la nivelul mașinilor virtuale definite cât și prin provizionare de noi resurse de procesare, stocare și comunicație prin scalare orizontala sau verticala. Aceasta soluție va fi instalata direct pe toate serverele furnizate în proiect și va beneficia de suportul acestora atât la nivelul capacității de procesare cât și la nivelul opțiunilor de conectica și integrare cu restul elementelor fizice de infrastructură (integrare nativa cu platformele de comunicație și platformele de stocare).

Componenta de virtualizare are rol primar în asigurarea mediului de operare pentru nodurile de procesare, respectiv asigurarea mediului de rulare pentru aplicațiile și serviciile oferite de sistem. Aceasta funcționalitate va fi oferita prin mecanisme proprii de abstractizare a componentelor fizice din nodurile de procesare, stocare și comunicație și nu vor adăuga complexitate și/sau penalizări de performanță sesizabile în funcționarea aplicațiilor și serviciilor deservite.

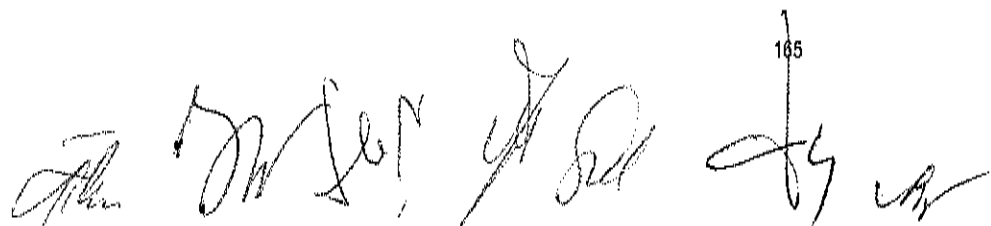
Componenta de virtualizare trebuie să ofere următoarele funcționalități principale:

- Să nu depindă de un sistem de operare gazda a cărui actualizare să afecteze disponibilitatea și funcționalitatea mașinilor virtuale;
- Capacitati de fail-over astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie repornite automat pe alte host-uri;

164

- Posibilitatea mutării simultane a mașinilor virtuale în funcționare, de pe un host pe altul/altele fără afectarea funcționării acestora, pentru a se putea executa activități de mentenanță pe host-ul respectiv;
- Balansarea automată a încărcării pe host-urile din cluster-ul de virtualizare prin mutarea mașinilor virtuale aflate în funcționare în vederea asigurării resurselor optime pentru funcționare;
- Funcționarea fără întrerupere a mașinilor virtuale critice chiar și în cazul defectării serverului fizic pe care acestea rulează, prin rularea în paralel a acestor mașini virtuale pe două servere fizice diferite și comutarea instantanee pe celălalt server fizic în cazul defectării unuia dintre ele;
- Mecanisme automate de economisire a energiei electrice prin concentrarea masivă a mașinilor virtuale pe câteva host-uri și oprirea host-urilor nefolosite în momentul în care încărcarea mașinilor virtuale scade. În mod similar, atunci când încărcarea mașinilor virtuale crește, host-urile nefuncționale vor fi pornite în vederea asigurării resurselor de procesare corespunzătoare prin balansarea automată a încărcării pe fiecare host din cluster;
- Să suporte diverse tipuri de storage de tip SAN și NAS prin protocoale de acces de tip FC, FCOE, iSCSI și NFS;
- Accesul către sistemul de stocare extern să poată fi făcut pe mai multe căi (multi-pathing), asigurându-se suport pentru fail-over și load balancing și având posibilitatea de alegere a politicii de stabilire a căii;
- Va permite accesul concurent al mai multor servere fizice (gazde) și al mai multor mașini virtuale la aceeași resursă de stocare;
- Posibilitatea de a crea echipamente de rețea virtuale (switch-uri) la care să se conecteze mașinile virtuale și interfețele de rețea fizice de pe sistemul host. Să ofere switch virtual integrat în serverele host, distribuit pe mai multe hosturi pentru configurarea centralizată a setărilor de rețea. De asemenea să ofere mecanisme automate de evaluare și prioritizare continuă a accesului mașinilor virtuale și aplicațiilor rezidente la resursele de comunicație disponibile, permițând alocarea și realocarea dinamică a acestor resurse în funcție de cerințele de moment;
- Trebuie să poată permite adăugarea de procesoare, memorie RAM, interfețe de rețea și HDD la mașinile virtuale fără oprirea acestora;
- Trebuie să permită crearea de grupuri de mașini virtuale care să împartă aceleași resurse puse la dispoziție în comun (memorie și timp de procesor);
- Balansarea dinamică a mașinilor virtuale între mai multe host-uri configurate în cluster de înaltă disponibilitate;
- Managementul salvărilor contextuale (snap-shot) ale mașinilor virtuale; o mașină virtuală se va putea restaura din orice salvare anterioară;
- Modul de management a serverelor gazda și a mașinilor virtuale create pe acestea, oferind următoarele facilități:
 - În vederea accesului facil la funcțiile de administrare și monitorizare oferite, platforma va permite acces prin browser web securizat SSL;

165



- Va permite autentificarea utilizatorilor bazata pe roluri și privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director LDAP;
- Va asigura și mecanisme de definire și aplicare a profilelor standard de configurație pentru serverele ce fac parte din infrastructura virtuala;
- Crearea, modificarea, pornirea și oprirea mașinilor virtuale pe serverele gazda controlate;
- Gruparea și organizarea logica a resurselor de procesare în funcție de necesități, precum și izolarea acestor grupări de resurse, respectiv va asigura flexibilitatea necesara mării cantității de resurse disponibile într-o grupare prin extragerea de resurse din alte grupări;
- Monitorizarea activității serverelor și mașinilor virtuale (memorie alocata, încărcarea procesoarelor, traficul de rețea);
- Consola web către sistemele de operare ce rulează în mașinile virtuale;
- Configurarea host-urilor în cluster de înaltă disponibilitate;
- Să ofere o vizualizare holistica, multi-nivel a mediului virtual;
- Să furnizeze o interfața de gestionare a întregului mediu virtual, cu vizualizări rapide ale marilor consumatori pentru fiecare resursa;
- Sa asigure managementul utilizarii resurselor virtuale;
- Să ofere implementarea centralizata a update-urilor pentru hypervisor și pentru modulul de management.

3.5.4.3.2 Componenta portal

Cerinte:

Componenta portal reprezintă principala interfața de acces către sistemului informatic deoarece are expunere către exterior - utilizatori persoane fizice și juridice. Interfața portalului va fi bazata pe o îmbunătățire a celei existente acum, ținând cont de noile reperi tehnologie precum și noile standarde privitoare la modul în care conținutul este generat și livrat către consumatori (WCAG - Web Content Accessibility Guidelines - Ghid de accesibilitate pentru conținut web). Totodată, portalul va gestiona în mod eficient partea de preluare date prin implementarea unui mecanism de gestiune a formularelor electronice web-based.

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

- Utilizatorii, indiferent de profil, să beneficieze de o interfața unitară cu acces la un meniu centralizat - interfața client trebuie să respecte standardul UTF-8 și să fie localizată în limba română și în limba engleză;
- Utilizatorii, în limitele drepturilor asociate de administrator, să poată personaliza secțiuni din paginile personale;
- Interfața cu utilizatorii să ofere un nivel ridicat de accesibilitate, conform cu cerințele nivelului I (A) de accesibilitate WCAG;

Handwritten signatures and initials at the bottom of the page, including a signature with the number 166 above it.

- Sistemul va permite ca administratorul să poată configura cine poate publica conținut, cine poate încărca fișiere până la nivel de utilizator/grupuri. Sistemul va răspunde solicitărilor utilizatorilor în funcție de drepturile acestora de acces;
- Suport cel puțin pentru protocoale de integrare standard SOAP, REST, RSS;
- Să îmbunătățească experiența utilizatorilor prin utilizarea unor tehnologii bazate pe Web 2.0 sau AJAX;
- Suport pentru drag & drop în cadrul paginii cel puțin la nivel de fragmente de interfață pe care le agregă (de exemplu portlets, web parts) și elementele sistemului de navigare;
- Posibilitatea de definire de câmpuri suplimentare cel puțin la nivel de pagini, foldere, documente, imagini, mesaje din forum, blog, calendar și wiki. Astfel, administratorii vor putea adăuga, edita sau șterge câmpuri suplimentare direct din cadrul sistemului, fără a fi nevoie să acceseze baza de date;
- Suport pentru personalizare folosind un sistem de reguli care să susțină cel puțin afișarea de conținut relevant utilizatorilor pe baza informațiilor demografice ale utilizatorului, precum și activități și proprietăți asociate profilului acestuia;
- Organizarea utilizatorilor în ierarhii precum și gruparea lor pe interese în comunități. Aceste moduri de organizare trebuie să poată fi folosite pentru a defini restricții de utilizare, pagini particulare și calendar comun unei comunități/organizații;
- Definirea de etichete de către orice utilizator cel puțin la nivel de conținut web, documente, forumuri și să permită căutarea după astfel de etichete în întregul portal. Sistemul trebuie de asemenea să ofere suport pentru căutare atât pe baza de meta-informații cât și pe baza de conținut, inclusiv în cadrul documentelor;
- Trebuie să permită crearea, modificarea și ștergerea de conținut web precum și posibilitatea de a publica materialele în cadrul paginilor definite de utilizatori sau administratori în sistem;
- Acces centralizat la o ierarhie de directoare și imagini cu posibilitatea restricționării accesului la nivel de comunitate, grup de utilizatori, utilizatori;
- Definirea de template-uri de pagini care să poată fi utilizate de utilizatori care publica conținut;
- Administratorii trebuie să poată crea șabloane de conținut web folosind unul sau mai multe fragmente în scopul standardizării conținutului. Autorii de conținut vor completa fragmentele respective iar sistemul va crea conținutul final prin agregarea fragmentelor conform șablonului;
- Suport pentru actualizarea automată a hărții de site la momentul adăugării de noi pagini;
- Funcționalități de editare instant a paginilor cu publicarea modificărilor într-un singur pas, fie la final fie programatic, specificând ce trebuie publicat, la ce ora și în ce locație;
- Funcționalități de rearanjare a hărții site-ului din interfață, prin drag & drop;
- Acces centralizat la o ierarhie de directoare și documente cu posibilitatea restricționării accesului la nivel de comunitate, grup de utilizatori, utilizatori. Librăria de documente trebuie să respecte standardul de stocare și accesare documente JSR-170 (Java Content Repository) și să ofere următoarele funcționalități:
 - Check în/check out;

167

- Integrare cu suita Office;
- Versionare;
- Sistem de permisiuni granularizat fin;
- Upload Multi-fișier
- Conversia formatelor de fișiere între formate comune (PDF, HTML);
- Sistemul trebuie să permită definirea de formulare electronice web care să ofere următoarele capacități:
 - Posibilitate de marcare câmpuri obligatorii cu elemente grafice distincte;
 - Accesarea formularelor de pe dispozitive multiple (laptop, mobil);
 - Calculare formule, precompletare câmpuri automat;
 - Posibilitate de a seta câmpuri vizibile sau ascunse - câmpuri completabile sau doar read-only;
 - Secțiuni repetitive de tip tabel;
 - Generare automata de PDF-uri plecând de la formularul web completat cu date;
 - Formulare cu pagini multiple, cu posibilitate de navigare între pagini;
 - Posibilitate de a utiliza servicii web sau REST (Representational State Transfer) pentru schimb de date cu alte aplicații;
- Sistemul trebuie să permită definirea de formulare de tip offline (se preconizează un număr maxim de 20 formulare ce conțin informații statice) care să ofere capacități de tipul:
 - Instrumente de design necesare pentru proiectarea și realizarea de formulare, de tip „pixel perfect”, cu posibilitate de export în PDF sau HTML5;
 - Asigurarea autenticității și integrității prin posibilitatea de aplicare de semnătură utilizând un certificat digital;
 - Descărcarea formularelor pe stația de lucru a solicitantului, completarea de informații și posibilitatea de a salva formularul cu datele completate, pentru o utilizare ulterioară;
 - Posibilitatea de a genera coduri de bare de tip 1D sau 2D ce vor codifica informațiile completate în formular, aceste coduri fiind la rândul lor conținute în respectivul formular, conform cu design-ul acestuia. Codul de bare generat trebuie să poată fi recunoscut ulterior atât în cazul în care formularul se tipărește / scanează, dar și în cazul în care este transmis în format electronic;
 - Câmpurile din formular trebuie să permită validări și selecții din liste statice;
 - Posibilitatea de precompletare a unor câmpuri în funcție de valorile introduse în alte câmpuri.

3.5.4.3.3 Componenta server web

Cerințe:

Componenta server web are rolul de a dirija traficul HTTP către serverele de aplicații, totodată activând și ca proxy server, respectând topologia propusă prin arhitectura logică a sistemului.

168

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

- Suport pentru SSL și autentificare de baza;
- Extensia funcționalităților pe baza de plugin-uri sau module;
- Operarea în mod reverse-proxy pentru virtualizarea accesului la resursele expuse de sistem;
- Funcționalități de rescriere a adreselor URL;
- Să dispună de mecanisme de balansare a încărcării;
- Să permită configurarea într-un mod de disponibilitate ridicată utilizând mecanisme de tip cluster;
- Să ofere suport pentru IPv4 și IPv6;
- Să permită rularea conținutului dinamic oferind suport pentru tehnologii de programare de largă răspândire;
- Să permită port tunneling;
- Să ofere servicii de web cache pentru creșterea performanței soluției și suport pentru compresia datelor.

3.5.4.3.4 Componenta server de aplicații

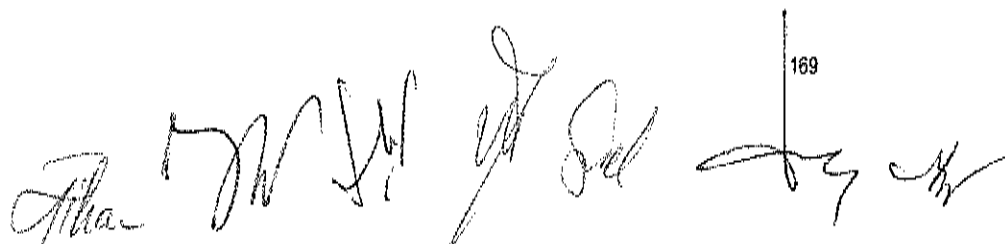
Cerinte:

Componenta server de aplicații va gestiona toate componentele aplicative din proiect, respectând topologia propusă prin arhitectura logică a sistemului.

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

- Compatibil cu specificațiile platformei Java Enterprise Edition 7. Platformă tehnologică completă pentru instalarea și execuția site-urilor web dinamice, serviciilor web și aplicațiilor JEE;
- Suport complet pentru specificațiile Java Servlets;
- Suport complet pentru specificațiile JavaServer Pages;
- Suport complet pentru specificațiile Enterprise JavaBeans;
- Transformarea datelor în format XML utilizând standardul W3C Extensible Stylesheet Language (XSL);
- Citirea și scrierea datelor în format XML utilizând interfețele de programare standard Document Object Model (DOM);
- Securizarea serviciilor web utilizând standardele WS-Security și WS-SecurityPolicy;
- Suport complet pentru standardul Java Database Connectivity (JDBC);
- Suport pentru conectarea la multiple sisteme de gestiune a bazelor de date relaționale;
- Cache-ul de date distribuit va oferi mecanisme de acces concurrent la date și participare în tranzacții distribuite;

169



- Partajarea conexiunilor de date (Connection Pooling) integrat cu mecanismele de clustering și detectarea a defectelor implementate la nivelul bazelor de date;
- Suport complet pentru standardul Java Messaging Service (JMS);
- Suport complet pentru managementul tranzacțiilor utilizând specificația Java Transaction API (JTA);
- Suport pentru standardul Java Authentication and Authorization Service (JAAS);
- Mecanisme de grupare a serverelor în clustere de servere de aplicații atât în topologii de tip activ-activ cât și activ-pasiv;
- Consolă de administrare a serverelor de aplicații cu capabilități de gestiune a schimbărilor de configurații.

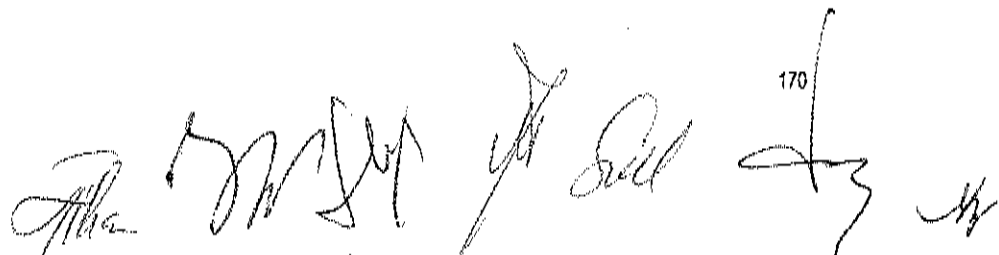
3.5.4.3.5 Componenta baze de date

Cerinte:

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

- Să fie un sistem de gestiune a bazelor de date de tip relațional;
- Să permită importul și exportul de date în formate de date general acceptate;
- Să permită minimizarea conflictelor de acces la date;
- Să ofere suport pentru proceduri stocate și triggeri;
- Să ofere suport pentru tranzacții autonome;
- Să permită partiționare logică a tabelor mari în scopul reducerii timpului de acces la date după diverse criterii de partiționare (list, range, hash);
- Să ofere suport pentru Unicode UTF-8;
- Să ofere suport de replicare bidirecțională a datelor între două instanțe ale bazei de date;
- Să ofere mecanisme de control și blocare la nivel de înregistrare și mecanisme de asigurare a consistenței la citire, pentru a permite accesul în mod concurent al utilizatorilor la date și pentru a se asigura integritatea datelor, baza de date trebuie să asigure suport pentru restricții de integritate în vederea prevenirii introducerii datelor invalide în tabelele bazei de date;
- Să permită restricționarea accesului la nivelul obiectelor bazei de date;
- Să permită instalarea unei singure baze de date pe mai multe noduri într-o arhitectură de tip cluster activ-pasiv;
- Va oferi un utilitar grafic pentru administrarea și monitorizarea SGBDR;
- Baza de date relațională va avea componente pentru optimizarea interogărilor;
- Va exista posibilitatea de a cripta tot traficul de rețea dinspre și către baza de date;
- Va permite oprirea temporară a unui nod pentru mentenanță, suport, upgrade, sistemul în acest timp fiind disponibil;

170



- Stocare criptată a datelor în baza de date în mod transparent față de aplicație, fără a fi necesară scrierea de cod în aplicație pentru a se cripta și decripta datele stocate în baza de date;

Notă: Ofertanții vor avea în vedere ca această componentă trebuie să asigure continuitatea și compatibilitatea nativă a tipurilor de date replicate pentru un schimb continuu și masiv de date în timp real, cu bazele de date ale unor instituții care dețin sisteme integrate de la nivel național și/sau alte instituții cu care ONRC are încheiate acorduri de colaborare corespunzătoare cerințelor de interconectare.

3.5.4.3.6 Componenta replicare date

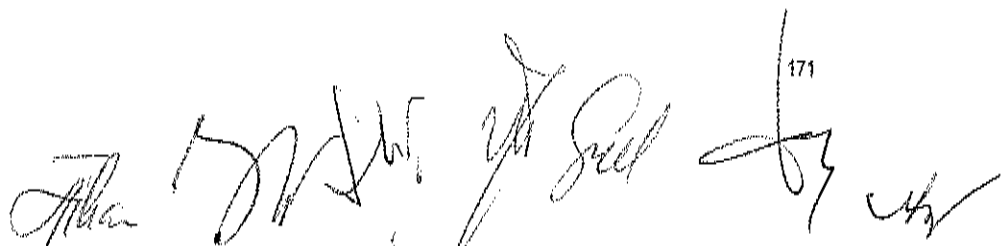
Cerinte:

Componenta de replicare date va avea rolul de a asigura replici de date între cele două site-uri (primar și secundar), astfel încât să se asigure consistența necesară reluării activității în site-ul secundar, în cazul în care exista o avarie în site-ul principal. Totodată, componenta de replicare va putea asigura replicarea selectivă de date și către alte surse de baze de date astfel încât să se poată implementa, în mod alternativ, și posibilitatea de integrare între sisteme sau servicii utilizând și mecanisme specifice bazelor de date, nu doar mecanisme specifice SOA (servicii web, schimb mesaje etc.).

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

- Captarea datelor modificate în baza de date sursa se va face prin mecanisme care nu au impact asupra performanței acestora. 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.
- Posibilitatea de replicare între diverse tipuri de baze de date (minim Oracle, MS SQL, baza de date ofertată);
- Replicarea se va baza pe mecanisme ce nu impactează performanța bazelor de date, cum ar fi log-ul tranzacțional al bazei de date;
- Trebuie să asigure independența de platformă și versiune de bază de date între sursa și destinație;
- Capabilități pentru replicarea tabelor, secvențelor precum și a comenzilor DDL;
- Replicarea întregii baze de date, a unui set de tabele sau chiar a unei singure tabele. Posibilitate de a replica doar un subset de coloane sau rânduri tabelă;
- 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;
- Posibilitatea de replicare bidirecțională cel puțin între instanțe de baza de date de același tip.

171



3.5.4.3.7 Componenta de integrare și schimb de mesaje

Cerinte:

Componenta de integrare și schimb de mesaje va avea rolul de a asigura suportul necesar pentru integrarea cu alte sisteme informatice, interne - ONRC, dar și externe (alte instituții). Integrarea se va realiza respectând principiile SOA, componenta de integrare având rolul de a fi un nivel intermediar între consumator (utilizator, sisteme) și furnizor (serviciile electronice ce rulează ca aplicații).

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

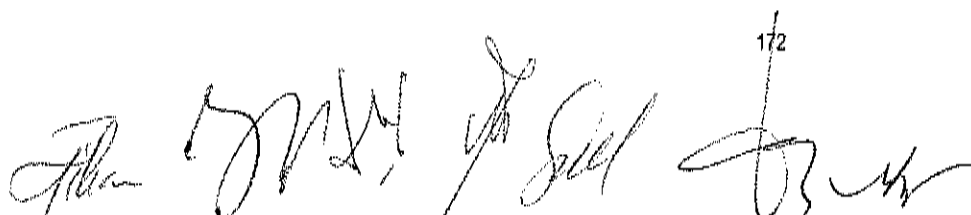
- Suport pentru soluții moderne și deschise de integrare conform principiilor și conceptelor arhitecturilor Service Oriented Architecture (SOA) și Event Driven Architecture (EDA);
- Să fie bazată pe standardele deschise de interoperabilitate a aplicațiilor WS-I Basic Profile, WSDL, WS-*, XML, SOAP, UDDI, REST;
- Permite comunicații sincrone și asincrone inter-aplicații;
- Permite folosirea de canale multiple de notificare pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicații;
- Se integrează cu soluții de tip Service Registry bazate pe standardul deschis Universal Description Discovery and Integration (UDDI);
- Tipurile de mesaje transportate suportate de soluția de tip Service Bus vor fi cel puțin: XML, text, binar, atașament;
- Capabilități extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL) și XQuery;
- Conectori la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje, sisteme de fișiere, FTP;
- Conectori la principalele platforme de tip server de aplicație;
- Servicii de transport cu suport pentru persistența datelor și garantarea livrării datelor;
- Capabilități extinse de transformare și dirijare a datelor bazate pe conținutul transportat;
- Posibilitatea definirii, la momentul execuției, a adreselor de destinație a mesajelor, eventual prin interogarea unei soluții de tip Service Registry;
- Să ofere servicii de securitate atât la nivel transport cât și la nivel de aplicație;
- Gestiunea încărcării livrării mesajelor către serviciile destinație înregistrate la nivelul magistralei de interconectare folosind cozi de mesaje tampon;

3.5.4.3.8 Componenta procese de business

Cerinte:

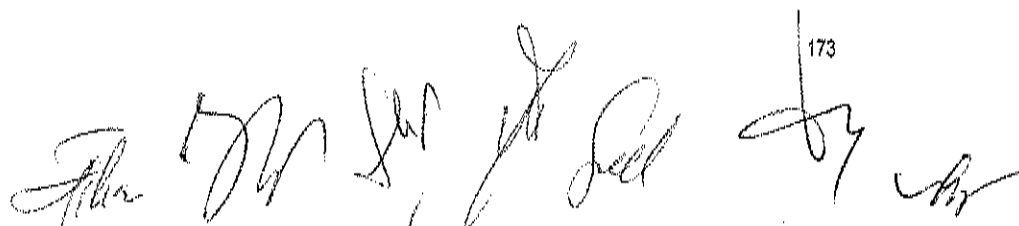
Componenta de gestiune a proceselor de business asigura suport la nivelul serviciilor electronice implementate prin implementarea / modelarea proceselor utilizând instrumente standardizate BPMN/BPEL,

172



publicarea proceselor și execuția acestora la nivelul fiecărui serviciu electronic ce implementează o automatizare de proces. Totodată, componenta de gestiune procese permite definirea de indicatori de performanță (KPI) ce pot fi urmăriți pe parcursul execuției proceselor/procesului aferent unui serviciu electronic, informațiile colectate fiind ulterior accesibile sub forma de rapoarte operaționale (dashboard-uri). Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care va trebui să le ofere sunt:

- Suport complet pentru dezvoltarea, testarea, execuția, monitorizarea, optimizarea și administrarea proceselor de flux;
- Să permită definirea și utilizarea în cadrul fluxurilor de lucru a unor formulare și câmpuri completabile în mod manual și automat;
- Fluxurile de business să se poată versiona în cadrul proiectării acestora, păstrând coerența/legătura cu versiunea la rulare;
- Modelarea declarativă a proceselor de afaceri utilizând BPMN sau BPEL cu ajutorul mediului de dezvoltare integrat al sistemului;
- Suport pentru standarde de largă răspandire cum ar fi: XML, web services, JMS, J2EE, SMTP, HTTPS;
- Trimitere automată de notificări de inițiere de activități, termene limita, stadiu de execuție, finalizare și să trateze automat acest tip de notificări primite de la sisteme externe;
- Oferă șabloane predefinite de dirijare a activităților către utilizatorii cu roluri specifice la nivelul aplicațiilor precum și interfețe grafice de lucru cu fluxurile automatizate;
- Va permite colectarea permanentă de statistici de execuție - timpi de execuție, frecvență de apariție evenimente, stări fluxuri - pentru procesele instalate;
- Pentru interacțiunea umană cu aplicațiile compozite, Să ofere șabloane predefinite de dirijare a activităților către utilizatorii cu roluri specifice la nivelul fluxurilor;
- Modul integrat de stocare și evaluare a regulilor de business, externe proceselor modelate, pe care personalul non-tehnic le va putea accesa și modifica ulterior;
- Suport pentru includerea sub-proceselor apelate dintr-un proces principal în tranzacția fluxului inițiator;
- Facilități de activare a auditării fluxurilor;
- Monitorizarea activității la nivelul proceselor, cu capabilități de colectare informații și raportare grafică;
- Monitorizarea în timp real a indicatorilor de performanță (KPI). Definirea de alerte și acțiuni în cazul în care indicatorii de performanță nu ating anumite praguri valorice;
- Asignare dinamică a responsabililor de activități, priorități și SAL-uri evaluată în timpul execuției proceselor pe baza datelor de business, datelor istorice sau a unor servicii externe;
- Integrare cu depozite de documente externe folosind componente de tip interfață utilizator existente în produsul de baza;



173

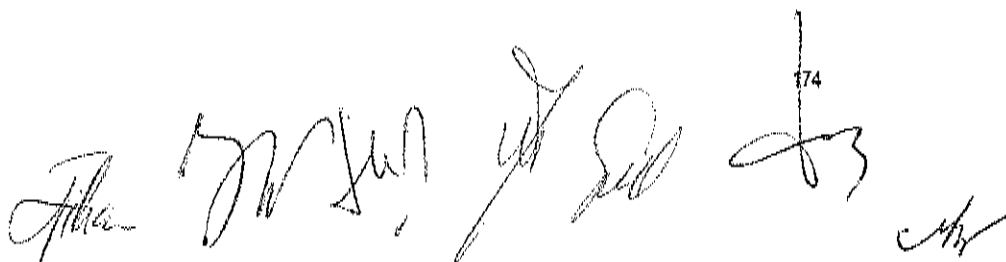
3.5.4.3.9 Componenta raportare și analiza

Cerinte:

Componenta de raportare și analiză va permite crearea și rularea de rapoarte peste informațiile stocate în baza de raportare, precum și efectuarea de analize și prezentare sub forma de dashboards pentru a constitui în orice moment o viziune de ansamblu asupra situației la zi din cadrul instituției. Se are în vedere un număr de 150 de utilizatori distribuiți între ONRC și ORCT-uri, precum și un număr de 5 administratori responsabili cu partea operațională.

Aceasta componenta va permite rularea de rapoarte atât de către utilizatori, cât și în mod neasistat, programat la un anumit moment. În urma obținerii rezultatelor executării rapoartelor neasistate, acestea vor fi automat transmise către anumiți utilizatori (specificați pentru fiecare raport în parte). Componenta de raportare și analiză avansată va oferi următoarele funcționalități majore:

- Prezentarea datelor în formate variate (de exemplu tabele, tabele pivot, grafice, texte derulante);
- Funcționalități de navigare ghidată pentru utilizatorii finali, cu posibilități multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât și pentru grafice;
- Combinarea rezultatelor obținute de pe platforme diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
- Salvarea rapoartelor în formate diferite (Excel, PDF, Word, HTML etc.);
- Definirea de tablouri de bord și includerea rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
- Modificarea tablourilor de bord sau a rapoartelor, posibilitatea de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
- Accesul la informație se va realiza printr-un nivel de metadata care va ascunde utilizatorilor finali complexitatea structurilor fizice de date;
- Nivelul de metadata expus utilizatorilor va fi comun la nivelul tuturor modulelor sistemului de raportare și analiză;
- Utilizatorii își vor putea crea singuri propriile rapoarte (analize ad-hoc) fără să fie nevoiți să cunoască structurile fizice de date pe care le accesează;
- Accesarea datelor de pe platforme relaționale, multidimensionale, foi de calcul sau din fișiere stocate în sisteme de fișiere distribuite de tip Big Data;
- Integrarea cu platforma de autentificare și management al utilizatorilor existentă în cadrul ONRC, oferind în același timp capacități proprii de definire a rolurilor pentru restricționarea accesului la rapoarte;
- Interacțiunea utilizatorilor finali cu aplicația se va face într-o interfață de tip web, fără a necesita instalarea de componente software suplimentare pe calculatoarele utilizatorilor;
- Va expune o interfață de administrare atât a drepturilor de acces la diferite zone, cât și a drepturilor de acces pe diferite tipuri de acțiuni;
- Va fi scalabilă și va dispune de mecanisme de clustering a componentelor, astfel încât să poată fi adăugate ulterior resurse hardware suplimentare;



Handwritten signatures and a stamp. The stamp is a vertical rectangle with the number '174' inside. There are several cursive signatures written across the bottom of the page.

- Va permite facilități avansate de formatare a rapoartelor;
- Va oferi posibilitatea de salva, organiza și partaja rapoartele cu alți utilizatori;
- Va oferi capabilități de drill-down (navigare în adâncime) pe diferite nivele de agregate;
- Va permite acces la surse de date multiple, în mod transparent pentru utilizatorul final;
- Accesul utilizatorului final se va face dintr-o singură interfață web din care să aibă acces la toate componentele de analiză și raportare;
- Va oferi utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât și în aplicația de analiză și raportare;
- Va dispune de mecanisme de alertare pentru utilizatorii finali;
- Va oferi utilizatorilor finali posibilitatea subscrierii la alertele definite;
- Rapoartele analitice să poată fi construite pe un număr variabil de interogări analitice. Instrumentul nu va limita numărul de astfel de interogări;
- Să asigure posibilitatea de writeback (scriere) în baza de date, atât relațională cât și multidimensională, din aplicația de raportare;
- Este necesar ca aplicația de raportare să poată afișa anumite valori identificate ca fiind critice, să semnalizeze depășirea unor praguri ale acestor valori, să semnalizeze apariția unor evenimente. Astfel, va oferi utilizatorilor posibilitatea de formatare condiționată a valorilor prin setarea unor praguri, pentru a evidenția valorile excepționale.
- Să nu necesite replicarea datelor pe un server separat, ci să folosească capabilitățile bazei de date sursa.
- Mediul de lucru pentru utilizatorii finali sau alți dezvoltatori de rapoarte/analize să fie în mediu web pur, interacțiunea cu sistemul să se realizeze prin operațiuni de tip „point and click” și „drag and drop” (să nu necesite cunoștințe de programare din partea utilizatorilor);
- Să ofere posibilitatea definirii de rapoarte înălțuite, datele din raportul copil fiind filtrate pe baza rezultatelor din raportul părinte;
- Să permită tuturor utilizatorilor crearea sau modificarea de rapoarte, analize ad-hoc și tablouri de bord, acordarea drepturilor specifice (consultare, creare de obiecte etc.) urmând a fi făcută de către administratori;

3.5.4.3.10 Componenta ETL

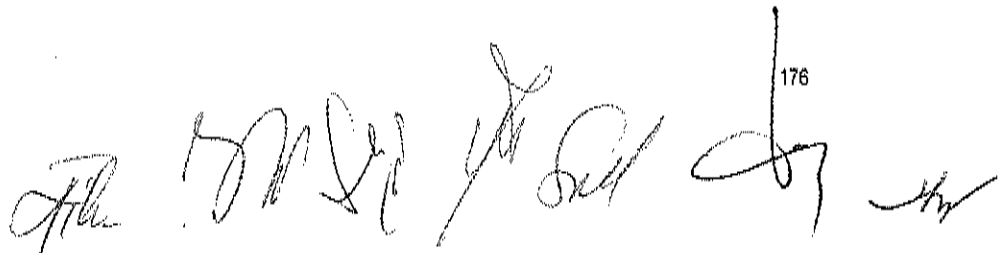
Cerinte:

Componenta Extragere, Transformare și Încărcare date (ETL) va asigura încărcarea datelor din baza operațională istorică a sistemului SII în baza de date operațională a noului sistem, precum și încărcarea datelor în alte surse de date ce mapează structuri similare de informație plecând de la datele operaționale din noul sistem, precum baza de date de raportare.

Handwritten signatures and initials at the bottom of the page, including a signature that appears to be 'Ala' and another that includes the number '175'.

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**, precum și de alocarea de resurse conform arhitecturii sistemului. Principalele funcționalități pe care componenta ETL va trebui să le ofere sunt:

- Compatibilitate cu tipurile de baze de date Oracle existente în infrastructura ONRC și cu baza de date oferită;
- Definirea proceselor de extragere - transformare - încărcare dintr-o interfață grafică;
- Gestionarea următoarelor cerințe de proces:
 - Agregare;
 - Compresie/Decompresie;
 - Conversie tip și/sau format date;
 - Manipulare și executare de operații aritmetice pe seturi de date;
 - Alocare (Assign) și conectare condițională;
 - Filtrare;
 - Partiționare/grupare pentru seturile de înregistrări;
 - Recunoaștere/împerechere pentru înregistrările duplicate;
 - Sortare;
 - Manipularea înregistrărilor;
 - Alocarea și rezoluția cheilor surrogat;
 - Validarea datelor;
- Procesarea înregistrărilor respinse;
- Executarea de job-uri multiple în mod concurrent;
- Să poată accesa și integra date din baze de date diferite și să ofere suport pentru accesarea datelor aflate în fișiere (.txt, .csv, .xml);
- Să permită implementarea propriului mecanism de detectare a modificării datelor (Changed Data Capture);
- Să suporte modalități diferite de încărcare a datelor:
 - încărcare masivă de date (Bulk Load);
 - încărcare incrementală (Incremental Update);
 - încărcare a datelor captate printr-un mecanism de detectare a modificării datelor (Changed Data Capture);
- Să permită definirea și incorporarea de componente reutilizabile suplimentare. Aceste componente trebuie să acopere majoritatea tipurilor de transferuri de date: din fișiere în suport relațional, între tipuri diferite de baze de date relaționale (de exemplu între Oracle și Fox Pro sau alt tip de bază de date relațională);



176

- Procesele de extracție, transformare și încărcare să poată fi definite sub formă declarativă, prin selectarea și maparea vizuală a tabelelor implicate și menționarea componentelor de transfer necesare (pentru optimizarea procesului de dezvoltare);
- Să permită vizualizarea/modificarea procesului sau codului generat și reluarea anumitor pași de proces astfel încât să se detecteze eventualele erori;
- Instrumentul propus trebuie să genereze automat codul programelor de încărcare și transformare, pornind de la specificațiile vizuale introduse de dezvoltator, fiind optimizat pentru fiecare tehnologie de baza de date accesată;
- În cadrul mapărilor de date, să se permită definirea de filtre și de restricții asupra câmpurilor implicate;
- Să permită consolidarea pașilor de integrare de date sub forma unor fluxuri cu operatori de loop, ramificare pe baza unor condiții etc.
- Să permită notificarea prin email a administratorilor în anumite condiții de lucru și să poată întrerupe fluxul de execuție în cazul unor erori considerate grave;
- Fluxurile definite să poată fi rulate în medii diferite (producție, dezvoltare) doar prin selectarea contextului de lucru;
- Mediul de lucru să nu necesite cunoștințe avansate de programare;
- Să permită păstrarea istoricului diverselor versiuni ale mapărilor de date;
- Pentru optimizarea proceselor și a accesului la date, soluția trebuie să se bazeze pe componente reutilizabile, gata construite, de tipul celor mai bune practici, care să încorporeze elemente predefinite pentru consolidarea, asigurarea calității și accesul specific pentru fiecare din tipurile de surse accesate;
- Să permită extinderea conectivității sistemului prin adăugarea de noi surse de date;
- Componentele reutilizabile predefinite pentru accesul la date trebuie să cuprindă logica necesară extracției și integrării de date, cu toți pașii ce trebuie parcurși, inclusiv pentru detectarea modificărilor (mecanism de Change Data Capture) la sursă pentru încărcări incrementale;
- În cadrul mapărilor trebuie să fie permisă utilizarea unor funcții native ale bazei de date accesate;

3.5.4.3.11 Componenta gestiune identități și acces utilizatori

Cerințe:

Componenta de gestiune identități și acces utilizatori (IDM) va asigura definirea unui profil extins asociat utilizatorului, asocierea acestuia la diferite politici de securitate, controlul accesului la resurse și implementarea Single Sign-On (SSO). Totodată, va oferi suport pentru integrarea cu componenta Active Directory prezenta în cadrul ONRC și totodată va asigura integrare și cu componenta PKI și cu cea de integrare cu eIDAS, astfel încât să se asigure o implementare completă în ceea ce privește accesul autentificat la resurse și gestiunea consolidată a utilizatorilor.

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori interni din capitolul **Capacitate și dimensionare date**. Principalele funcționalități pe care componenta IDM va trebui să le ofere sunt:

177

- Va asigura serviciul de autentificare a utilizatorului la intrarea în sistemul informatic integrat (Single Sign-On centralizat). Din pagina principală utilizatorul va putea introduce numele utilizatorului și parola. După ce utilizatorul a fost autentificat, el va avea acces la toate zonele aplicative pentru care este autorizat, fără a i se mai cere user și parolă de acces;
- Utilizatorii și drepturile de acces sunt stocate și gestionate în cadrul unui sistem standard de autentificare unică. Accesul la oricare din aplicațiile componente ale soluției se va face utilizând o autentificare unică la începutul sesiunii de lucru. Drepturile și rolurile utilizatorului să fie stocate în mod unic în serviciul de tip director oferit;
- Trebuie să permită stocarea politicilor de acces și a configurației de sistem într-un sistem de tip director;
- Autentificarea unică a utilizatorilor și autorizarea acestora în sistem prin mecanisme de tip autentificare unică prin intermediul rolurilor și privilegiilor;
- Definiere centralizată de drepturi la nivel de serviciu director compatibil cu standardul LDAP. Utilizatorii vor avea acces numai la aplicațiile și documentele pentru care au drepturi;
- Mod flexibil și unitar pentru gestiunea drepturilor și politicilor de acces ale utilizatorilor la toate resursele sistemului integrat prin definiere, modificare, ștergere, explorare, păstrare istoric sesiuni de acces;
- Integrare cu alte soluții de tip serviciu director oferind sincronizare și interoperabilitate;
- Mecanisme de securitate implementate pe mai multe niveluri, la nivel sistem de operare, la nivel de acces în rețea, la nivel de aplicație și la nivel de bază de date;
- Alocare automata de resurse către utilizatori pe baza de politici și drepturi. Pentru orice set de utilizatori, administratorii pot specifica nivelul de acces pentru fiecare resursa ce urmează a fi alocata, astfel încât fiecare utilizator să aibă doar drepturile de acces necesare îndeplinirii sarcinilor de lucru specifice;
- Autentificarea, identificarea, verificarea drepturilor și permisiunilor;
- Suport pentru delegarea administrării utilizatorilor;
- Suport pentru politici avansate de parole: lungime parola, număr și tipuri de caractere necesare, să împiedice reutilizarea aceleași parole în mod repetat după expirarea/schimbarea acesteia, dicționar de parole care nu trebuie utilizate;
- Să poată genera parole în mod automat la înregistrarea utilizatorilor;
- Definierea de ierarhii de roluri și organizații;
- Accesarea datelor despre utilizatori atât din baze de date cât și din directoare LDAP, cu posibilitatea de agregare selectivă a profilurilor și expunerea acestor informații în format LDAP către alte sisteme;
- La înrolarea unui nou utilizator în sistem să genereze automat, fără intervenția unui administrator, drepturile de acces necesare pentru utilizatorul respectiv conform cu rolul alocat utilizatorului în sistemul ONRC;
- La părăsirea organizației de către un utilizator să închida automat toate conturile aferente utilizatorului respectiv, fără intervenția unui administrator;

Handwritten signatures and initials at the bottom of the page, including a signature that appears to be 'Alban' and another with the number '178' written above it.

- Să identifice automat conturile orfane / neutilizate sau cu perioada mare de neutilizare (perioada de neutilizare trebuie să fie un parametru configurabil) și să asigure închiderea automată a acestor conturi în conformitate cu politica de securitate stabilită în organizație;
- Pentru a eficientiza operațiunile de resetare a parolelor fără intervenția unui administrator, utilizatorii trebuie să își poată configura singuri întrebări și răspunsuri de securitate care să fie utilizate pentru resetarea parolei de acces la sistemul informatic dintr-o interfață web cu acces facil;

3.5.4.3.12 Componenta integrare eIDAS

Cerințe:

Componenta de integrare eIDAS este responsabilă cu integrarea dintre propria infrastructură de PKI și de gestiune a identității și accesului și nodul național eIDAS. Adaptorul eIDAS va acționa ca o punte între propria infrastructură de gestiune a identității, de PKI (gestiune certificate), serviciile electronice (ca și aplicații de business) și cetățeni, instituții sau utilizatori proprii ONRC ce se vor autentifica și autoriza pentru acces securizat la serviciile electronice.

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori de la capitolul **Capacitate și dimensionare date**.

Componenta va trebui să implementeze la nivelul sistemului integrat următoarele funcționalități de bază:

- Identificare, autentificare tip two-factor și semnătură electronică de pe orice dispozitiv;
- Autentificare multiplă: certificat digital, SMS/email OTP, LDAP sau dispozitiv mobil;
- Clasificarea autentificării: suport pentru eIDAS assurance levels, ITU-T X.1254, ISO/IEC 29115, NIST AAL;
- Suport pentru SAML 2.0 și OAuth/OpenID pentru implementarea Web SSO la nivelul interfețelor de utilizare;
- Suport cel puțin pentru standardele ETSI - PDF Advanced Electronic Signature (PAdES), XML Advanced Electronic Signatures (XAdES), CMS Advanced Electronic Signatures (CAAdES) și PKCS #1;
- Integrare cu echipamente de tip Hardware security module (HSM), compatibilitate cu echipamentele HSM incluse în proiect;
- Integrare cu componenta SIEM pentru procesarea syslog sau format raw;
- Suport pentru integrare autentificare avansată tip OTP (One Time Password) cu servere SMTP și gateway-uri SMS;

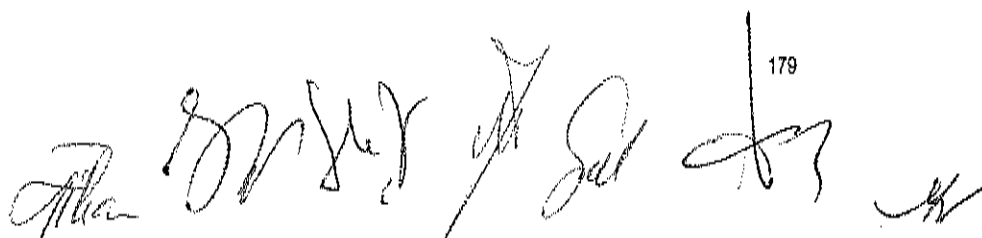
3.5.4.3.13 Componenta PKI

Cerințe:

Sistemul trebuie să fie proiectat și să conțină toate componentele astfel încât să se asigure următoarele principii de securitate:

- a) Autentificare
- b) Confidențialitate
- c) Integritate

179



d) Non-repudiere

În acest sens se are în vedere utilizarea tehnologiilor PKI (Public Key Infrastructure), mai precis certificate digitale și aplicații specifice de utilizare a acestora în vederea implementării principiilor mai sus menționate, astfel:

- Autentificare: va fi asigurată prin certificate digitale emise individual, pentru fiecare utilizator în parte. Sistemul va utiliza aceste certificate digitale pentru autentificare prin integrare cu componenta de gestiune a identității utilizatorilor și a accesului.
- Confidențialitate: va fi asigurată prin criptarea documentelor/informațiilor, utilizând tehnologiile PKI și algoritmi standard, și prin ștergerea documentelor utilizând algoritmi recunoscuți la nivel internațional. Sistemul va utiliza certificatele digitale pentru criptare.
- Integritate și Non-repudiere: vor fi asigurate prin semnătura electronică, utilizând tehnologiile PKI și algoritmi standard. Sistemul va utiliza certificatele digitale și echipamentele HSM pentru semnătura electronică.

Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori interni de la capitolul **Capacitate și dimensionare date**. Componenta PKI va trebui să includă următoarele funcționalități:

- Sistemul va avea un sistem de securitate care permite protejarea informației, atât față de accesul neautorizat intern, cât și față de accesul neautorizat extern. Protecția va fi asigurată atât la nivel hardware cât și software;
- În acest sens, sistemul va îndeplini anumite cerințe din punct de vedere al securității, cum ar fi autentificarea unică a utilizatorilor și autorizarea acestora în sistem prin mecanisme de tip autentificare unică prin intermediul rolurilor și privilegiilor;
- Se vor asigura autentificarea, verificarea drepturilor și permisiunilor printr-un mecanism de securitate, se vor oferi facilități extinse de autentificare și autorizare a utilizatorilor;
- Utilizatorii se vor conecta utilizând certificate digitale a căror valabilitate și validitate va fi verificată prin intermediul serviciului de verificare a validității certificatelor digitale prevăzut în sistem;
- Utilizatorii se vor autentifica la sistem exclusiv prin intermediul certificatelor digitale, prin conexiune SSL mutual. La fiecare acces, sistemul va verifica valabilitatea certificatului utilizat pentru autentificare, prin protocol OCSP în conformitate cu RFC 6960. Având în vedere faptul că certificatul digital poate fi stocat în oricare dintre cele trei variante (PKCS #12 stocat în propriul PC, smartcard sau terminal mobil), sistemul trebuie să permită autentificarea utilizatorilor indiferent de mediul de stocare al certificatelor digitale (și al cheilor private aferente);
- Accesul unui utilizator la sistem de pe PC se va putea realiza utilizând certificatul digital propriu, astfel:
 - în format PKCS #12, importat la nivelul sistemului de operare, în propriul PC; astfel procesul de autentificare se realizează direct între PC și sistem;
 - stocat pe dispozitivul criptografic propriu, conectat la PC, pe care sunt disponibile drivere aferente dispozitivului criptografic; astfel procesul de autentificare se realizează direct între PC și sistem;
 - stocat pe dispozitivul criptografic propriu, conectat la terminalul mobil propriu, sau stocat pe terminalul mobil propriu. Aceasta situație este aplicabilă în următoarele situații:
 - pe respectivul PC nu este importat certificatul digital în format PKCS #12;



180

- driverele dispozitivului criptografic nu sunt instalate sau utilizatorul nu este în posesia propriului dispozitiv;
- În cazul folosirii certificatului digital stocat pe dispozitivul criptografic propriu, conectat la terminalul mobil propriu, sau stocat pe terminalul mobil propriu procesul de autentificare necesită un mecanism de tip „challenge-response” pentru identificarea cu exactitate a utilizatorului care dorește să se autentifice la sistem. Mecanismul de tip „challenge-response” va utiliza tehnologia PKI pentru semnarea digitală a unui mesaj codificat în mod standardizat, de către ambele entități implicate în procesul de autentificare, respectiv componenta de server și utilizatorul. Fiecare dintre cele două entități va semna mesajul cu propriul certificat digital. Mesajul codificat trebuie să fie vizibil utilizatorului și să includă informații despre timpul de expirare al procesului de autentificare. Sistemul de autentificare trebuie să fie capabil și să permită operațiunile de semnătură cu certificate stocate în memoria terminalului mobil, cu certificate stocate pe Secure SD conectat la terminal, și cu certificate stocate pe dispozitive de tip smartcard (standard FIPS 140-2 level 2) cu interfața standard PKCS #11 conectate la terminal;
- Accesul unui utilizator la sistem se va putea realiza și de pe propriul terminal mobil utilizând certificatul digital propriu, stocat astfel:
 - pe dispozitivul criptografic propriu, conectat la terminalul mobil;
 - pe terminalul mobil
- În ambele situații, procesul de autentificare se realizează direct între terminalul mobil și sistem.

Modulul de autentificare și autorizare trebuie să ofere următoarele funcționalități:

- Să permită contexte diferite de securitate în funcție de secțiunea din sistem accesată de către utilizator. Soluția trebuie să permită prin configurare conexiuni HTTP (publice, care nu necesită autentificare) și HTTPS (cu autentificare) în funcție de aceste contexte;
- Să permită autentificarea utilizatorilor exclusiv pe baza certificatului digital X.509 v3 personal. Certificatele digitale pot fi emise de multiple Autorități de certificare definite de încredere, iar modulul trebuie să fie configurabil să se integreze cu oricare dintre ele folosind interfețe și protocoale standard;
- Să permită autorizarea utilizatorilor pe baza listelor de acces definite la nivelul modulului;
- Să permită autorizarea utilizatorilor pe baza extensiilor din certificatul digital (standard sau private, în conformitate cu standardul x509v3);
- Să realizeze criptarea comunicației dintre client și modul prin SSL (protocol HTTPS);
- Să permită configurarea credențialelor utilizatorilor pentru aplicațiile accesate prin intermediul sau (nume utilizator și parolă, număr serial certificat digital, Autoritatea de certificare emitentă);
- Să permită configurarea metodelor de autentificare utilizate de aplicațiile accesate prin intermediul sau (minim Basic Authentication, Form authentication, LDAP);
- Să permită verificarea validității certificatelor digitale atât prin protocol OCSP, conform RFC 6960, cât și pe baza listelor de certificate revocate publicate în servere de directoare conforme standardului LDAPv3;

3.5.4.3.14 Componenta semnare electronică

Cerințe:

Handwritten signatures and initials of several individuals, including a large signature at the top center and several smaller ones below it.

Componenta de semnare electronica este integrata cu componentele de gestiune identității și acces utilizatori și PKI și asigura posibilitatea de a semna documente în format electronic utilizând un certificat calificat. Componenta permite semnarea documentelor în interfața web, prin integrare cu restul de componente aplicative – semnarea având loc în interfața aplicației sau programatic, utilizând echipamentul HSM ce va stoca securizat certificatele utilizate în procesul de semnare în bloc a unui document sau set de documente. Componenta va fi dimensionată ținând cont de informațiile de volumetrie utilizatori interni de la capitolul **Capacitate și dimensionare date**.

Cerințele specifice la care aceasta componenta a sistemului trebuie să răspundă sunt următoarele:

- Suport pentru integrare la nivelul interfețelor web ale aplicațiilor prin intermediul unui API accesibil Java sau .NET;
- Implementare standard OASIS DSS ca protocol de acces la servicii web;
- Suport REST/WS și SOAP/WS pentru integrare cu aplicații;
- Autentificare bazată pe certificate digitale sau parole, posibilitate delegare autentificare către terți utilizând RADIUS sau LDAP. Suport SAML pentru implementare identitate federalizată;
- Incapsulare digitală a documentelor utilizând standarde precum PKCS #7, PAdES, XAdES, CAdES, W3C XML-DSig, W3C XML-Enc;
- Suport pentru digital time-stamping conform RFC 3161;
- Posibilitate de verificare status certificat utilizând liste de certificate revocate (CRL) sau OCSP;
- Suport la integrare cu aplicații externe utilizând WebDAV sau XAM.


3.5.4.3.15 Componenta monitorizare și management infrastructură

Cerinte:

Componenta management și monitorizare infrastructură va asigura managementul infrastructurii și serviciilor furnizate de noul sistem în cazul operării sistemului în producție. Scopul acestei componente este eficientizarea activității în organizația IT, precum și creșterea calității serviciilor oferite, bazat pe bune practici și pe automatizarea proceselor. Aceasta va asigura un management cuprinzător al evenimentelor, o monitorizare proactivă a performanței, precum și un sistem automatizat de alertare (pe email și SMS), raportare și realizare grafică pentru elemente de rețea, sisteme de operare, pachete software dezvoltate intern sau adaptate și aplicațiile ce se vor implementa în cadrul proiectului.

Componenta de Management și monitorizare infrastructură va realiza monitorizarea serviciilor prin modelare bazată pe componentele de infrastructură, iar informațiile colectate vor fi puse la dispoziția administratorilor într-un tablou de bord unic. Componenta va fi dimensionată ținând cont de alocarea de resurse conform arhitecturii sistemului. Cerințele specifice la care aceasta componenta a sistemului trebuie să răspundă sunt următoarele:

- monitorizarea integrată a elementelor de infrastructură legate de rețea, sisteme, aplicații eterogene. Platforma va gestiona dispozitive de rețea provenind de la diferiți producători, diferite sisteme de operare, diferite tipuri de aplicații - baze de date, servere de internet etc.;



182

- crearea (descoperirea automată) și prezentarea de hărți care să prezinte legăturile dintre diferite componente de infrastructură (elemente de rețea, servere, aplicații) pentru a oferi o imagine totală a sistemului și a serviciilor din rețea;
- generarea și prezentarea în interfață grafică de evenimente în cazul în care apar situații de excepție;
- afișarea stării serviciilor în timp real, prin intermediul tabloului de bord;
- colectarea datelor de performanță despre infrastructură și servicii respectiv raportarea acestora;
- păstrarea evenimentelor într-o bază de date relațională accesibilă prin ODBC/JDBC;
- folosirea de standarde: comunicarea între componentele soluției să fie bazată pe protocoale standard, să fie utilizate limbaje de programare standard;
- să existe capabilități de monitorizare predefinite incluse în soluția livrată, adaptate tehnologiilor oferite în cadrul celorlalte subsisteme/platforme funcționale;
- capabilități de monitorizare configurabile;
- să dispună de o interfață grafică nativă web, prin care să se poată realiza operațiile de configurare
- componenta de monitorizare a infrastructurii hardware și software va permite următoarele:
 - capabilități de monitorizare fără agenți a infrastructurii IT, a serviciilor IT și a performanței aplicațiilor;
 - monitorizarea nativă și fără agenți a echipamentelor de rețea, a sistemelor de operare și aplicațiilor;
 - inițierea de acțiuni corective cum ar fi repornirea echipamentelor, curățarea spațiului de pe disk și executarea comenzilor;
 - metode de notificare cum ar fi: e-mail, SNMP trap, POST și alerte în baze de date;
 - monitorizarea infrastructurii hardware și software bazată pe agenți de monitorizare, ce vor suporta diferite sisteme de operare.
 - agenții de monitorizare vor include pachete de monitorizare predefinite cel puțin pentru infrastructura software de tipul sisteme de gestiune a bazelor de date, servere de aplicație, sisteme de mail, sisteme de stocare a profilurilor de utilizator (conform tehnologiilor existente în sistemul informatic al ONRC și oferite în cadrul acestui proiect);
- posibilitatea descoperirii automate a configurațiilor și managementul configurațiilor:
 - descoperirea de calculatoare, echipamente de rețea, imprimante, baze de date, aplicații, procese, porturi, adrese IP;
 - descoperirea automată a dependențelor funcționale dintre elementele arhitecturii IT;
 - utilizarea de protocoale standard, precum ICMP, SSH, NTCMD, WMI, HTTP, Telnet, SNMP;
 - împărțirea și descoperirea infrastructurii pe zone funcționale și/sau administrative;
- Managementul serviciilor oferite de sistem, având următoarele funcționalități:
 - să dispună de o consolă unică pentru vizualizarea și gestionarea evenimentelor;
 - să permită exportul evenimentelor conținute în consola de monitorizare, cel puțin în format Excel și CSV;
 - să permită monitorizarea stării de sănătate a unui serviciu sau proces de infrastructură;

183



- să permită vizualizarea stării operaționale a serviciilor oferite de sistem, pe baza unei hărți personalizate;
- să permită auditarea modificărilor efectuate asupra configurației unei componente parte a unui serviciu;

3.5.4.3.16 Componenta SIEM/SOC

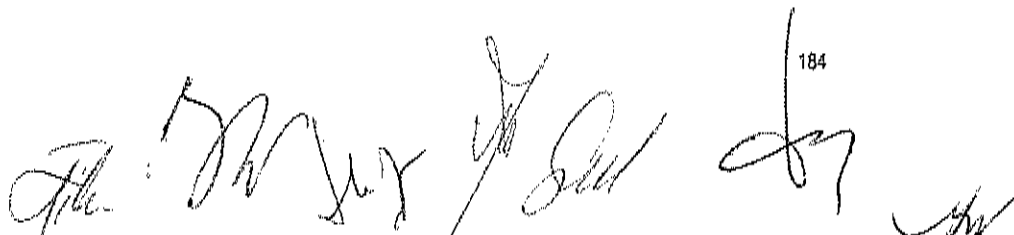
Cerinte:

Componenta SIEM/SOC poate fi livrată ca appliance fizic sau virtual, în funcție de soluția tehnică adoptată, și va implementa funcționalități de colectare și de analiză a potențialelor incidente de securitate, inclusiv de identificare a comportamentelor abuzive sau a încercărilor de utilizare neconformă a sistemului.

Componenta va fi dimensionată ținând cont de alocarea de resurse conform arhitecturii sistemului. Cerințele specifice la care aceasta componenta a sistemului trebuie să răspundă sunt următoarele:

- Să se poată colecta informații atât de pe echipamentele care au instalat agent de monitorizare, cât și de pe echipamente fără agent;
- Managementul datelor colectate se va realiza distinct pentru date recente și pentru date istorice. Managementul datelor recente se va face într-o bază de date on-line, din care se vor realiza toate operațiunile de analiză, emiteră a alertelor, raportare etc. Datele istorice se vor păstra într-o bază de date off-line, în format comprimat care să asigure eficiența spațiului de stocare. Pentru asigurarea integrității datelor, datele arhivate vor fi semnate digital. În cazul în care este necesar, datele arhivate vor putea fi mutate în baza de date operațională pentru prelucrare și analiză;
- Analiza și prelucrarea informațiilor colectate, inclusiv să se poată programa acțiuni ca urmare a îndeplinirii unor anumite condiții (evenimente identificate). Colectarea datelor să se poată realiza cu agenți de colectare instalați în diferite puncte ale rețelei, iar datele colectate să fie centralizate în scop de stocare și analiză;
- Datele colectate din diferite surse vor fi inițial prelucrate în scopul normalizării, după care vor fi stocate folosind un model comun de date, care să permită analiza integrată ulterioară a datelor;
- Analiza datelor se va realiza atât automat, prin programarea unor criterii și alerte, cât și manual, prin funcționalități de căutare și de raportare;
- Analiza manuală va include posibilitatea filtrării informațiilor conform unor criterii de filtrare configurabile. De asemenea, datele vor putea fi ordonate în funcție de atributele disponibile;
- Vor exista funcționalități de raportare și rapoarte predefinite pe tipologii de incidente, tipuri de sisteme de operare și sisteme de autentificare;
- În scopuri de raportare sau de analiză a evenimentelor, se va putea urmări corelarea între evenimente de tip DHCP (alocare de adrese IP), acces VPN, autentificare Directory, astfel încât să fie posibilă identificarea și urmărirea sesiunilor de utilizatori;
- Evenimentele înregistrate în conformitate cu politica de securitate stabilită vor fi etichetate, pentru o gestionare mai ușoară și vor fi stocate într-o structură optimizată pentru căutare și pentru păstrarea unei

184



dimensiuni mici a spațiului de stocare necesar. În scopuri de raportare sau analiză, datele vor fi importate din această structură intermediară într-o structură de bază de date;

- Va oferi suport pentru detecția automată a amenințărilor și atacurilor cibernetice, oferind totodată vizibilitate și posibilități de răspuns;
- Dispune de capabilitati de analiza comportamentala bazata pe inteligenta artificiala (self-learning) a atacurilor cibernetice;
- Va dispune de capabilități de analiză a traficului, a fișierelor log de la sisteme de securitate, sisteme de autentificare sau aplicații tip SaaS;
- Va dispune de capabilități de analiză corelată a amenințărilor cibernetice cu prioritizare a răspunsului în funcție de nivelurile de risc asociate amenințărilor;
- Va oferi suport pentru automatizarea răspunsurilor la diferite tipuri de atacuri/amenințări cibernetice, dispunând totodată și de capabilități de integrare cu componente tip endpoint, firewall sau NAC;
- Vor exista funcționalități de raportare și rapoarte predefinite pe tipologii de incidente, tipuri de sisteme de operare și sisteme de autentificare;
- În scopuri de raportare sau de analiză a evenimentelor, se va putea urmări corelarea între evenimente de tip DHCP (alocare de adrese IP), acces VPN, autentificare Directory, astfel încât să fie posibilă identificarea și urmărirea sesiunilor de utilizatori;
- Evenimentele înregistrate în conformitate cu politica de securitate stabilită vor fi etichetate, pentru o gestionare mai ușoară și vor fi stocate într-o structură optimizată pentru căutare și pentru păstrarea unei dimensiuni mici a spațiului de stocare necesar. În scopuri de raportare sau analiză, datele vor fi importate din această structură intermediară într-o structură de bază de date relațională;

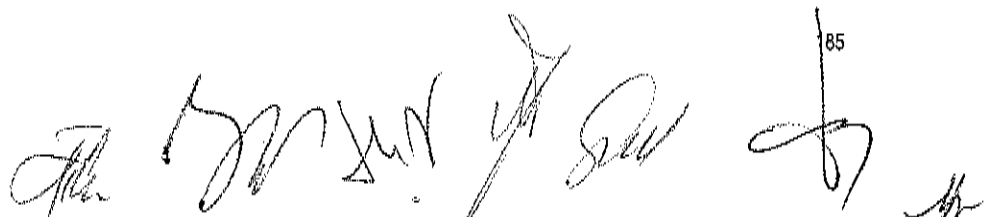
3.5.4.3.17 Componenta protecție servere

Cerinte:

Rolul acestei componente este de a oferi securitate serverelor fizice și virtuale din cadrul proiectului, fiind integrată cu componenta de virtualizare servere și având un modul centralizat de control astfel încât toate incidentele de securitate să fie accesibile unitar printr-o singură interfață.

Componenta va fi dimensionată ținând cont de alocarea de resurse conform arhitecturii sistemului. Funcționalitățile principale pe care trebuie să le ofere componenta de protecție servere sunt următoarele:

- Integrare cu platforme de virtualizare servere pentru asigurarea protecției mașinilor virtuale, inclusiv cu tehnologia de virtualizare propusă în cadrul proiectului;
- Apărarea serverelor împotriva amenințărilor la nivel de rețea prin intermediul funcțiilor de prevenire a intruziunilor și firewall la nivel de host/dispozitiv;



185

- Aplicarea unui patch virtual sistemelor vulnerabile prin intermediul functionalitatii de prevenire a intruziunilor;
- Protejarea împotriva atacurilor de tip ransomware;
- Detectarea și stoparea modificărilor de sistem malițioase sau suspicioase printr-un sistem de securitate bine pus la punct care include controlul aplicațiilor și monitorizarea integrității serverelor;
- Implementarea unor controale de securitate multiple cu ajutorul unei singure console de management și raportare;
- Descoperirea rapida și protejarea proceselor din producție prin intermediul integrării la nivel de API;
- Gestionarea proceselor de producție bazata pe arhitectura aplicațiilor și nu pe localizarea fizica sau logica a serverelor;
- Raportarea centralizată cuprinzând toate mediile de producție pentru o conformitate cu GDPR și alte regulamente în vigoare;
- Reducerea riscurilor prin intermediul aplicării automate a politicilor de securitate și a controalelor de securitate bazate pe context;
- Protejarea împotriva vulnerabilităților pentru sute de aplicații și sisteme de operare inclusiv pentru sisteme care nu mai au suport valabil sau sunt învechite;
- Operațiuni optimizate prin integrarea de soluții de provizionare în medii virtuale și soluții de tip SIEM;
- Capabilități anti-malware și IP reputation, inspecție fișiere log și monitorizarea integrității fișierelor;
- Capabilități de monitorizare a evenimentelor, assesment al vulnerabilităților și suport pentru automatizare flux;
- Suport pentru scalare și suport atât pentru arhitectura non-intruziva (fără agenți) cât și pentru arhitectura bazată pe agenți.

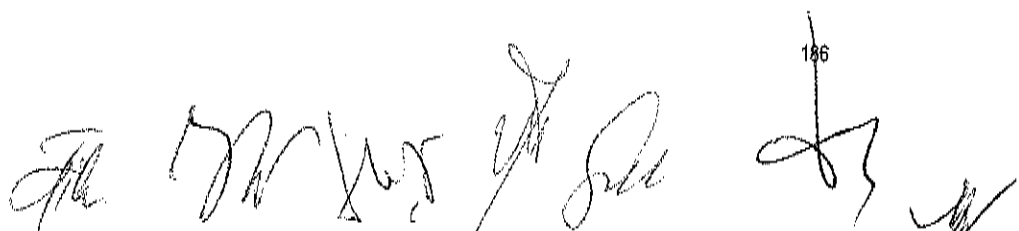
3.5.4.3.18 Componenta protecție endpoints

Cerinte:

Rolul acestei componente este de a oferi securitate stațiilor de lucru aferente infrastructurii IT din cadrul ONRC cu un modul centralizat de control astfel încât toate incidentele de securitate să fie accesibile unitar printr-o singură interfață. Componenta va fi dimensionată pentru 2000 de endpoints. Funcționalitățile principale pe care trebuie să le ofere componenta de protecție endpoints sunt următoarele:

- Protecție multiplă prin încorporarea de tehnologii si functionalitati variate: antivirus, device control, firewall, IPS, criptare pe statia si pe mail, DLP la nivel de statie sau mail, virtual patching sau inspectie SSL pentru trafic WEB;
- Protecție extinsa pentru dispozitive mobile (smartphones, tablete) si stick-uri USB sau hard-diskuri portabile;

186



- Inventarierea aplicațiilor pe dispozitiv și controlarea acestora, posibilitatea de a permite instalarea unora și blocarea altora. Posibilitate de instalare sau rula exclusiv aplicațiile permise de către politica IT;
- Criptarea datelor la nivel de disc sau fișiere prin integrare cu Windows Bitlocker sau prin metode proprii de criptare;
- Protecție împotriva spam-ului sau a atacurilor cu malware la nivelul componentei de e-mail;
- Protecție la navigarea de web prin implementarea unui proxy ce trebuie să ofere funcționalități precum: filtrare conținut, categorizare URL-uri, antimalware, control aplicații la nivel web, inspecție trafic SSL, modul DLP pentru web;
- Protecție pentru aplicațiile din suita Office;
- Capabilități de testare independentă, analiza comportamentală și „machine learning” în faza de execuție;
- Capabilități tip „application control”, „exploit prevention”, „web reputation” și „browser exploit protection”;

3.5.4.3.19 Componenta de tip terminale self-service

Terminalele de tip self-service (kiosk) sunt folosite ca alternativă la serviciile furnizate prin ghișeau tradițional solicitanților care nu doresc sau nu pot, din diferite motive, să utilizeze serviciile electronice oferite prin intermediul Portalului. În acest sens, se va implementa în sediile ORCT și respectiv la sediul ONRC o soluție bazată pe terminale de tip self-service, cu software-ul aferent și care vor putea fi utilizate de persoanele interesate pentru inițierea unor cereri de servicii sau pentru ridicarea de documente inclusiv în afara orelor de program cu publicul.

Componenta implementată prin terminale de tip self-service va permite cetățenilor să obțină informații personalizate, să completeze formulare electronice, să scaneze documente, să efectueze plăți și să ridice documente tipărite, emise din sistemele interne ale ONRC, fără a fi asistați de un funcționar.

Software-ul de aplicație utilizat de această componentă va fi integrat în platforma de servicii electronice, oferind utilizatorilor o experiență de utilizare unitară, în sensul similarității modalității de accesare a unui serviciu electronic din Portal sau de la echipamentul self-service. Serviciile electronice implementate prin terminalele self-service vor fi în general cele care nu necesită introducerea unei cantități mari de informații de către solicitant, astfel încât deservirea solicitanților să se poată face rapid, iar terminalul self-service să fie într-adevăr o alternativă mai rapidă la serviciile oferite prin ghișee. Astfel, va fi posibilă tipărirea de formulare tipizate, studierea procedurilor aferente unui anumit tip de solicitare, completarea de cereri, căutarea disponibilității sau rezervarea de denumire, căutarea informațiilor despre o firmă, eliberarea de certificate constatatoare sau de copii ale unor documente asociate unei firme, în baza unei cereri prealabile înregistrate fie de la terminalul self-service, fie din portal și după ce s-a primit prin email sau prin portal confirmarea faptului că respectivul document este disponibil.

Componenta self-service va fi complet integrată în soluția informatică de servicii electronice, în sensul în care un demers inițiat din soluția self-service va putea fi finalizat în soluția portal, de exemplu prin trimiterea de documente scanate suplimentare unei anumite cereri, sau prin efectuarea unei plăți online. De asemenea,

187

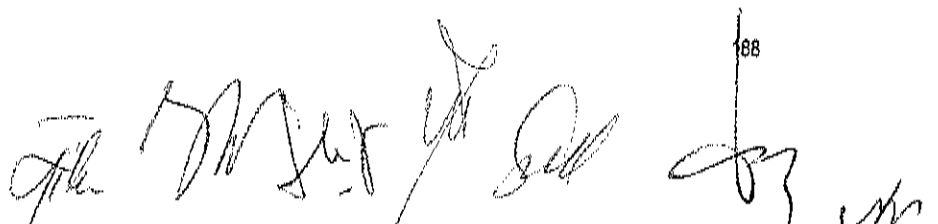
un demers inițiat în Portal se va putea finaliza cu eliberarea unui document tipărit de către subsistemul self-service.

Distribuția terminalelor de tip self-service la nivelul locațiilor Beneficiarului este următoarea:

Tip locație	Cantitate
ONRC - (1 sediul central x 2 bucăți)	2
ORCT București (1 locație x 4 bucăți)	4
ORCT Mare - peste 40.000 operațiuni pe an (9 locații x 2 bucăți)	18
ORCT Mediu - între 20.001 - 40.000 operațiuni pe an (14 locații x 1 bucată)	14
ORCT Mic - până în 20.000 operațiuni pe an (18 locații x 1 bucată)	18
TOTAL (terminale)	56

De asemenea, componenta de tip terminal self-service trebuie să respecte următoarele cerințe:

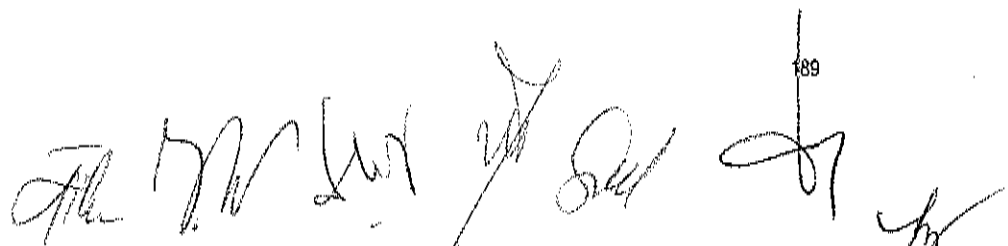
- Terminalul interactiv va integra componentele hardware într-o carcasă robustă, cu dimensiuni maxime: 170 cm înălțime, 100 cm lățime, 100 cm adâncime, confecționată din materiale metalice sau cu caracteristici similare de durabilitate;
- Terminalul va dispune de finisaje exterioare de calitate, cu finisaje corespunzătoare amplasării într-un loc public (inclusiv din punctul de vedere al protecției la lovire/tăiere);
- Terminalul va dispune de protecție electrică pentru prevenirea riscului de electrocutare a utilizatorului;
- Terminalul va fi amplasat în sediile/spațiile de lucru cu publicul ale ORCT/ONRC, eventual în zone „tampon” unde accesul se va putea face și în afara orelor de program la ghișeu, și va trebui să poată funcționa în intervalul de temperatură 0 – 40 grade Celsius și condiții de umiditate relativă de 0-95%;
- Terminalul va fi alimentat de la rețeaua electrică și va avea încorporată o sursă de alimentare neîntreruptibilă care să permită funcționarea cel puțin 10 minute în lipsa alimentării, înainte de a da comanda de shutdown automat;
- Terminalul va fi conectat prin cablu Ethernet la rețeaua locală de date a ORCT/ONRC;
- Terminalul va încorpora următoarele periferice:
 - Touchscreen 19”;
 - Tastatură alfanumerică metalică;
 - Dispozitiv de tip mouse pad, track point sau track ball;
 - Signature pad;
 - Scanner de documente A4;
 - Scanner pentru cărțile de identitate naționale;
 - Scanner pentru coduri de bare (pentru recunoașterea codului unei cereri anterioare);



188

- Imprimantă format A4 pentru documente;
- Modul de cititor de carduri bancare pentru plăți cu cardul;
- Perifericele vor fi expuse pe panoul frontal al terminalului, pentru a putea fi ușor accesibile utilizatorului;
- Utilizatorul nu va avea acces direct de manipulare la modulele de imprimare și scanare, introducerea și respectiv preluarea foilor de hârtie scanate sau tipărite realizându-se numai prin fante realizate în carcasa echipamentului, dedicate acestui scop;
- Terminalul va permite scanarea documentelor în format A4, color, simultan pe ambele fețe;
- După scanarea fiecărei pagini, utilizatorul va putea vizualiza și valida imaginea documentului scanat;
- După scanare, documentele vor putea fi fie returnate utilizatorului, fie stocate în interiorul terminalului;
- După preluare, toate documentele aferente unei sesiuni de utilizare a unui utilizator vor fi automat capsate împreună în interiorul terminalului;
- Pentru a facilita identificarea și arhivarea lor ulterioară, fiecărui set de documente preluate de la utilizator i se va adăuga, înainte de capsarea în interiorul terminalului, o pagină de gardă, generată automat de terminal, pe care vor fi imprimate informațiile necesare identificării ulterioare a cererii;
- Echipamentul va permite capsarea automată în interiorul echipamentului a cel puțin 15 coli de hârtie A4 pentru un calup de hârtii;
- Terminalul va dispune de senzori de monitorizare a capacității containerului de documente stocate, pentru a permite alertarea personalului de deservire în cazul în care este necesară golirea acestuia;
- În cazul în care utilizatorul întrerupe sesiunea de lucru fără a o finaliza, atunci terminalul îi va returna toate documentele depozitate până în acel moment;
- La finalizarea scanării, terminalul va putea tipări un document de confirmare, conținând numărul de pagini scanate, precum și alte informații introduse în prealabil de către utilizator de la ecranul terminalului;
- Terminalul va permite generarea și eliberarea de documente format A4, imprimate din sistemul intern de management al documentelor/cererilor;
- În scopul asigurării confidențialității informațiilor din documentele eliberate din terminal, mecanismul de distribuție a documentelor tipărite de către terminal va dispune de un sistem de retragere înapoi în terminal a paginilor tipărite în cazul în care utilizatorul nu le ridică într-un interval de timp predefinit;
- Terminalul va dispune de o cameră web și de un receptor telefonic ce vor permite utilizatorului să contacteze un funcționar în vederea acordării de suport pe parcursul utilizării terminalului;
- Se va avea în vedere posibilitatea dotării terminalului cu un subsistem de ștampilare automată a documentelor emise, astfel încât acestea să poată fi utilizate în mod similar documentelor elaborate și semnate/ștampilate olograf/manual;

189



- Utilizarea unui serviciu al terminalului va presupune parcurgerea de către utilizator a unei succesiuni de activități asistate de aplicația care va rula pe terminal, activități care vor putea include:
 - Prezentarea unor ecrane de informare;
 - Identificarea solicitantului prin scanarea cărții de identitate și preluarea automată a datelor de identificare necesare pentru pre-completarea formularelor electronice;
 - Completarea unor formulare, inclusiv cu preluarea automată a informațiilor scanate de pe cartea de identitate;
 - Scanarea unor documente ale utilizatorului;
 - Scanarea unui cod de bare de pe un document al utilizatorului;
 - Preluarea semnăturii olografe a utilizatorului prin intermediul ecranului touch-screen;
 - Efectuarea unor plăți cu cardul;
 - Imprimarea și eliberarea unui document justificativ sau a unui document eliberat din sistemul informatic al ONRC, în cazul furnizărilor de informații (de exemplu).

Terminalul va fi livrat cu o soluție de monitorizare care să transmită în timp real într-un sistem central cu interfața de administrare accesibilă via web-browser, statusul terminalului la nivel de componentă funcțională și la nivel de aplicație client.

Solicitățile de servicii realizate prin intermediul terminalelor self-service vor fi preluate și prelucrate de funcționari în componenta back-end a portalului de servicii electronice, în mod similar cu solicitările inițiate prin intermediul celorlalte canale disponibile.

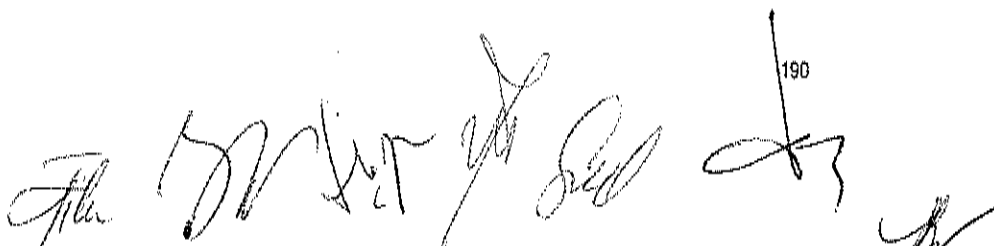
3.5.4.3.20 Componenta de automatizare a lucrului la ghișee

Această componentă are rolul de a îmbunătăți lucrul la ghișeu prin implementarea de automatizări în zona identificării solicitanților, de îmbunătățire a modului în care se preiau solicitările la ghișeu precum și a asigura preluarea cererilor fizice cât mai rapid în sistemul informatic prin digitalizarea acestora și transmiterea ulterioară pe flux. Totodată, aceste automatizări au rolul și de a reduce timpii de așteptare și de procesare la ghișeu, atunci când solicitanții nu au posibilitatea de a utiliza serviciile online prin intermediul portalului.

Pentru identificarea solicitanților se va utiliza o soluție hardware-software ce va permite extragerea informațiilor de interes conținute în cardul de identitate al solicitantului în momentul în care acesta se prezintă la ghișeu. Cardul de identitate se va scana utilizând echipamente specializate de scanare, iar informațiile de interes se vor extrage utilizând componente software de captură specifice, ce vor permite ulterior transmiterea informațiilor colectate către operatorul de la ghișeu pentru inițierea cererii, dar și ulterior către sistemul informatic.

Fiecare ghișeu ORCT/ONRC va avea în dotare un echipament de scanare acte de identitate conectat la stația de lucru a operatorului. Utilizând aplicația de scanare și extragere date din cardul de identitate al

190



solicitantului, operatorul de la ghișeu va putea iniția rapid cererea, minimizând totodată și erorile ce pot apărea atunci când datele de identificare se introduc manual.

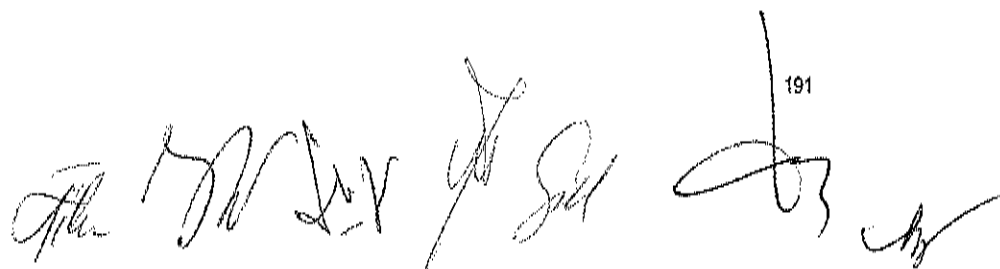
Distribuția echipamentelor de scanare acte de identitate la nivelul locațiilor Beneficiarului este următoarea (se are în vedere dotarea cu câte un echipament per ghișeu ORCT/ONRC):

Tip locație	Cantitate
ONRC (1 locație x 12 ghișee)	12
ORCT București (1 locație x 38 ghișee)	38
ORCT Mare - peste 40.000 operațiuni pe an (9 locații x 14 ghișee)	126
ORCT Mediu - între 20.001 - 40.000 operațiuni pe an (14 locații x 9 ghișee)	126
ORCT Mic - până în 20.000 operațiuni pe an (18 locații x 6 ghișee)	108
TOTAL (scannere)	410

Funcționalitățile minimale necesare pentru scanarea actelor de identitate, extragerea informațiilor de interes și utilizarea acestora în cadrul sistemului informatic integrat sunt următoarele:

- Să permită scanarea cardurilor de identitate emise în România și să ofere posibilitatea transmiterii imaginii scanate pentru adăugarea la documentele electronice constituite ulterior;
- Trebuie să aibă o interfață dedicată de scanare / indexare a documentelor de identitate de tip CI (Carte de Identitate) în care operatorul de la ghișeu să poată vizualiza și eventual corecta informațiile extrase din imaginea scanată;
- Aplicația trebuie să permită utilizarea de echipamente de scanare specializate pentru documente format A6;
- Trebuie să ofere extracția prin OCR a cel puțin următoarelor informații (în funcție de datele disponibile): nume, prenume, CNP, adresă, dată naștere, loc naștere, cetățenie, sex, emitentul, seria și numărul, dată eliberare și dată expirare;
- Aplicația trebuie să permită exportul imaginii scanate în formate standardizate JPEG sau PDF;
- Trebuie să permită validarea codului de siguranță MRZ (Machine Readable Zone) prezent la documentele de identitate de tip Carte de Identitate;
- Echipamentul de scanare trebuie să permită reglarea incrementală a rezoluției de scanare până la 600 dpi;
- Conectivitatea cu stația de lucru trebuie să fie pe USB 2.0;
- Echipamentul trebuie să de tip flatbed de format maxim A6, de dimensiuni și greutate redusă, astfel încât să nu ocupe spațiu semnificativ pe biroul operatorului și să poată fi manipulat ușor;

191



- Pentru a acomoda toate situațiile de lucru la ghișeu, alimentarea echipamentului trebuie să se poată realiza la priză (AC) sau direct prin conexiunea USB;
- Scanarea și extragerea informației trebuie să fie un proces rapid, astfel că viteza de scanare color a documentului de identitate trebuie să fie sub 10 secunde la o rezoluție de minim 300 dpi;
- Echipamentul trebuie să fie compatibil cu sisteme de operare Windows, inclusiv versiunea 10;
- Echipamentul trebuie să fie livrat împreună cu drivere ISIS / TWAIN sau să aibă API;

Pentru îmbunătățirea modului în care se preiau solicitările de la ghișeu se are în vedere implementarea unei soluții hardware-software care să permită pe de o parte realizarea de programări online în cadrul portalului public precum și programarea la ghișeu direct în locația ORCT/ONRC.

Pentru programările din portal se are în vedere implementarea unei interfețe în care se poate efectua o programare la sediul ORCT de care aparține solicitantul, portalul generând automat un bon de ordine astfel încât solicitantul să obțină data și ora, precum și codul asociat respective programări - acest bon de ordine electronic poate fi tipărit pentru utilizarea ulterioară. La nivel de ORCT/ONRC va exista ghișeu dedicat procesării programărilor realizate prin intermediul portalului online, complet separat de celelalte ghișee existente.

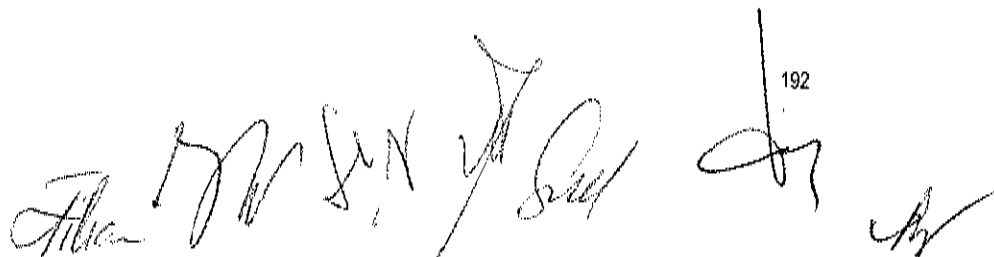
Pentru programările în locația ORCT/ONRC se are în vedere o soluție de tip "queue management" capabilă pe de o parte să poată oferi suport solicitanților în vederea obținerii unui bon de ordine personalizat utilizând un dispozitiv de ticketing de tip self-service și pe de altă parte capabilă să afișeze ordinea bonurilor de ordine pe un tablou grafic centralizat precum și bonul de ordine aflat în procesare la nivel de ghișeu, la fel utilizând un tablou grafic.

Soluția de tip "queue management" va fi dimensionată ținând cont de numărul de ghișee la nivel de ORCT/ONRC:

Tip locație	Număr locații	Total ghișee
ONRC (12 ghișee)	1	12
ORCT București (38 ghișee)	1	38
ORCT Mare - peste 40.000 operațiuni pe an (14 ghișee per locație)	9	126
ORCT Mediu - între 20.001 - 40.000 operațiuni pe an (9 ghișee per locație)	14	126
ORCT Mic - până în 20.000 operațiuni pe an (6 ghișee per locație)	18	108
TOTAL (ghișee)		410

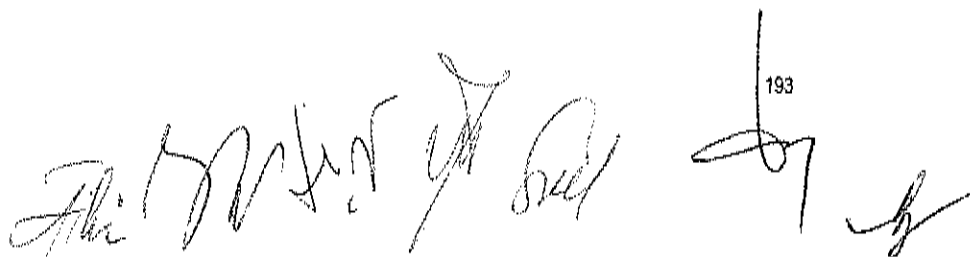
Funcționalitățile minimale necesare pentru automatizarea și eficientizarea preluării solicitărilor la ghișeu sunt următoarele:

192



- Componenta trebuie să includă minimal următoarele module hardware la nivel de locație:
 - Terminal self-service de emisie tichete care să cuprindă ecran de tip touchscreen, imprimantă termică, PC încorporat, UPS;
 - Afișoare centrale cu led-uri: 1 x afișor cumulativ central cu 3 linii, 1 x afișor cumulativ secundar cu 6 linii, 8 x afișor ghișeu cu o linie;
 - TV LCD pentru afișare coadă clienți și materiale publicitare;
 - Unitate redare conținut video;
- Va permite ca, la sosire, clienții să intre într-o coadă de așteptare, corespunzător nevoilor lor. Soluția trebuie să poată segmenta clienții în cozi de așteptare diferite (corespunzătoare diverselor tipuri de ghișee, conform segmentării serviciilor oferite clienților de către Beneficiar), în funcție de nevoile lor și nu plasarea tuturor clienților într-o coadă unică de așteptare. Segmentarea va permite alegerea personalului cu competența cea mai potrivită, care să răspundă cel mai bine nevoilor fiecărui client;
- Clienții care solicită servicii complexe trebuie să poată fi gestionați separat, pentru a reduce riscul de "blocare" a altor clienți, cu un impact negativ asupra experienței lor în relația cu ONRC/ORCT;
- Va exista și posibilitatea de solicitare și primire de număr de ordine online (rezervare online), prin intermediul componentei portal; va exista posibilitatea de transmitere SMS-uri către solicitanți, de confirmare sau avertizare privind ora la care solicitantul este așteptat la ghișeu; solicitantul va avea la rândul său posibilitatea de confirmare, anulare sau solicitare de reprogramare la nevoie;
- După ce un solicitant a fost servit, funcționarul care a prestat serviciul respectiv închide operațiunea, iar datele relevante sunt înregistrate;
- Pentru emiterea de tichete de ordine, componenta trebuie să ofere o interfață în limba. În momentul în care solicitantul face selecția, înainte de a i se elibera tichetul de ordine se va afișa pe monitorul terminalului atât un timp minim de așteptare până când va fi preluat de funcționar cât și numărul solicitanților în așteptare la serviciul ales. Astfel, solicitantul decide dacă să rămână și să aștepte în funcție de timpul pe care îl are la dispoziție;
- Se vor putea afișa pe ecranul terminalului listele cu documente necesare pentru rezolvarea operațiunilor dorite în momentul solicitării operațiunii;
- Pe tichet se va tipări numărul de ordine, denumire operațiune, ora la care a fost tipărit, locație și totodată trebuie să existe posibilitatea de a se tipări și alte informații precum: nume solicitant, alte mesaje și servicii;
- Pentru fiecare ghișeu în parte (sau tip de ghișeu) se va stabili/limita care operațiuni sau grupuri de operațiuni pot fi efectuate la ghișeul respectiv; solicitantul poate fi redirecționat către un alt ghișeu și va putea fi stabilit ca prioritar tratarea redirecționării făcute;
- Chemarea clienților se va face cu ajutorul ecranului LCD, acesta va permite afișarea ultimelor tichete chemate, afișarea numărului tichetului nou distinct, alertă la o nouă chemare. Pe lângă afișajul LCD vor mai exista afișoare cumulative: unul cu 3 linii și unul secundar de 6 linii care se vor monta pe geam astfel încât să poată fi văzute de către solicitanții care au ieșit afară;

193



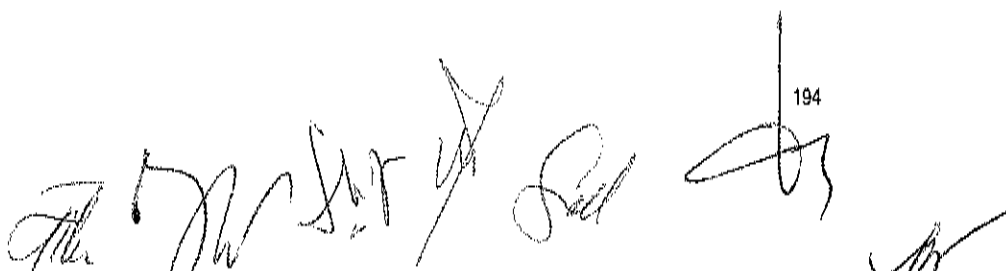
- Pentru programările online utilizând portalul - solicitanții vor introduce numele și adresa de email după care tipul de solicitant (conform segmentării puse la dispoziție de Beneficiar), motivul programării precum și locația. Structura operațiunilor solicitate (și programate) afișată în portal va fi o replică a structurii existente în terminalul de eliberat tichete existent în locație. În funcție de tipul operațiunii se vor putea afișa mesaje de comunicare comercială. Funcție de tipul de solicitant se va putea prioritiza rezervarea;
- Solicitantul va primi detaliile rezervării pe adresa de email comunicată, împreună cu numărul tichetului de ordine. Numărul tichetului de ordine va trebui să permită identificarea rezervării când se va afișa la sediul Beneficiarului;
- Soluția trebuie să permită reprogramarea/anularea/invalidarea rezervărilor online;
- În ziua respectivă, la momentul stabilit de solicitant, se va afișa la panou numărul de ordine dat de înregistrarea online. Dacă solicitantul nu se află în sediu, se preia un alt client și se reafișează în momentul în care se eliberează primul funcționar. Acest lucru se poate face de un număr de ori stabilit în soluție după care se consideră „absent”. Se va comunica la eliberarea tichetului online ca rezervarea are o perioadă de valabilitate;
- Soluția nu va permite realizarea de rezervări pentru ziua în curs și va putea limita numărul de rezervări pe care le poate face un client în decursul unei zile.

În vederea asigurării preluării cererilor fizice cât mai rapid în sistemul informatic, prin digitalizarea acestora și transmiterea ulterioară pe flux, se are în vedere implementarea unei soluții complete hardware-software care să permită organizarea cererilor fizice, transmiterea acestora pentru scanare, indexarea informațiilor cheie de referință pentru cerere și transmiterea imaginilor digitalizate către sistemul informatic integrat în vederea utilizării pe fluxurile de business. În acest sens au fost identificate următoarele componente necesare implementării soluției de digitalizare cereri fizice:

- imprimante de birou pentru tipărire etichete autocolante cu cod de bare - fiecare ghișeu care va prelua cereri fizice va fi dotat cu câte o astfel de imprimantă pentru tipărirea codului de bare ce identifică cererea fizică ce urmează a fi preluată - codul de bare este generat automat de către sistemul informatic;
- echipamente de scanare capabile să scaneze cererile fizice în vederea digitalizării acestora,
- aplicație de captură distribuită capabilă să gestioneze echipamentele de scanare, să preia imaginea scanată, să realizeze extragerea de indecși necesari identificării cererii fizice și să transmită documentele digitalizate către sistemul informatic central;
- echipament de stocare de tip network attached storage (NAS) la nivel local capabil să stocheze cererile digitalizate precum și alte documente de suport și să le gestioneze ca suport de rezervă (în cazul în care există probleme cu cererea transmisă în sistemul informatic central, cererea să poată fi accesată local și retransmisă ulterior către centru). Cererile vor fi păstrate în copie locală până când acestea vor fi arhivate la nivelul SAE.

Imprimantele de birou pentru tipărire etichete autocolante cu coduri de bare vor fi alocate câte una per ghișeu ORCT/ONRC:

194



Tip locație	Cantitate
ONRC (1 locație x 12 ghișee)	12
ORCT București (1 locație x 38 ghișee)	38
ORCT Mare - peste 40.000 operațiuni pe an (9 locații x 14 ghișee)	126
ORCT Mediu - între 20.001 - 40.000 operațiuni pe an (14 locații x 9 ghișee)	126
ORCT Mic - până în 20.000 operațiuni pe an (18 locații x 6 ghișee)	108
TOTAL (imprimante)	410

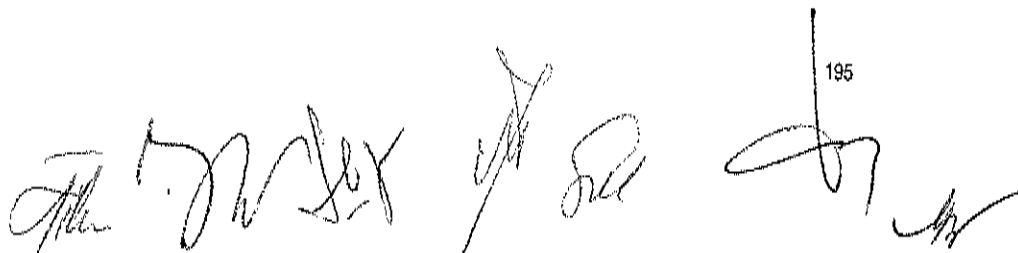
Cerințele minime pentru imprimantele de birou pentru tipărire etichete autocolante sunt următoarele:

- Capabilitate de imprimare prin transfer termic și direct termic;
- Rezoluție de tipărire de minim 200 dpi;
- Viteza de imprimare de minim 200 mm/s;
- Dimensiuni compacte, echipamentul trebuie să poată fi amplasat pe biroul operatorului (maxim 30x40cm);
- Conectivitate prin USB sau Ethernet;
- Afișaj de tip LCD sau LED;
- Posibilitate de integrare din aplicație a imprimantei utilizând o interfață sau un limbaj de programare pus la dispoziție de către producător;
- Calibrare rapidă a echipamentului după adăugarea rolei, minimizarea intervenției operatorului uman în acest proces;
- Detecția automată a rolei de etichete, posibilitate de tăiere automată a etichetelor;
- Coduri de bare suportate: 1D, 2D;
- Fiecare imprimantă trebuie să fie furnizată cu 5 role de etichete autoadezive de minim 50x25 mm, rola având o capacitate de minim 2500 etichete per rolă;

Echipamentele de scanare sunt de două tipuri (separație în funcție de capacitatea de procesare și viteza de scanare) și vor fi distribuite la nivel ORCT, după cum urmează:

Tip locație	Scanner tip 1	Scanner tip 2
ONRC (1 locație x 4 scannere)	-	4
ORCT București (1 locație x 8 scannere)	-	8
ORCT Mare - peste 40.000 operațiuni pe an (9 locații x 4 scannere)	-	36

195



ORCT Mediu - între 20.001 - 40.000 operațiuni pe an (14 locații x 2 scannere)	28	-
ORCT Mic - până în 20.000 operațiuni pe an (18 locații x 2 scannere)	36	-
TOTAL (scannere)	64	48

Cerințele minime pentru echipamentele de scanare de tip 1 sunt următoarele:

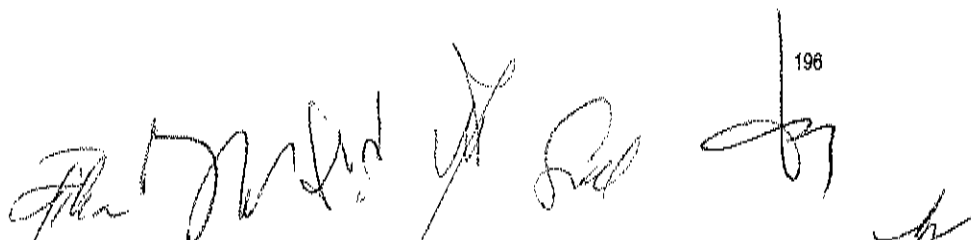
- Scanner de producție tip A3;
- Capacitate de scanare de 80 de pagini A4 per minut;
- Alimentator automat de documente cu o capacitate de 100 de coli;
- Volum zilnic de procesare de minim 10.000 pagini;
- Posibilitate de scanare simplex sau duplex (față-verso);
- Rezoluție optică 600 dpi;
- Conectivitate la stația de lucru prin USB ;
- Funcții integrate de procesare: îndreptare imagine, detecție automată dimensiune pagină, detecție pagină albă, eliminare borduri, eliminare găuri de la perforare, îmbunătățire contrast;
- Detecția alimentării duble cu hârtie;
- Conectivitate cu stația de lucru utilizând drivere standard de tip ISIS / TWAIN;

Cerințele minime pentru echipamentele de scanare de tip 2 sunt următoarele:

- Scanner de producție tip A3;
- Capacitate de scanare de 100 de pagini A4 per minut;
- Alimentator automat de documente cu o capacitate de 300 de coli;
- Volum zilnic de procesare de minim 25.000 pagini;
- Posibilitate de scanare simplex sau duplex (față-verso);
- Rezoluție optică 600 dpi;
- Conectivitate la stația de lucru prin USB ;
- Funcții integrate de procesare: îndreptare imagine, detecție automată dimensiune pagină, detecție pagină albă, eliminare borduri, eliminare găuri de la perforare, îmbunătățire contrast;
- Detecția alimentării duble cu hârtie;
- Conectivitate cu stația de lucru utilizând drivere standard de tip ISIS / TWAIN;

Aplicația de captură distribuită / digitizare va integra echipamentele de scanare la nivelul sistemului și va putea gestiona întreg procesul de captură a documentelor, inclusiv extragerea informației necesare (indecși) identificării cererii fizice și transmiterea (export) documentelor electronice către sistemul informatic central în

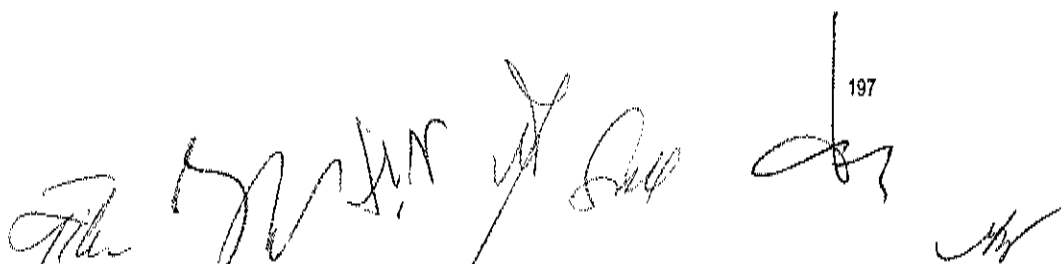
196



vederea procesării și ulterior al arhivării acestuia în cadrul SAE. Aplicația va fi licențiată să acopere întreaga soluție de captură (scannere), respectiv stațiile de scanare conectate la echipamentele de scanare. Din punct de vedere tehnic și funcțional, aplicația trebuie să respecte următoarele cerințe:

- Aplicația trebuie să asigure funcții standard precum: scanare document, import document, procesare manuală sau automată de imagine, completare atribute (indecși) document, validare informații completate ca atribute (indecși), export pe disc, în baze de date sau în alte sisteme prin integrare de tip web-service;
- Aplicația de captură distribuită nu trebuie să impună limitări în ceea ce privește numărul de pagini sau de documente procesate;
- Trebuie să ofere mecanisme de detecție și extragere a codurilor de bare (BCR) de tip 1D și 2D;
- Trebuie să permită separarea automată a documentelor (scanarea în loturi) având la bază separatori de documente de tip patch-codes;
- Trebuie să completeze automat indecșii asociați având la dispoziție informațiile extrase din codurile de bare;
- Trebuie să permită și adăugarea manuală de imagini în aplicație, în cazul în care acestea au fost scanate pe o altă stație de lucru;
- Aplicația trebuie să permită gestionarea echipamentului de scanare – conectare la acesta utilizând driverele puse la dispoziție de către producătorul echipamentului precum și configurarea profilului de scanare;
- La nivelul profilului de scanare trebuie să permită configurări la nivelul rezoluției, a modului de scanare (alb-negru sau color), a dimensiunii paginii, în funcție de facilitățile oferite de echipamentul de scanare;
- Va permite scanarea în loturi de documente folosind separatori de documente pentru separarea automată a documentelor din cadrul unui lot. Separatorii de documente (patch-codes) trebuie să fie eliminați automat din imaginile scanate, după ce aceștia au fost utilizați;
- Trebuie să permită exportul imaginilor în formate multiple standardizate - minim JPEG și PDF;
- Trebuie să permită re-scanarea unei/unor imagini, atunci când operatorul consideră necesar acest lucru;
- Atributele asociate unui document trebuie să poată fi exportate în formă structurată tip XML;

În vederea stocării cererilor în formatul electronic rezultat în urma procesului de captură, vor fi prevăzute în proiect echipamente de stocare la nivel local ORCT/ONRC astfel încât acestea să poată stoca tot conținutul în formă electronică pentru ca acesta să poată fi exportat ulterior către sistemul informatic integrat. Totodată, rolul acestor echipamente este de a păstra informațiile pentru o perioadă determinată de timp – uzual până la arhivarea cererilor în SAE (caz în care documentele electronice vor fi șterse la nivel local), dar și pentru a stoca o serie de documente în formă electronică ce pot fi preluate de pe alte canale decât scanare (ex: email, fax).



197

Aceste echipamente de stocare locală sunt de două tipuri (separație în funcție de capacitatea de stocare) și sunt distribuite la nivel ORCT/ONRC, după cum urmează:

Tip locație	NAS tip 1	NAS tip 2
ONRC (1 locație)	1	-
ORCT București (1 locație)	1	-
ORCT Mare - peste 40.000 operațiuni pe an (9 locații)	9	-
ORCT Mediu - între 20.001 - 40.000 operațiuni pe an (14 locații)	-	14
ORCT Mic - până în 20.000 operațiuni pe an (18 locații)	-	18
TOTAL (echipamente stocare locală)	11	32

Cerinte:

Cerințele minime pentru echipamentele de stocare locală (NAS) de tip 1 sunt următoarele:

- Suport pentru sisteme de operare optimizate pentru stocare de tip NAS;
- Suport pentru protocoale: CIFS, NFS, FTP, SMB;
- Dimensiune în rack: minim 2U;
- Procesare: Două procesoare Xeon 10-core, min 2.2 Ghz, cache min. 13MB L3;
- Memorie: 64 GB;
- Capacitate: 12 discuri 4TB SAS în configurație RAID 6 și 2 discuri 600 GB SAS;
- Conectivitate: 2 porturi 10GbE și 2 porturi 1 GbE;
- Răcire prin ventilatoare redundante;
- Facilități de protecție a datelor stocate;
- Două surse de alimentare AC 220V redundante.

Cerinte:

Cerințele minime pentru echipamentele de stocare locală (NAS) de tip 2 sunt următoarele:

- Suport pentru sisteme de operare optimizate pentru stocare de tip NAS;
- Suport pentru protocoale: CIFS, NFS, FTP, SMB;
- Dimensiune în rack: minim 2U;
- Procesare: Un procesor Xeon 6-core, min 1.7 Ghz, cache min. 8MB L3;
- Memorie: 16 GB;
- Capacitate: 12 discuri 1TB SAS în configurație RAID 6 și 2 discuri 600 GB SAS;
- Conectivitate: 2 porturi 10GbE și 2 porturi 1 GbE;

198

- Răcire prin ventilatoare redundante;
- Facilități de protecție a datelor stocate;
- Două surse de alimentare AC 220V redundante.

3.5.4.3.21 Componenta de informare și suport tip call-center

Soluția de informare și suport de tip call-center va asigura procesarea solicitărilor venite din partea clienților prin multiple canale de comunicație: telefon, email, chat, fax, social media și altele.

Componenta solicitată va fi implementată într-o arhitectură virtualizată, redundată, extensibilă, cu posibilități multiple de interconectare cu sistemele de business. Vor fi oferite funcționalități avansate de tip self-service prin care clienții vor putea să rezolve anumite tipuri de solicitări fără intervenția unui agent.

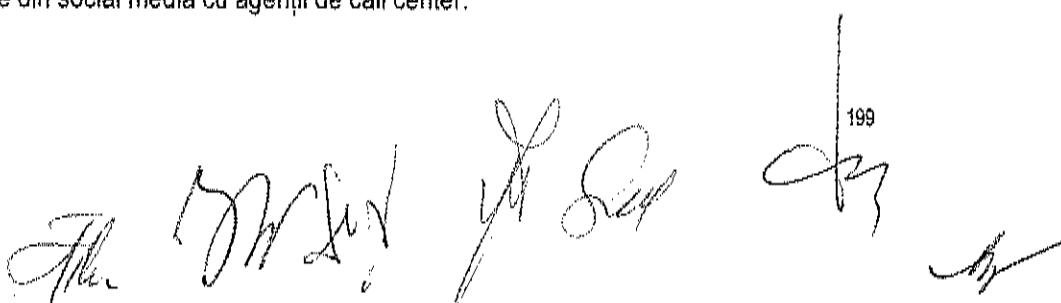
De asemenea, componenta va oferi funcții avansate de monitorizare și raportare pentru urmărirea în timp real și istoric a parametrilor de funcționare. Soluția va fi dimensionată pentru un număr de 50 de operatori din partea Beneficiarului și nu trebuie să impună restricții geografice în ceea ce privește distribuția operatorilor la nivelul locațiilor.

Cerinte:

Componenta va pune la dispoziție toate modulele necesare pentru a oferi următoarele funcționalități:

- **Telefonie:** Pentru asigurarea comunicațiilor vocale, sistemul va oferi funcții de telefonie pentru agenți folosind softphones, precum și interconectarea cu providerii de telefonie folosind fluxuri E1 și trunchiuri SIP.
- **Automatic contact distribution (ACD):** Sistemul va asigura eșalonarea, rutarea și raportarea apelurilor sosite în contact center. Rutarea va fi programabilă pentru a permite alegerea celui mai liber agent care posedă calificările necesare.
- **Outbound:** Campaniile de outbound permit comunicarea proactivă cu clienții, pentru feedback sau comunicarea unor informații, prin apelarea automată a unor liste de contacte.
- **Interactive Voice Response (IVR):** Asigură tratarea automată a apelurilor vocale fără intervenția unui agent. Permite integrarea cu aplicații externe pentru a furniza informații interactive. Suportă adăugarea opțională de funcționalități de speech recognition și text to speech.
- **Email management:** Soluția va permite tratarea solicitărilor sosite prin e-mail, asigurând distribuția mesajelor către agenți, tracking-ul conversațiilor precum și generarea de rapoarte istorice și în timp real.
- **Chat:** Vor fi oferite capacități de interacțiune cu clienții folosind o interfață de chat web-based integrată în portalul pentru clienți, cu capacități complete de rutare și raportare.
- **Agent/Supervisor Desktop/CTI:** Pentru tratarea apelurilor, agenții vor fi dotați cu o interfață desktop bazată pe tehnologii web, care să nu necesite instalarea de aplicații pe PC și să permită integrarea cu aplicații de business pentru furnizarea de informații contextuale în timp real.
- **Social media:** Sistemul va permite integrarea cu rețele sociale (Facebook/Twitter/Forums/Blogs), conectând interacțiunile din social media cu agenții de call center.

199



- **Reporting:** Pentru monitorizarea permanentă a activității call center-ului dar și a trend-urilor pe perioade mai lungi, sistemul va oferi funcționalități avansate de definire de rapoarte, dashboard-uri atât în timp real cât și istorice.
- **Recording:** Sistemul va asigura înregistrarea tuturor apelurilor vocale, precum și a ecranului agenților atunci când este cazul, precum și păstrarea lor pe o perioadă predefinită de timp.
- **Workforce Management (WFM):** Asigură managementul resurselor umane ale call center-ului, planificarea schimburilor, concediilor, etc

Descrierea modulelor principale funcționale ale componentei de informare și suport de tip call-center:

Telefonie

Modulul de telefonie asigură comunicațiile de voce pentru agenți și interconectarea cu PSTN. Soluția va fi de tip VoIP și va rula în medii virtualizate. Vor fi furnizate 50 de licențe de utilizatori tip SoftPhone, precum și căști USB adecvate pentru call center. Interconectarea cu providerii de telefonie va fi redundată, asigurând minim 60 de trunchiuri SIP și 2 interfețe ISDN PRA chiar în caz de defecțiune hardware.

Automatic contact distribution (ACD)

Modulul ACD va permite rutarea condițională a apelurilor în funcție de informații externe, inclusiv obținute din sisteme externe. Rutarea va fi bazată pe nivelul de competență al agentului în diferite domenii pentru a asigura alegerea celui mai potrivit agent pentru fiecare apel. De asemenea vor fi disponibile diverse niveluri de prioritate pentru clienți pe baza numărului de telefon sau diferitelor informații introduse de acesta. Vor fi oferite 50 de licențe pentru agenți/supervizori concurenți, supervizorii având posibilitatea de a prelua apeluri în situații de încărcare crescută.

Interactive Voice Response (IVR)

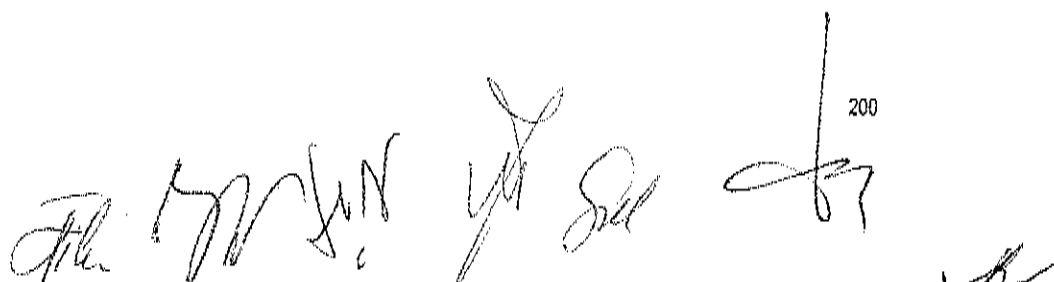
Modulul IVR permite implementarea de fluxuri de tip self-service în care clientul obține informațiile necesare fără a interacționa cu un agent. În acest scop, IVR-ul se va integra cu aplicații externe prin interfețe standard (REST) sau cu baze de date (ODBC, JDBC). Va fi disponibilă integrarea unor componente externe pentru funcționalități de tip Text to Speech (TTS) și Advanced Speech Recognition (ASR). Va fi disponibil un editor grafic pentru definirea scripturilor IVR. Se va furniza un număr minim de 100 porturi de IVR simultane.

Outbound

Modulul Outbound dialer va permite desfășurarea de campanii pentru informarea clienților sau obținerea de feedback. Campaniile vor putea fi definite atât cu agenți cât și pe bază de IVR și vor oferi dialing de tip preview, progressive și predictive.

Listele vor putea fi încărcate local sau trimise din aplicații externe printr-o interfață API standard (REST). Agenții vor putea fi dedicați pentru campaniile de outbound sau blended (inbound/outbound).

200



Email Management

Modulul va implementa funcționalități de esalonare al interacțiunilor primite prin email sau fax (folosind un gateway extern fax2email), permițând integrarea cu Exchange, Office365 sau Gmail. Va permite definirea mai multor cozi de email pe baza adresei de email. Interfața de tratare a email-urilor va fi integrată în agentul desktop permițând unui agent să trateze simultan email-uri și apeluri vocale.

Chat

Modulul de chat va fi integrat cu portalul și va permite utilizatorilor acestuia interacțiunea cu agenții folosind un browser web. Agentul poate trata simultan mai multe sesiuni de chat și poate implica un alt agent/expert sau poate transfera chat-ul. Interfața de tratare a chat-ului va fi integrată în agentul desktop permițând unui agent să trateze simultan apeluri vocale și sesiuni de chat.

Agent/Supervizor desktop/CTI

Agenții și supervizorii vor fi echipați cu o interfață de lucru de tip Web extensibilă și programabilă care le va furniza toate informațiile necesare pentru tratarea apelurilor. În acest scop, aceasta va permite integrarea cu aplicațiile de business necesare folosind protocoale standard (HTTP, REST, XML). Configurația interfeței va putea fi definită diferit pentru fiecare tip de apel/coadă cu informațiile relevante. De asemenea, interfața va implementa funcțiile de CTI pentru controlul direct al aplicației softphone, eliminând nevoia ca agentul să utilizeze mai multe aplicații. La nivelul supervizorilor vor fi oferite informații detaliate despre starea agenților, starea cozilor, KPI-uri, etc.

Social Media

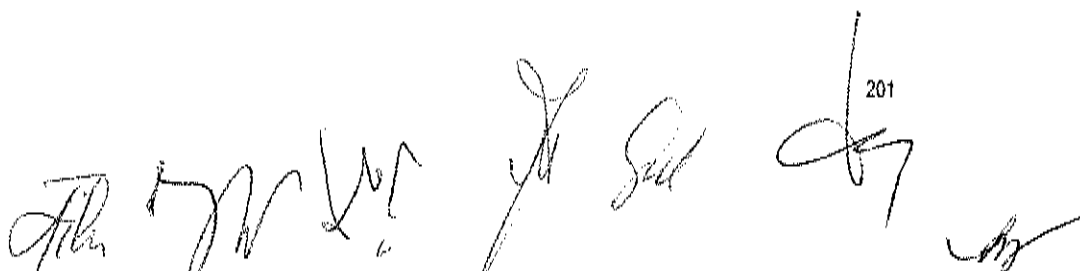
Modulul de social media va asigura monitorizarea rețelelor sociale pe baza unor reguli/filtre permițând generarea unor interacțiuni în call center atunci când utilizatorii social media doresc să interacționeze. Vor fi suportate pagini Facebook, Twitter, Forumuri, Blog-uri.

Reporting

Modulul va oferi funcționalități avansate de reporting, atât istorice cât și în timp real, permițând definirea ușoară de rapoarte personalizate și dashboard-uri, inclusiv combinate cu date din sisteme externe. Interfața va fi web-based fără a necesita instalarea de componente locale. Vor putea fi definite permalinks pentru accesul direct la anumite rapoarte.

Recording

Modulul va permite înregistrarea tuturor convorbirilor telefonice, iar la nevoie, pentru evaluarea performanței agenților, va fi posibilă inclusiv înregistrarea ecranului. Supervizorii și administratorii de sistem vor putea asculta înregistrările și crea rapoarte de evaluare a activității agenților. Va fi integrat atât cu sistemul de raportare cât și cu agent/supervizor desktop.



Handwritten signatures and initials at the bottom of the page, including a date stamp '201'.

Workforce Management (WFM)

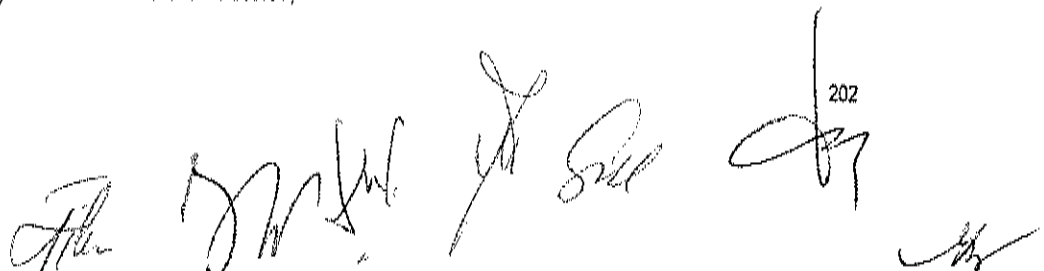
Modulul de workforce management administrează resursele umane din call center. Permite programarea schimburilor de lucru, a concediilor și pauzelor pentru agenți. Realizează forecast-uri pentru necesarul de resurse în viitor și măsoară nivelul de implicare al agenților.

3.5.4.3.22 Componenta de testare automată și de performanță

Această componentă are rolul de a asigura tot suportul necesar efectuării de teste automate și de performanță a aplicațiilor la nivelul întregului sistem informatic. Pentru a se asigura un nivel de calitate ridicat al sistemului integrat, **Autoritatea Contractantă va achiziționa printr-o procedură de achiziție publică distinctă atât licențele necesare cât și serviciile de implementare și testare** ce vor utiliza aceasta componentă achiziționată, ca parte a serviciilor prestate, urmând ca în perioada de mentenanță a sistemului, personalul Beneficiarului să preia toate livrabilele rezultate în urma activităților de testare (inclusiv script-uri) și să acopere testarea continuă a sistemului informatic. Se vor avea în vedere un număr de 3000 utilizatori virtuali pentru testare de performanță și minim 10 utilizatori concurenți pentru testare automată.

Această componentă trebuie să respecte următoarele cerințe:

- Funcționalitățile trebuie să fie disponibile standard la nivelul componentei oferite, fără a fi necesare dezvoltări suplimentare pentru acoperirea cerințelor;
- Permite folosirea unui limbaj de programare standard (Javascript, VBscript, Jscript, Python) pentru crearea de teste pe interfața utilizator sau îmbunătățirea înregistrărilor testelor existente;
- Permite convertirea facilă în script-uri a testelor înregistrate în interfața grafică utilizator;
- Dispune de un mediu integrat de testare;
- Permite rularea de teste de tip cross-browser;
- Permite rularea unui test automatizat pe mai multe editii și versiuni de browsere, suportând browserele majore existente pe piață;
- Permite automatizarea testării funcționale pentru multiple tehnologii desktop (de exemplu Windows / Java / .NET / Oracle Forms);
- Permite separarea datelor de comenzi de test și modificarea datelor de intrare pentru lărgirea ariei de testare;
- Conține o platformă de testare completă și integrată, atât pentru testarea desktop cât și pentru cea a aplicațiilor mobile și web.
- Oferă suport pentru cele mai recente tehnologii web, cel puțin pentru: HTML5, WebSocket și Oracle Forms;
- Permite, pentru crearea testelor, designul acestora fără a fi necesare scripturi;
- Oferă suport pentru programarea vizuală a testelor;



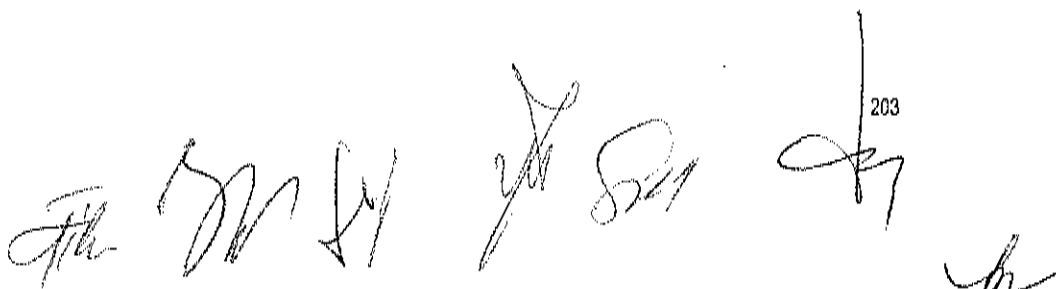
202

- Permite crearea de reguli pentru extragerea datelor variabile din pagini;
- Suporta cel puțin SSL, Kerberos, NTLM și autentificări de tip Basic, Digest sau folosind certificate client;
- Permite înregistrarea aplicațiilor mobile (cu browser de tip nativ, hibrid sau mobil) direct, de pe orice dispozitiv mobil;
- Permite adăugarea/eliminarea de utilizatori virtuali în timpul execuției testelor;
- Oferă suport pentru o gamă largă de produse software, incluzând însă nelimitându-se la sisteme de operare, servere de aplicații, servere web, baze de date;
- Permite monitorizarea fără agenți;
- Oferă suport pentru GIT;
- Oferă suport pentru testarea cel puțin a aplicațiilor .NET și Java;
- Permite rularea de teste de încărcare la nivelul API (SOAP, REST), la nivelul componentelor sau la nivelul microservicilor;
- Permite analizarea performanței sistemului după rularea unui test pe baza datelor colectate din straturile arhitecturale relevante;
- Permite rularea de rapoarte de analiză a performanței pe diferite nivele de detaliu (de tip sumar sau la nivel de tranzacție) și rapoarte pentru determinarea încadrării performanței într-un SLA predefinit;
- Permite localizarea, extragerea și înlocuirea valorilor dinamice din cadrul paginilor web precum id-ul de sesiune, authentication token, customer id, etc asigurând astfel acceptarea cererilor de către serverele web supuse testării;

Pentru urmărirea execuției aplicațiilor aflate în mediul de producție este necesară includerea unui modul specializat care să permită urmărirea directă sau prin agenți instalați la nivelul componentelor aplicative în vederea raportării rezultatelor și alertarea administratorilor cu privire la nivelul de performanță al sistemului. Modulul trebuie să includă următoarele funcționalități:

- Executarea de tranzacții în mod controlat, din locații multiple înainte sau după firewall pentru identificarea disponibilității și performanței aplicațiilor;
- Urmărirea performanței tranzacțiilor la nivel de aplicații în medii virtualizate pentru izolarea rapidă a problemelor de performanță prin diagnoza de tip „deep dive” care identifică unitățile de cod cu probleme de performanță cum ar fi metode ale obiectelor din cod sau statement-uri SQL;
- Posibilitatea de identificare și agregare tranzacții la nivel de utilizator, server sau baza de date;
- Monitorizarea end-to-end a fluxurilor tranzacțiilor la nivel de aplicații;
- Identificarea blocajelor în aplicații independente de mediul pe care sunt implementate;

203



- Identificarea in timp real a incidentelor pentru a permite echipei IT sa detecteze problemele inainte ca acestea sa afecteze utilizatorii finali;
- Posibilitatea de configurare de actiuni automate de remediere;
- Urmărirea executiei la nivel de aplicatii si tranzactii web (script-uri, URL), notificare echipa IT pe canale multiple (mail, SMS);
- Refolosirea script-urilor de testare de performanta pentru monitorizare aplicatiilor;

3.5.4.3.23 Componenta de testare de securitate

Această componentă are rolul de a asigura tot suportul necesar efectuării de teste de securitate la nivelul aplicațiilor dezvoltate în cadrul sistemului. Pentru a se asigura un nivel de calitate ridicat al sistemului integrat, **Autoritatea Contractanta va achiziționa printr-o procedura de achiziție publică distinctă atât licențele necesare cât și serviciile de implementare și testare ce vor utiliza aceasta componentă, ca parte a serviciilor prestate**, urmând ca în perioada de mentenanță a sistemului, personalul Beneficiarului să preia toate livrabilele rezultate în urma activităților de testare (inclusiv script-uri) și să acopere testarea continuă a sistemului informatic. Se va asigura un număr de 50 utilizatori pentru testare de securitate.

Componenta va asigura suport pentru măsurarea și îmbunătățirea calității aplicațiilor software realizate pe mai multe platforme și multiple limbaje de programare pe tot parcursul ciclului de dezvoltare, oferind analize privitoare la calitatea structurii și complexității, măsurarea și monitorizarea stării aplicației și productivitatea echipei de dezvoltare.

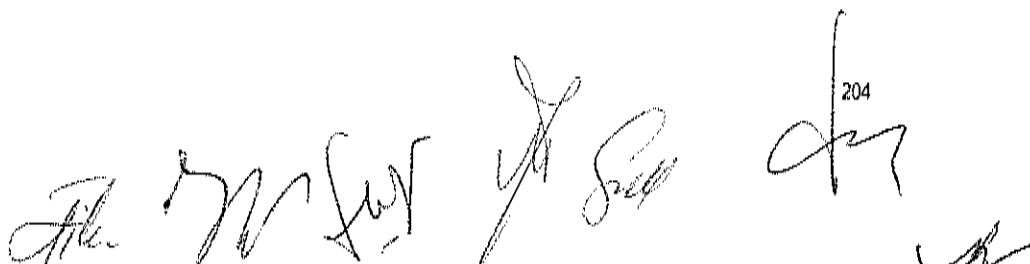
Componenta de testare de securitate va trebui sa utilizeze metrice multiple precum:

- Calitatea: robustețe, securitate, performanță, transferabilitate și adaptabilitate;
- Imaginea tehnologică și evoluția documentației, proiectării arhitecturale și a practicilor de programare;
- Identificarea vulnerabilităților critice;
- Identificarea celor mai riscante componente ale software-ului;
- Număr de reguli critice și obiecte modificate recent;
- Dimensionare tehnică și funcțională (funcții automate, linii de cod sursă, fișiere și artefacte);
- Estimarea efortului de întreținere;
- Compararea scorurilor aplicațiilor cu repere utilizate și standarde;

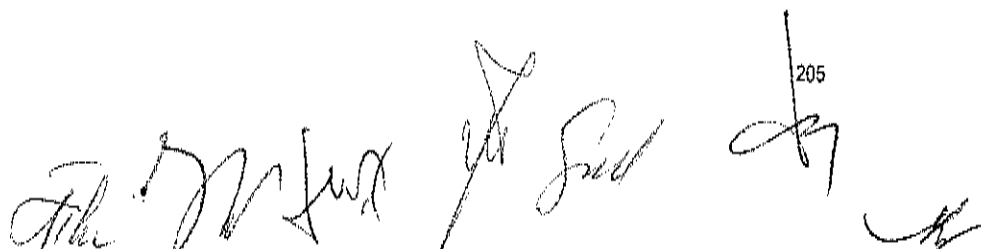
Totodată, componenta trebuie să permită și scanarea dinamică de securitate a aplicațiilor web, compuse din diferite tehnologii web:

- Furnizarea unei palete largi de teste de securitate dinamice și detectarea noilor tipuri de vulnerabilități;
- Gestionarea riscurilor de securitate a aplicațiilor prin monitorizarea tendințelor utilizând automatizarea și integrarea;
- Management-ul de conformitate referitoare la securitatea aplicațiilor web precum OWASP sau NIST;

204



- Integrarea analizei dinamice și la runtime pentru a găsi mai multe vulnerabilități și pentru a putea fi rezolvate mai repede;
- Utilizarea tehnicilor de "crawl" pentru a extinde acoperirea suprafeței de atac (directoare și pagini ascunse, autentificare OAUTH, parametri utilizați de backdoor-uri, încălcări de confidențialitate) și pentru a detecta noi tipuri de vulnerabilități care pot fi nedetectate de alte tehnologii de testare a securității;
- Rularea de politici personalizate adaptate la specificul aplicațiilor web;
- Controlul securității aplicațiilor prin scanări bazate pe roluri și administrarea rapoartelor;
- Gestionarea artefactelor și a descoperirilor de la scanări multiple;
- Reutilizarea șabloanelor de scanare și configurare pentru scanări repetate și consecvente;
- Protejarea informațiilor sensibile;
- Analiza compozițională a software-ului pentru descoperirea integrală a componentelor open source în codul sursă, maparea componentelor cu vulnerabilități cunoscute, identificarea licențierii a riscului de calitate a componentelor, stabilirea și aplicarea politicilor open source, integrarea managementului open source în ciclul de dezvoltare și monitorizarea și alertarea la noile amenințări;
- Utilizarea tehnologiei specifice pentru a evalua riscul prin descoperirea vulnerabilităților cunoscute ale software-ului terță și al software-ului open source și ale componentelor utilizate pentru implementarea unei aplicații;
- Analiza vulnerabilităților pentru identificarea și evaluarea riscurilor de securitate în două etape: identificarea și validarea vulnerabilităților;
- Realizarea hărții grafice a dispozitivelor;
- Prioritizarea remedierii prin atribuirea unui impact asupra fiecărui activ;
- Identificare ce sistem de operare, porturi, servicii și certificate există pe fiecare dispozitiv din rețea;
- Control asupra dispozitivelor din rețea care pot fi scanate;
- Monitorizarea continuă a perimetrului pentru schimbări neașteptate;
- Etichetarea dinamică a activelor pentru a clasifica automat serverele prin atribute precum adresa de rețea, porturile deschise, sistemul de operare, software-ul instalat și vulnerabilitățile găsite;
- Selectare dispozitive de rețea țintă după adresa IP, grupul de elemente sau eticheta de active;
- Scanare manuală, conform unui program sau continuu;
- Scanare rețele interne complexe, chiar și cu adrese IP suprapuse;
- Monitorizarea certificatele digitale în rețea - ce urmează să expire, ce gazde sunt folosite, dimensiunea cheii și dacă acestea sunt sau nu asociate cu orice vulnerabilități;



- Identificare dispozitive care au nevoie de actualizări;
- Examinarea vulnerabilităților din rețea în timp, la diferite nivele de detaliu;
- Prezice ce gazde sunt expuse riscului atacurilor Zero-Day;
- Generare rapoarte consolidate despre ce dispozitive au nevoie de patch-uri;
- Gestionarea excepțiilor atunci când o vulnerabilitate ar putea fi mai riscantă decât un anumit prag.

3.5.4.3.24 Sisteme de operare

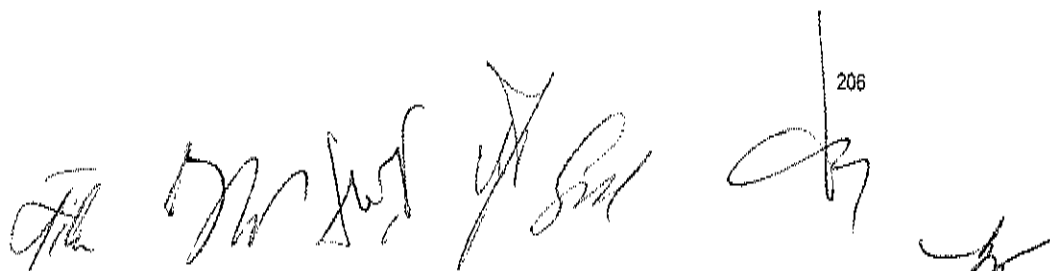
Componenta sisteme de operare va fi folosită în toate instanțele fizice și/sau virtuale suport pentru aplicațiile și serviciile oferite de sistem. Componenta sisteme de operare trebuie să respecte următoarele cerințe funcționale specifice:

- Trebuie să ofere suport pentru arhitectura de procesor pe 64 biți;
- Trebuie să ofere suport pentru lucrul cu minim 1 TB memorie RAM;
- Trebuie să ofere suport pentru lucrul cu sisteme de fișiere jurnalizate (minim EXT3/4, NTFS);
- Trebuie să ofere suport pentru lucrul în regim multi-tasking;
- Trebuie să ofere suport pentru lucrul cu memoria virtuala (SWAP);
- Trebuie să ofere suport nativ pentru cel puțin o tehnologie de virtualizare a resurselor de procesare, stocare și rețea;
- Trebuie să ofere suport pentru stocarea și replicarea datelor;
- Trebuie să ofere suport pentru lucrul cu servere de aplicație, web și/sau baze de date;
- Trebuie să ofere suport pentru controlul accesului și al identității;
- Trebuie să ofere suport pentru lucrul la nivel de rețea (DNS, DHCP, SDN, VPN, QoS, Firewall, Load Balancing);
- Trebuie să ofere suport pentru accesul de la distanță (Remote Desktop sau echivalent);
- Trebuie să ofere suport pentru securitate sporită (utilizator/parola, token-uri, Kerberos, TLS- SSL);
- Trebuie să ofere suport pentru diagnoza;
- Trebuie să include o consola grafică de administrare;
- Trebuie să include o componenta de execuție automatizată a sarcinilor;
- Trebuie să ofere suport pentru lucrul cu browsere de internet.

3.5.4.4 Modelul operațional al sistemului

Modelul operațional al sistemului este structurat per site în câte două medii – producție și testare / dezvoltare pentru site-ul primar și producție și testare de performanță pentru site-ul secundar. Mediul de producție are 3 zone de separare - DMZ, INTERN și SECURITATE / ADMINISTRARE, separarea ținând cont de destinația componentelor sau a modulelor asociate componentelor din cadrul proiectului. Sistemul va fi instalat atât în centrul de date principal cât și în centrul de date secundar, iar testarea va viza funcționarea sistemului informatic în ambele centre de date.

206



Notă: Ofertanții vor avea în vedere integrarea în proiect, din punct de vedere monitorizare, a echipamentelor prevăzute pentru subsistemele SIIBRIS, BigData, BSC, IRI și SAE.

Componenta de virtualizare va fi extinsă pentru a integra și echipamentele hardware prevăzute pentru SII și achiziționate în cadrul proiectului Big Data. Ofertanții vor ține cont de specificațiile echipamentelor respective, acestea fiind descrise în cadrul secțiunii Arhitectura hardware a sistemului.

Principalele caracteristici ale modelului sunt prezentate în continuare:

- pentru implementarea cluster fail-over la nivelul mașinilor virtuale se vor utiliza funcționalitățile puse la dispoziție de către platforma de virtualizare. În cazul mașinilor fizice se vor utiliza funcțiile sistemelor de operare sau cele puse la dispoziție de componentele aplicative (ex: baza de date, server de aplicații), dacă este cazul;
- mașinile de baze de date pentru componentele portal, integrare și schimb de informații, servicii electronice, raportare și analiză, ETL și gestiune identitate și acces utilizatori vor rula într-o configurație de tip cluster activ-pasiv;
- mașinile de server de aplicații pentru serviciile electronice vor rula într-o configurație de tip cluster activ-activ cu balansarea încărcării;
- componentele non-critice vor fi implementate în regim de tip cluster fail-over, nefiind necesară balansarea încărcării, respectiv ca nodurile să fie toate active;
- mediul de producție al sistemului este împărțit în trei zone principale: DMZ, INTERN și SECURITATE / ADMINISTRARE. Toate zonele comunică securizat între ele, separarea logică realizându-se în funcție de destinația operațională a acestora, respectiv: DMZ - comunicarea cu exteriorul (portal, integrare), INTERN - nucleul de procesare pentru serviciile electronice și componentele suport (BPM, Integrare, Raportare, ETL) și SECURITATE / ADMINISTRARE - partea de securitate și componente de administrare, monitorizare a infrastructurii și gestiune a dispozitivelor;
- ambele site-uri au aceeași topologie și alocare de resurse la nivelul componentelor cu precizarea că mediul de testare/dezvoltare se află doar în site-ul primar, iar mediul de testare de performanță se află în site-ul secundar. Alegerea distribuției mediului de testare/dezvoltare și testare de performanță între site-uri are rațiuni economice, se optimizează numărul de mașini fizice necesare și totodată ambele site-uri vor avea noduri active accesibile, astfel încât investiția în echipamente și software să fie maximizată;
- implementarea cross-site cluster fail-over (mediu de producție) va presupune ca fiecare site să găzduiască componente "active" (nodurile sunt active), respectând o balansare în ceea ce privește alocarea resurselor necesare unei componente "active" la nivel de site. Fail-over-ul între site-uri se va realiza prin intermediul platformei de virtualizare și/sau prin mecanismele puse la dispoziție de către sistemele de operare sau componentele aplicative (server de aplicații, baza de date);
- mediul de testare/dezvoltare din site-ul primar este separat complet de mediul de producție și implementează o topologie arhitecturală similară cu cel de producție astfel încât să se poată realiza testare funcțională sau non-funcțională relevantă în ceea ce privește lucrul în condiții asemănătoare cu mediul de producție. Diferența este că alocarea de resurse este mai redusă.



207

- mediul de testare de performanță din site-ul secundar este separat complet de mediul de producție și implementează o topologie arhitecturală similară cu cel de producție astfel încât să se poată realiza testare relevantă în ceea ce privește lucrul în condiții asemănătoare cu mediul de producție, în special desigur pentru teste de performanță. În cazul în care testarea de performanță va necesita resurse mai puternice, se pot alocă mașini noi virtuale (ca și noduri suplimentare) sau mașinile virtuale existente pot avea o suplimentare de resurse de procesare. Provizionarea se poate face foarte ușor la nivelul platformei de virtualizare;
- Alocarea de resurse (CPU, RAM) pentru toate componentele sistemului trebuie să țină cont de: numărul de utilizatori ce generează conexiuni la nivelul sistemului, tehnologiile actuale la nivelul serverelor de aplicații sau baze de date, precum și numărul actualizat de servicii electronice ce vor fi puse la dispoziția persoanelor fizice și juridice.

3.5.4.5 Arhitectura hardware a sistemului

Platforma hardware și infrastructura pe care se va baza sistemul va fi una robustă, scalabilă și redundantă pe verticală. Sistemul propus va lua în considerare volumele de informații procesate și vehiculate și modul în care acestea pot fi distribuite pentru o productivitate maximă. Drept urmare, sistemul rezultat va fi unul flexibil și stabil din punct de vedere al repartizării resurselor de calcul, dar și în ceea ce privește fluxurile informaționale.

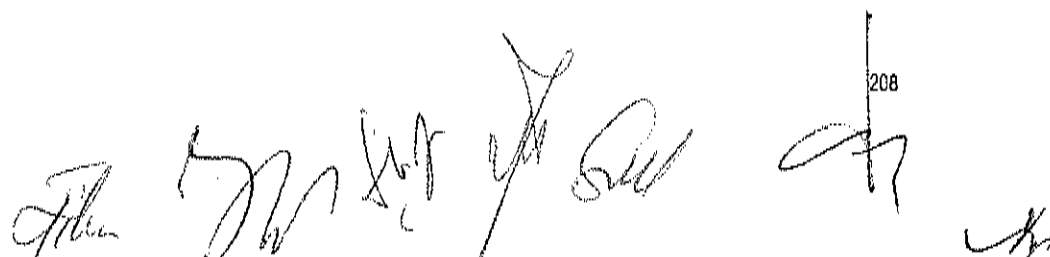
Noul sistem informatic integrat se va baza pe o arhitectură centralizată într-o singură locație ce îndeplinește următoarele cerințe:

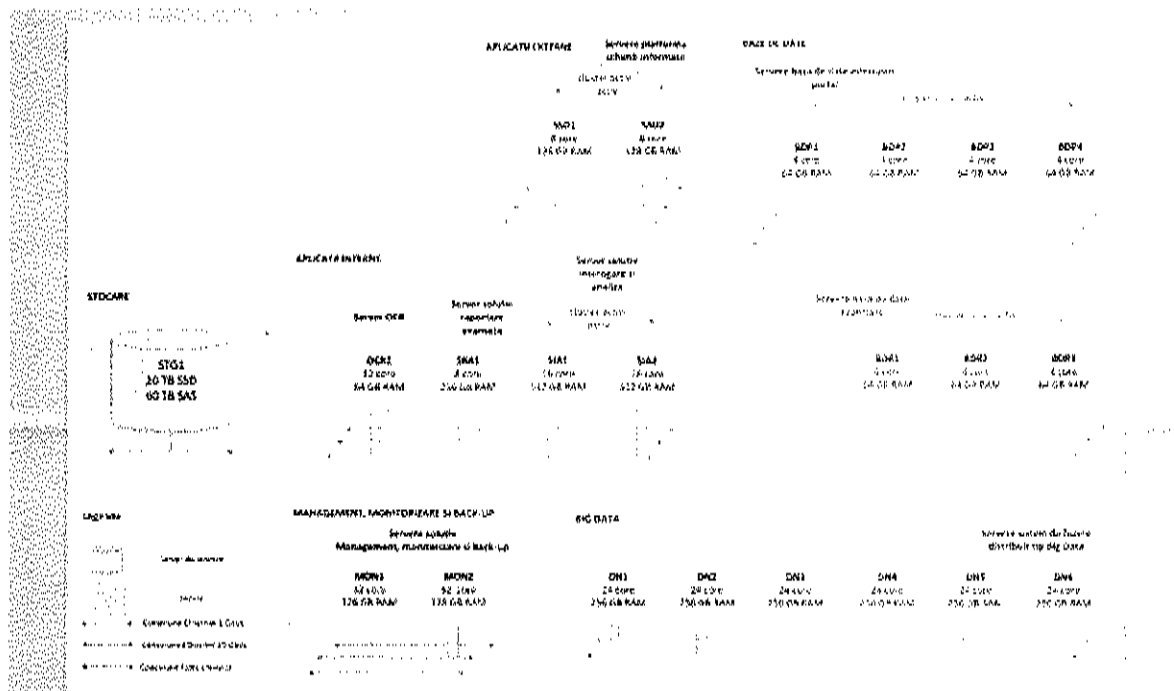
- adăpostește fizic echipamentele și logic aplicațiile necesare pentru realizarea funcționalităților sistemului;
- stochează datele rezultate din activitățile aferente proiectului;
- stochează copii de siguranță.

Arhitectura sistemului va fi în principal bazată pe o infrastructură complet virtualizată ce va asigura un transfer dinamic de capacitate de procesare și necesar memorie pornind de la capacitățile minime solicitate la nivel de modul / aplicație sau componentă aplicativă, în funcție de necesarul de resurse disponibil într-un moment de timp. Astfel, se va asigura o capacitate de procesare ce va putea susține și perioade de vârf de lucru și de asemenea va permite o extensie facilă pe viitor atât prin scalare orizontală ca și număr de instanțe active cât și prin scalare verticală prin număr de resurse procesare minim alocate.

Notă: Arhitectura propusă va integra în proiect și echipamentele prevăzute pentru SII în proiectul "Îmbunătățirea Capacității de Procesare a Datelor și Creșterea Performanțelor de Raportare ale ONRC prin Arhitecturi și Tehnologii Big Data". Astfel, se va constitui o infrastructură dedicată pentru accesarea portalului de către utilizatori din afara țării, schimb de date cu sistemele externe, precum și capabilități de raportare către persoane / entități din Uniunea Europeană - interfață în limba engleză. Pentru integrarea facilă în noul concept arhitectural al SII 2.0, se va avea în vedere dimensionarea componentei de virtualizare din proiect

208





Figură: Arhitectura logică proiect "Big Data"

Astfel, nu se va mai bugeta o infrastructură suplimentară pentru asigurarea interfațării / accesului cu persoane / entități din Uniunea Europeană - cu interfață în limba engleză, se vor utiliza echipamentele prevăzute în proiectul "Îmbunătățirea Capacității de Procesare a Datelor și Creșterea Performanțelor de Raportare ale ONRC prin Arhitecturi și Tehnologii Big Data".

Totodată, din perspectiva integrării cu instituțiile europene, sistemul propus se va integra și cu SIIBRIS (sistem informatic implementat în cadrul ONRC) pentru asigurarea interoperabilității cu platforma centrală europeană.

Punctele de interacțiune cu SIIBRIS vor fi:

- la nivelul bazei de date unde se folosesc mecanisme de replicare între actuala bază de date a SII al ONRC și baza de date SIIBRIS;
- la nivel de aplicație prin intermediul serviciilor web expuse de SII al ONRC, servicii care vor fi furnizate de către noul sistem ce face obiectul prezentului proiect;

Infrastructura existentă în proiectul "Big Data" ce va fi integrată în cadrul proiectului SII 2.0, este următoarea:

- Servere baze de date pentru portal:

Denumire	CPU (core-uri)	RAM (GB)
----------	----------------	----------

209

BDP1	4	64
BDP2	4	64
BDP3	4	64
BDP4	4	64

Specificațiile pentru serverele de baze de date pentru portal prevăzute și achiziționate în proiectul Big Data sunt următoarele:

- CPU: 1 x 4core Xeon E5 v4 (sau echivalent) min. 3.5 GHz;
- RAM: 128 GB;
- RAID: controller RAID HW 0,1;
- Discuri interne: 2 x 300GB 10k rpm SAS 2.5";
- Porturi rețea LAN: 2 x 10 Gbps Ethernet (SFP+ optic) și 2 x 1 Gbps Ethernet (RJ45);
- Porturi rețea SAN: 2 x 16 Gbps Fibre Channel;
- Surse alimentare: redundante și hot-swap;
- Management: out of band cu controller dedicat cu posibilitate de KVM remote;
- Format: rack-mount maxim 1U;

- Servere baze de date pentru raportare:

Denumire	CPU (core-uri)	RAM (GB)
BDR1	4	64
BDR2	4	64
BDR3	4	64

Specificațiile pentru serverele de baze de date pentru raportare prevăzute și achiziționate în proiectul Big Data sunt următoarele:

- CPU: 1 x 4core Xeon E5 v4 (sau echivalent) min. 3.5 GHz;
- RAM: 128 GB;
- RAID: controller RAID HW 0,1;
- Discuri interne: 2 x 300GB 10k rpm SAS 2.5";
- Porturi rețea LAN: 2 x 10 Gbps Ethernet (SFP+ optic) și 2 x 1 Gbps Ethernet (RJ45);
- Porturi rețea SAN: 2 x 16 Gbps Fibre Channel;
- Surse alimentare: redundante și hot-swap;
- Management: out of band cu controller dedicat cu posibilitate de KVM remote;
- Format: rack-mount maxim 1U;

210

- Servere platformă schimb de informații:

Denumire	CPU (core-uri)	RAM (GB)
SSD1	8	128
SSD2	8	128

Specificațiile pentru serverele de schimb de informații cu sisteme externe prevăzute și achiziționate în proiectul Big Data sunt următoarele:

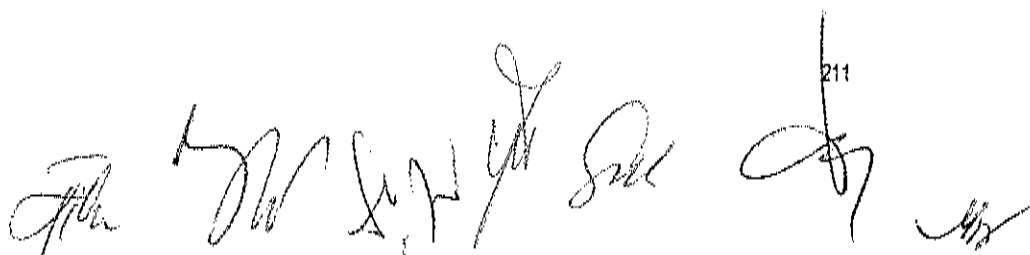
- CPU: 1 x 8core Xeon E5 v4 (sau echivalent), min. 3.2 GHz;
- RAM: 128 GB;
- RAID: controller RAID HW 0,1;
- Discuri interne: 2 x 300GB 10k rpm SAS 2.5";
- Porturi rețea LAN: 2 x 10 Gbps Ethernet (SFP+ optic) și 2 x 1 Gbps Ethernet (RJ45);
- Porturi rețea SAN: 2 x 16 Gbps Fibre Channel;
- Surse alimentare: redundante și hot-swap;
- Management: out of band cu controller dedicat cu posibilitate de KVM remote;
- Format: rack-mount maxim 1U;

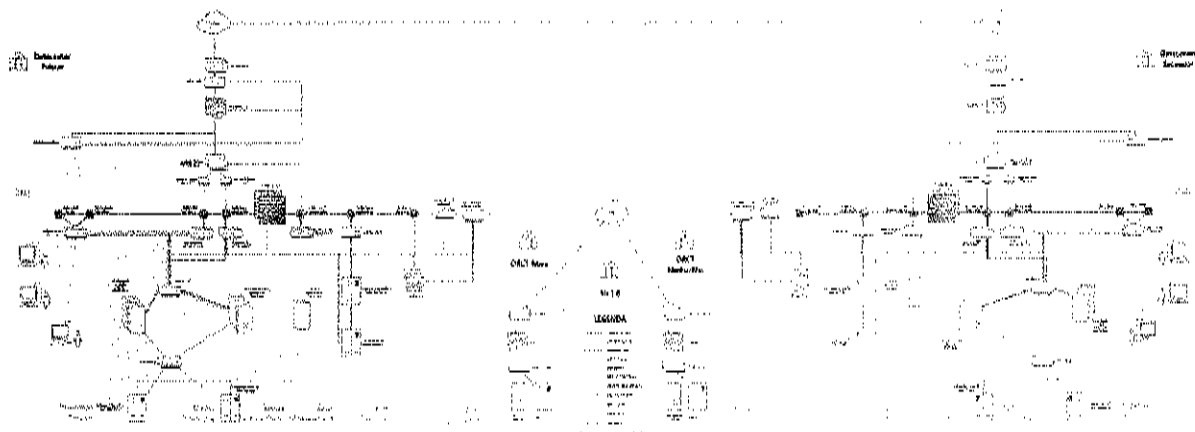
Echipamentele de mai sus sunt în locația din București și vor fi integrate la nivelul întregului sistem SII 2.0, la nivel de management - prin intermediul componentei de virtualizare și la nivel funcțional prin intermediul serviciilor web și al replicării de date între baza de date principală aferentă serviciilor electronice, cea a portalului accesibil la nivel național și baza de date a portalului destinat utilizatorilor din Uniunea Europeană. Similar, pentru raportare, va exista posibilitatea de replicare a datelor din cadrul bazei de date de raportare la nivel de servicii electronice și cea destinată utilizatorilor externi.

Pentru a beneficia de capacități crescute de procesare la nivel de noduri active definite în cadrul arhitecturii propuse utilizând componenta de virtualizare din cadrul sistemului, se va implementa un mecanism de fail-over cross-site (între site-ul principal și cel secundar), astfel încât site-ul secundar să conțină și noduri active capabile să preia și să proceseze cereri. Implementarea mecanismului de fail-over între site-uri se va realiza în două moduri:

- la nivelul componentei de virtualizare, utilizând mecanismele specifice ale acestei componente - mașinile virtuale vor fi pornite automat de către componenta de virtualizare în site-ul secundar, în caz de defecțiune în site-ul primar - și invers;
- la nivelul sistemelor de operare sau componentelor aplicative, în cazul în care serverele fizice nu sunt virtualizate - după caz;

211





Figură - Arhitectura fizică

Cele două site-uri (principal și secundar) vor avea o arhitectură în oglindă - mediul de producție având o topologie de instalare identică (cu excepția zonei dedicate interacțiunii cu Uniunea Europeană, care este gestionată în site-ul principal), cu mențiunea că se va ține cont de implementarea mecanismului de fail-over cross-site ce va presupune că anumite noduri vor fi active iar altele în regim stand-by. La nivelul site-ului principal va exista și un mediu de testare și dezvoltare ce va avea o topologie similară cu mediul de producție, dar va avea alocate mai puține resurse de procesare și stocare, în site-ul secundar nu va exista mediu de testare/dezvoltare.

3.5.4.5.1 Concepte generale de arhitectura

Arhitectura hardware a infrastructurii propuse va respecta următoarele principii arhitecturale de bază:

- **înaltă disponibilitate pentru componentele sistemului;**

Înaltă disponibilitate este implementată printr-o arhitectură de tip „No Single Point Of Failure” (NSPOF) pentru componentele sistemului. În acest scop se vor utiliza următoarele elemente de arhitectură:

- instalarea pe cel puțin două noduri operaționale folosind configurații de tip cluster, inclusiv în regim multi-nod cu distribuție la nivel de mașini virtuale, cu împărțirea puterii de procesare în mod egal pe acestea, astfel încât indisponibilitatea unui nod să nu reducă semnificativ puterea totală de procesare;
- folosirea de echipamente de tip switch redundante (Ethernet sau Fibre Channel), dispuse în perechi de echipamente identice (cu excepția switch-ului necesar pentru rețeaua de management, care nu necesită redundanță, nedeservind un serviciu fără de care nu se poate utiliza sistemul). Toate echipamentele se vor conecta la ambele switch-uri din cadrul perechilor folosind tehnologii ce asigură disponibilitate ridicată a conexiunilor la rețelele LAN (porturi de rețea fizice conectate la switch-uri Ethernet fizice diferite și configurate în bonding) și SAN (porturi fizice conectate la switch-uri Fibre Channel fizice diferite și configurate cu căi multiple/multi-pathing);
- utilizarea într-o cât mai mare măsură a redundanței interne a echipamentelor hardware, cum ar fi: surse de alimentare redundante, porturi fizice multiple de conectare la rețelele LAN și SAN, discuri

212

interne configurate în RAID la nivel hardware/controller hardware, echipamente de stocare cu controllere RAID hardware redundante;

- **scalabilitate;**

Atingerea obiectivelor de scalabilitate a infrastructurii hardware propuse se va putea realiza în 2 moduri:

- orizontal, prin adăugarea de noi procesoare sau servere fizice;
- vertical, prin adăugarea de procesoare suplimentare și RAM în echipamentele de tip server, respectiv discuri suplimentare în echipamentele de stocare.

- **uniformitate;**

Uniformitatea arhitecturii este realizată prin:

- utilizarea aceleiași tehnologii hardware de procesor (tip CISC) pentru toate serverele sistemului;
- utilizarea aceluiași sistem de operare pentru majoritatea echipamentelor de tip server din arhitectură. Excepțiile vor fi prezentate de către ofertant motivat în cadrul propunerii tehnice.

3.5.4.5.2 Infrastructura aferentă mediilor de lucru ale sistemului

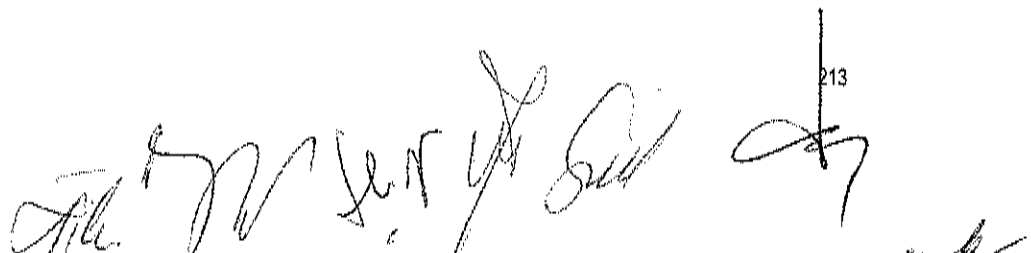
Mediul de producție rulează în mod virtualizat pe serverele de procesare lamelare. Aceste servere fizice sunt partajate și cu mediul de testare, dar sistemul va implementa o separare logică a mediilor, controlul resurselor de procesare (CPU, RAM) fiind gestionate independent prin intermediul componentei de virtualizare. Serverele de procesare lamelare sunt conectate la sistemul de stocare tip 1 prin intermediul switch-ului SAN (conexiune FC) în vederea gestionării datelor operaționale, la nivelul sistemului de stocare tip 1 fiind de altfel gestionate și mașinile virtuale (ca imagini binare). Bazele de date vor fi gestionate la nivelul echipamentului de stocare tip 2 care este unul de tip all-flash ce oferă performanțe superioare la accesarea și scrierea datelor față de modelele clasice.

Mediul de testare / dezvoltare localizat în site-ul principal partajează serverele de procesare lamelare fizice cu mediul de producție, dar este separat logic la nivelul componentei de virtualizare prin alocarea unui pool dedicat de resurse de procesare (CPU, RAM). La fel ca și mediul de producție, mediul de testare-dezvoltare este conectat la sistemul de stocare tip 1 prin intermediul switch-ului SAN (conexiune FC) în vederea gestionării datelor de test, iar bazele de date de test sunt gestionate la nivelul echipamentului de stocare tip 2.

Mediul de testare de performanță localizat în site-ul secundar partajează serverele de procesare lamelare fizice cu mediul de producție, dar este separat logic la nivelul componentei de virtualizare prin alocarea unui pool dedicat de resurse de procesare (CPU, RAM). La fel ca și mediul de producție, mediul de testare de performanță este conectat la sistemul de stocare tip 1 prin intermediul switch-ului SAN (conexiune FC) în vederea gestionării datelor de test, iar bazele de date de test sunt gestionate la nivelul echipamentului de stocare tip 2.

Comunicarea între serverele de procesare lamelare se realizează prin intermediul echipamentului de interconectare privată instalat împreună cu serverele la nivelul șasiului modular, la rândul lui acesta fiind instalat în rack. Echipamentul de stocare tip 3 este unul dedicat în special colectării informației nestructurate (documente) de la nivelul ORCT-urilor, arhitectura de implementare fiind de tip cluster multi-node / multi-site.

213



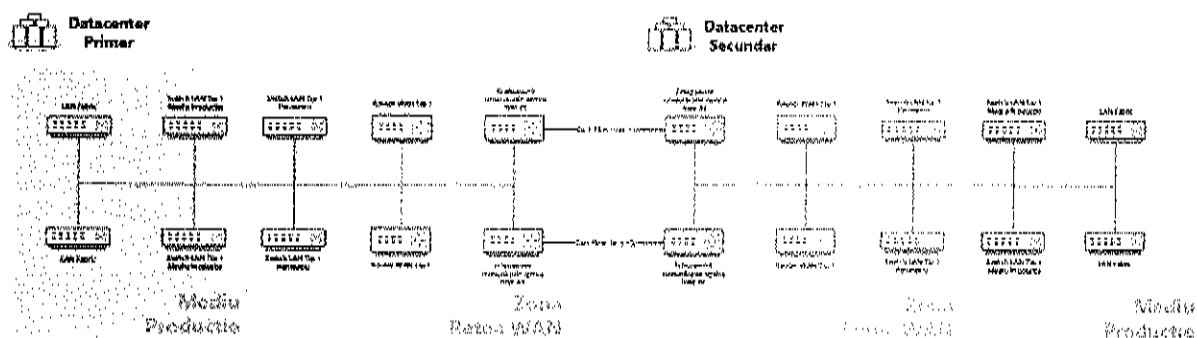
Serverele de procesare lamelare sunt conectate și la acest echipament prin intermediul switch-ului LAN tip 1 (conexiune Ethernet) astfel încât aplicațiile să aibă acces la datele nestructurate colectate, atât cele din mediul de producție, cât și cele din mediile de testare.

3.5.4.5.3 Comunicarea între sedii

Pentru implementarea comunicației între ORCT București (site primar) și ORCT Constanța (site secundar) va fi necesară realizarea unei comunicații cu lățime mare de bandă și latență mică între cele două sedii. Costurile privitoare la aceste lucrări vor fi suportate de către ONRC, în cadrul proiectului fiind incluse doar echipamentele de comunicație optică (câte două per site).

În acest scop, cele 2 locații se vor interconecta prin intermediul a 2 fibre optice single mode (recomandat pe trasee fizice diferite). Pentru a interconecta cele 2 site-uri se vor folosi (pentru asigurarea redundanței) câte 2 echipamente de comunicație optică securizată. Aceste echipamente vor realiza extensia comunicației de tip Ethernet, prin interconectarea cu latență mică a switch-urilor core din fiecare locație.

Pentru securizare comunicației, echipamentele vor suporta criptarea traficului la nivel de mediu de transport al informației pe fibră optică dintre site-uri. Conectivitatea între cele două sedii (site primar București și site secundar Constanța) se va face conform diagramei de mai jos:



Figură - Conectivitatea între site-uri

3.5.4.5.4 Cerințe tehnice minimale și cantități pentru echipamente

Calculul de cantități este realizat ținând cont de ambele site-uri (primar și secundar). Echipamentele propuse în cadrul arhitecturii tehnice trebuie să îndeplinească următoarele cerințe tehnice minimale:

3.5.4.5.4.1 Server de procesare lamelar - 64 bucăți

Cerinte:

- Server de procesare generala de tip lamelar, compatibil cu șasiurile modulare oferitate;
- CPU: 2x14 core Xeon E5 v4 (sau echivalent), min.2.3 GHz, cache min. 35MB L3;

214

- RAM: 256 GB DDR4 2166 MHz cu posibilitate de extensie pana la 3 TB;
- Stocare interna:
 - minim 2 module SD sau SSD în RAID 1 cu o capacitate totala de minim 32 GB (folosite exclusiv pentru instalarea hipervizorului platformei de virtualizare);
- Porturi LAN: minim 4x 10Gbps Ethernet cu suport unificat Ethernet/ iSCSI/FCoE;
- Porturi SAN: minim 2x 16Gbps FC;
- Management: out of band cu controller dedicat și suport pentru KVM la distanta;
- Securitate: Trusted Platform Module 2.0;
- Format: lamelar;

3.5.4.5.4.2 Șasiu modular servere - 8 bucati

Cerinte:

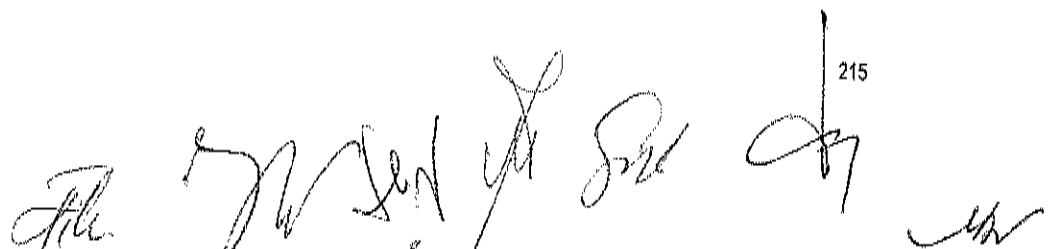
- Arhitectura: Montabil în rack standard de 19";
- Capacitate: minim 5 noduri de procesare în format lamelar;
- Midplane: pasiv, fără elemente de comutare active, cu lărgime de banda agregata de minim 1Tbps;
- Interconectare: cu alte șasiuri similare pentru agregarea resurselor de procesare, stocare și a extensiilor I/O ale acestora într-o singura platforma unificata, administrabila prin intermediul unui singur set unitar de unelte de management;
- Porturi LAN: capabilitatea de a asigura minim 4x 10Gbps Ethernet cu suport unificat Ethernet/ iSCSI/FCoE pentru fiecare nod de procesare în echiparea maxim suportată cu noduri de procesare;
- Porturi SAN: capabilitatea de a asigura minim 2x 16Gbps FC pentru fiecare nod de procesare în echiparea maxim suportată cu noduri de procesare;
- Alimentare: minim 4 surse de alimentare redundante/hot-swap.

3.5.4.5.4.3 Echipament de interconectare privată - 4 bucati

Cerinte:

- Arhitectura: cluster activ-activ, montabil în rack standard de 19";
- Management: fara management local, administrabile la nivelul intregului sistem compus din sasiurile modulare de servere si serverele tip 1;
- Porturi LAN: capabilitatea de a asigura minim 4x 10Gbps Ethernet cu suport unificat Ethernet/ iSCSI/FCoE pentru fiecare nod de procesare în echiparea maximă cu noduri de procesare a șasiurilor modulare;
- Porturi SAN: capabilitatea de a asigura minim 2x 16Gbps FC pentru fiecare nod de procesare în echiparea maximă cu noduri de procesare a șasiurilor modulare;
- Porturi interconectare: minim 4x 40Gbps de tip unificat Ethernet/ iSCSI/FC/FCoE;

215



- Performanță de comutare: minim 950 Gbps;
- Funcționalități Layer 2 de comutare: minim 1000 VLAN-uri și VSAN-uri, QoS, capabilități de priorizare strictă (CoS);

3.5.4.5.4.4 Switch SAN - 4 bucăți

Cerinte:

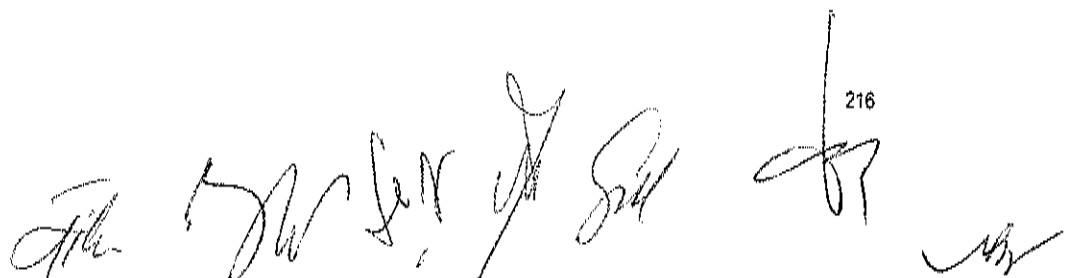
- Porturi: minim 48 porturi FC 16Gbps;
- Porturi de consola: minim 1;
- trebuie să ofere suport pentru izolare fabric VSAN, zonare pe baza de ACL-uri, autentificare între switch-uri și servere pe baza protocolului FC-SP, autentificare bazata pe roluri de administrare (RBAC)/TACACS+ și LDAP;
- Trebuie să includă capabilități de management și acces SFTP, SSH, și SNMP;
- Trebuie să includă următoarele funcționalități: backplane pasiv ce permite repornirea proceselor fără întreruperea comunicației, agregarea porturilor de comunicație în orice configurație, multi-pathing la nivelul întregului fabric, definirea fabric-ului la nivel de VSAN, monitorizarea activa a porturilor de comunicație, VRRP pentru porturile de management, diagnosticarea online a echipamentului și modulelor;
- Doua surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.5 Complet stocare tip 1 - 2 bucati

Cerinte:

- Arhitectura: cluster activ-activ cu minim 2 controller-e hot-swap, montabil in rack standard de 19";
- Capacitate bruta: minim 50TB pe discuri de tip Flash (SSD, NVMe, etc);
- Capacitate utila: minim 150TB capacitate utila pe discuri de tip Flash NVMe, indiferent de rata de optimizare în urma proceselor de deduplicare și/sau compresie;
- Conexiuni: minim 24x 16Gbps FC in configuratie de 2 controller-e;
- RAID: Mecanisme de redundanta cu minim un disc si doua discuri de paritate;
- Cache: minim 1TB per controller;
- Capabilitati integrate hardware de compresie si deduplicare in timp real (inline);
- Sistemul trebuie să poată acomoda minim 1 PB pentru extensie ulterioara;
- Capabilitati de thin-provisioning si overcommitment;
- Capabilități de multipathing: fail-over și load-balancing, indiferent de numărul de servere care se vor conecta la sistem;
- Capabilități de hot sparing;

216



- Suport pentru replicare locala a volumelor (snapshot și clone) și replicare la distanta (sincron și asincron);
- Software de management inclus.

3.5.4.5.4.6 Complet stocare tip 2 - 2 bucati

Cerinte:

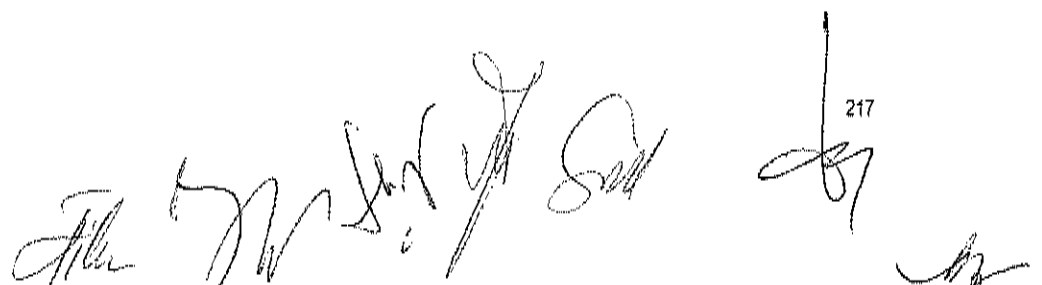
- Arhitectura: cluster activ-activ cu minim 2 controller-e hot-swap, montabil in rack standard de 19";
- Capacitate bruta: minim 20TB pe discuri de tip Flash (SSD, NVMe, etc);
- Capacitate utila: minim 15TB capacitate utila (indiferent de rata de optimizare în urma proceselor de deduplicare și/sau compresie);
- Conexiuni:
 - minim 8x 16Gbps FC in configuratie de 2 controller-e;
 - minim 4x 10Gbps Ethernet/iSCSI in configuratie de 2 controller-e;
- RAID: Mecanisme de redundanta cu minim un disc si doua discuri de paritate;
- Cache: minim 1TB per controller;
- Capabilitati integrate hardware de compresie si deduplicare in timp real (inline);
- Sistemul trebuie sa poata acomoda minim 4 PB pentru extensie ulterioara;
- Capabilitati de thin-provisioning si overcommitment;
- Capabilitati de multipathing: failover si load-balancing, indiferent de numarul de servere care se vor conecta la sistem;
- Capabilitati de hot sparing;
- Suport pentru replicare locala a volumelor (snapshot si clone) si replicare la distanta (sincron si asincron);
- Software de management inclus.

3.5.4.5.4.7 Complet stocare tip 3 - 1 bucala

Cerinte:

- Complet-ul va fi implementat într-o arhitectură de tip cluster multi-node / multi-site;
- Arhitectura: cluster activ-activ cu minim 4 controller-e hot-swap, montabil in rack standard de 19";
- Capacitate bruta: minim 800TB pe discuri de tip SATA/NL-SAS;
- Capacitate utila: minim 500TB capacitate utila (indiferent de rata de optimizare in urma proceselor de deduplicare si/sau compresie);
- Conexiuni: minim 8x 10Gbps Ethernet in configuratie de 4 controller-e;
- RAID: Mecanisme de redundanta de tip mirror pe cel putin 3 din 4 controller-e;

217



- Protocol de acces la date: protocol de tip file (NAS), prin NFS, HDFS (Hadoop), Object (CAS, Atmos, Swift);
- Sistemul trebuie sa poata acomoda minim 3.5 PB pentru extensie ulterioara;
- Capabilitati de multipathing: failover si load-balancing, indiferent de numarul de servere care se vor conecta la sistem;
- Capabilitati de hot sparing;
- Software de management inclus.

3.5.4.5.4.8 Complet rack și accesorii - 12 bucati

Cerintele pentru aceste echipamente sunt mentionate în cadrul capitolului Cerințe privind amenajarea și dotarea centrelor de date, subcapitol Planul de amplasare al echipamentelor.

3.5.4.5.4.9 Soluție backup - 2 bucăți

Cerinte:

- Solutie de backup cu stocare pe doua niveluri (disk backup, virtual tape backup);
- Arhitectura: cluster activ-standby cu minim 2 unitati, montabil in rack standard de 19";
- Capacitate bruta: minim 120TB pe discuri de tip SATA/NL-SAS;
- Conexiuni:
- minim 4x 16Gbps FC in configuratie de 2 unitati;
- minim 8x 10Gbps Ethernet in configuratie de 2 unitati;
- Capabilitati integrate hardware de compresie si deduplicare;
- Sistemul trebuie sa poata acomoda minim 800 GB pentru extensie ulterioara;
- Capabilitati de multipathing: failover si load-balancing, indiferent de numarul de servere care se vor conecta la sistem;
- Capabilitati de hot sparing;
- Suport pentru replicare la distanta (sincron si asincron);
- Software de management si backup inclus cu urmatoarele capabilitati:
- Aplicatie de backup livrata si licentiata pentru intreaga capacitate, compatibila cu dispozitivele de stocare propuse;
- Aplicatia de backup trebuie sa fie o solutie backup de tip enterprise, capabila sa efectueze backup in mod centralizat si programat, fara interventie umana;
- Aplicatia de backup trebuie sa fie capabila sa realizeze backup pentru medii eterogene cu suport pentru sisteme de operare Windows, Linux, Unix, respectiv pentru platforme de virtualizare (cel puțin pentru toate tipurile de sisteme de operare/virtualizare incluse in arhitectura care va fi ofertata de furnizor);

- Soluția de backup va oferi acces la datele stocate, respectiv către platformele și aplicațiile ce beneficiază de procesele de backup, prin protocol de tip file (NAS), prin NFS și CIFS;
- Conectivitate prin protocol de tip FTP, NDMP și VTL;
- Va permite utilizarea simultană a tuturor protocoalelor și interfețelor de rețea, respectiv va permite rularea simultană a proceselor de backup și restore utilizând protocoale diferite și/sau interfețe diferite de rețea;
- Procesul de deduplicare a datelor va putea fi distribuit la sursă sau la destinație în funcție de aplicația de salvare și restaurare utilizată;
- Procesul de deduplicare a datelor se va face utilizând segmente de dimensiuni variabile, în scopul eficientizării factorului de deduplicare.

3.5.4.5.4.10 Router internet - 4 bucăți

Cerințe:

- Echipament router cu funcționalități avansate de rutare acces internet și voce;
- Număr interfețe Ethernet 1 Gbps: minim 8;
- Număr interfețe Ethernet 10 Gbps: minim 8;
- Modul E1 PRI (Trunk Voice T1/E1): 2;
- IPv4 Forwarding: minim 60 Gbps;
- Criptare IPSec: minim 10 Gbps;
- Arhitectura modulară și de tip multiprocesor/multi-core;
- Management de tip out-of-band: port Ethernet, port USB;
- Configurare liste de acces (ACL) bazate pe IP sursă și destinație și/sau porturi UDP/TCP;
- Posibilitate de inspecție la nivel de aplicație (DPI) pentru 1000 protocoale;
- Suport pentru: IPv6, IPv4/IPv6 Dual Stack, Bidirectional Forward Detection, Policy Based Routing, Multicast Internet Group Management Protocol, Unicast Reverse Path Forwarding;
- Tipuri de încapsulare: Ethernet, Generic route encapsulation, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, High Level Data Link Control, PPP over Ethernet;
- Algoritmi criptare: DES, 3DES, AES-128, AES 256;
- Autentificare: RSA 768/1024/2048, ECDSA 256/384;
- Hash: MD5, SHA, SHA-256, SHA-384, SHA-512;
- Suport Next Generation Encryption;
- Posibilitate gestionare trafic de voce, inclusiv conversie analogic-digital;
- Suport conectare trunchiuri SIP (SBC);
- Capacitate (module instalate) pentru procesarea vocii pe cel puțin 64 de canale concomitente;
- Codec-uri: G.711, G.722, G.726, G.728, G.729;

- Capacitati voce: Echo cancellation, Tone detection, Noise reduction, Acoustic shock prevention, Gain control;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19'.

3.5.4.5.4.11 Router WAN tip 1 - 4 bucăți

Cerinte:

- Echipament router cu funcționalități avansate de rutare destinat pentru acces WAN;
- IPv4 Forwarding: minim 2 Gbps;
- Criptare IPSec VPN (AES256 și SHA-384 sau AES256 și SHA-512): minim 1 Gbps;
- Arhitectura modulara și de tip multiprocesor;
- Management de tip out-of-band: port Ethernet, port USB;
- Configurare liste de acces (ACL) bazate pe IP sursa și destinație sau porturi UDP/TCP;
- Posibilitate de inspecție la nivel de aplicație (DPI) pentru 1000 protocoale;
- Suport pentru: IPv6, IPv4/IPv6 Dual Stack, Bidirectional Forward Detection, Policy Based Routing, Multicast Internet Group Management Protocol, Unicast Reverse Path Forwarding;
- Tipuri de încapsulare: Ethernet, Generic route encapsulation, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, High Level Data Link Control, PPP over Ethernet;
- Algoritmi criptare: DES, 3DES, AES-128, AES 256;
- Autentificare: RSA 768/1024/2048, ECDSA 256/384;
- Hash: MD5, SHA, SHA-256, SHA-384, SHA-512;
- Porturi Ethernet 1 Gbps: minim 4;
- Porturi Ethernet 10 Gbps cu interfețe optice SFP+: minim 4;
- Porturi de consola: minim 1;
- Criptare prin IPSec VPN și SLL VPN cu sau fara necesitatea clientului de VPN, pentru IPv4 și IPv6;
- Funcții de QoS ce includ traffic shaping, traffic policing și coada prioritara;
- Funcții translatate NAT de la IPv4 la IPv6 și reciproc, NAT64, NPTv6;
- Rutare: static, policy-based routing, OSPF, BGP (cu suport IPv6);
- Trafic IPS pentru trafic multiprotocol (HTTP, SMTP, FTP, IMAP): minim 2 Gbps;
- Număr de tunele IPSec VPN: minim 4000;
- Numar de tunele SSL VPN concurente incluse: minim 100, cu scalabilitate la 4000;
- Numar clienti VPN concurenti: minim 4000;
- Număr VLAN-uri procesabile: minim 1000;
- Posibilitate funcționare în mod high-availability;

- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.12 Router WAN tip 2 - 41 bucăți

Cerinte:

- Echipament router cu funcționalități avansate de rutare destinat pentru acces WAN;
- IPv4 Forwarding: minim 1 Gbps;
- Criptare IPSec VPN (AES256 și SHA-384 sau AES256 și SHA-512): minim 500 Mbps;
- Arhitectura modulară și de tip multiprocesor;
- Management de tip out-of-band: port Ethernet, port USB;
- Configurare liste de acces (ACL) bazate pe IP sursa și destinație sau porturi UDP/TCP;
- Posibilitate de inspecție la nivel de aplicație (DPI) pentru 1000 protocoale;
- Suport pentru: IPv6, IPv4/IPv6 Dual Stack, Bidirectional Forward Detection, Policy Based Routing, Multicast Internet Group Management Protocol, Unicast Reverse Path Forwarding;
- Tipuri de încapsulare: Ethernet, Generic route encapsulation, 802.1q VLAN, Point-to-Point Protocol, Frame Relay, High Level Data Link Control, PPP over Ethernet;
- Algoritmi criptare: DES, 3DES, AES-128, AES 256;
- Autentificare: RSA 768/1024/2048, ECDSA 256/384;
- Hash: MD5, SHA, SHA-256, SHA-384, SHA-512;
- Porturi Ethernet 1 Gbps: minim 4;
- Porturi Ethernet 10 Gbps cu interfețe optice SFP+: minim 4;
- Porturi de consola: minim 1;
- Criptare prin IPSec VPN și SSL VPN cu sau fără necesitatea clientului de VPN, pentru IPv4 și IPv6;
- Funcții de QoS ce includ traffic shaping, traffic policing și coada prioritară;
- Funcții de traducere NAT de la IPv4 la IPv6 și reciproc, NAT64, NPTv6;
- Rutare: static, policy-based routing, OSPF, BGP (cu suport IPv6);
- Trafic IPS pentru trafic multiprotocol (HTTP, SMTP, FTP, IMAP): minim 1 Gbps;
- Număr de tuneluri IPSec VPN: minim 1000;
- Număr de tuneluri SSL VPN concurente incluse: minim 100, cu scalabilitate la 1000;
- Număr de clienți VPN concurenți: minim 1000;
- Număr de VLAN-uri procesabile: minim 1000;
- Posibilitate de funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;

- Montabil în rack standard de 19"

3.5.4.5.4.13 Echipament de comunicație optică - 4 bucăți

Cerinte:

- Echipament router pentru asigurarea comunicației prin fibră optică între cele site-uri principale;
- Management de tip out-of-band: port Ethernet, port USB;
- Porturi:
 - Minim 80 porturi Ethernet 1/10 Gbps cu interfețe optice SFP+;
 - Minim 4 porturi 100 GBps pentru uplink - QSFP;
- Switching Layer 2:
 - IEEE 802.1Q VLAN;
 - IEEE 802.1ad;
 - IEEE 802.3ad;
- Switching Layer 3:
 - Protocoale de rutare: Static, OSPFv2, OSPFv3, ISIS, BGP;
 - Bidirectional Forwarding Detection (BFD);
 - IPV6 unicast;
 - IEEE 802.3ad;
- Securitate:
 - ACLs;
 - AAA;
 - TACACS+;
 - SSH;
 - SNMPv3;
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19";

3.5.4.5.4.14 Switch LAN tip 1 - 12 bucăți

Cerinte:

- Switch de agregare cu capabilități Layer 2 și Layer 3;
- Porturi:
 - Minim 48 porturi Ethernet 1/10 Gbps SFP+;
 - Minim 12 porturi 100 GbE QSFP pentru uplink;

- Minim 1 port de consola;
- Capacitate de comutare pachete: 4 Tbps în mod full-duplex;
- Putere procesare: 1.5 bpps;
- Tehnologie stacking de pana la minimum 1.2 Tbps, minim 12 echipamente în stiva;
- Stocare internă de minimum 64 GB în tehnologie flash/SSD;
- Număr de VLAN-uri suportat: minimum 3500;
- Suport pentru: template-uri ACL, protocol IEEE 802.1ae pentru toate porturile, routare VXLAN, Layer 2 multi-pathing, tabele de routare ECMP;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19”;

3.5.4.5.4.15 Switch LAN tip 2 - 4 bucăți

Cerinte:

- Switch de agregare cu capabilități Layer 2 și Layer 3;
- Porturi:
 - Minim 48 porturi Ethernet 1 Gbps;
 - Minim 8 porturi 10 Gbps pentru uplink;
 - Minim 1 port de consola;
- Capacitate de comutare pachete: 250 Gbps în mod full-duplex;
- Putere procesare: 180 Mpps;
- Tehnologie stacking de minim 450 Gbps, minim 8 echipamente în stiva;
- Număr de VLAN-uri suportat: minim 3500;
- Suport pentru: template-uri ACL, protocol IEEE 802.1ae pentru toate porturile, RIP, EIGRP, OSPF, PBR, PIM Multicast, PVLAN, VRRP, PBR, QoS, FHS, 802.1x, SXP, SSO;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19”;

3.5.4.5.4.16 Switch LAN tip 3 - 41 bucăți

Cerinte:

- Switch de agregare cu capabilități Layer 2 și Layer 3;
- Porturi:
 - Minim 24 porturi Ethernet 1 Gbps;
 - Minim 4 porturi 10 Gbps pentru uplink;
 - Minim 1 port de consola;
- Capacitate de comutare pachete: 200 Gbps în mod full-duplex;

- Putere procesare: 150 Mpps;
- Tehnologie stacking de minim 450 Gbps;
- Număr de VLAN-uri suportat: minim 3500;
- Suport pentru: template-uri ACL, protocol IEEE 802.1ae pentru toate porturile, RIP, EIGRP, OSPF, PBR, PIM Multicast, PVLAN, VRRP, PBR, QoS, FHS, 802.1x, SXP, SSO;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.17 Firewall tip 1 - 4 bucăți

Cerinte:

- Posibilitate de provizionare securizata;
- Implementare firewall de tip stateful;
- Oferire suport pentru implementare bazata pe zone de securitate;
- Throughput firewall: 200 Gbps;
- Throughput Threat prevention: 50 Gbps;
- Throughput IPSec VPN: 120 Gbps;
- Stocare internă de minimum 1 TB în tehnologie flash/SSD;
- Număr de sesiuni: 100.000.000, suport pentru: 2.000.000 sesiuni pe secunda;
- Număr tuneluri IPsec VPN : 80.000;
- Utilizatori SSL VPN: 30.000;
- Număr de zone de securitate definite: 500;
- Număr de politici definite: 200.000;
- VLANs: 802.1q, 802.3ad, LACP;
- Funcții translatare NAT de la IPv4 la IPv6 și reciproc, NAT64, NPTv6;
- Routing: OSPF, BGP, RIP, rutare statica, policy-based, PPPoE, Multicast PIM-SM / IGMP, BFD;
- Porturi: 24 x 1/10 Gbps Ethernet SFP+, 4x 40/100 Gbps Ethernet SFP+, 2x 10 Gbps Ethernet SFP+ pentru functiile de HA;
- Management de tip out-of-band: 2x 1 Gbps Ethernet, 1x 1/10 Gigabit Ethernet SFP+, port USB;
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.18 Firewall tip 2 - 4 bucăți

Cerinte:

- Posibilitate de provizionare securizata;

- Implementare firewall de tip stateful;
- Oferire suport pentru implementare bazata pe zone de securitate;
- Throughput firewall: 60 Gbps;
- Throughput Threat prevention: 30 Gbps;
- Throughput IPSec VPN: 20 Gbps;
- Stocare interna de minim 200 GB in tehnologie flash/SSD, 2 TB in tehnologie SAS/SATA;
- Număr de sesiuni: 20.000.000, suport pentru: 400.000 sesiuni pe secunda;
- Numar de zone de securitate definite: 25;
- Număr de politici definite: 2000;
- VLANs: 802.1q, 802.3ad, LACP;
- Funcții translate NAT de la IPv4 la IPv6 și reciproc, NAT64, NPTv6;
- Routing: OSPF, BGP, RIP, rutare statica, policy-based, PPPoE, Multicast PIM-SM / IGMP, BFD;
- Porturi: 4 x 1/10 Gbps Ethernet, 4x 40/100 Gbps Ethernet SFP+, 16x 1/10 Gigabit Ethernet SFP+, 1x 40/100 Gbps Ethernet SFP+ pentru functiile de HA;
- Management de tip out-of-band: 2x 1 Gbps Ethernet;
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19”.

3.5.4.5.4.19 Firewall tip 3 - 41 bucăți

Cerinte:

- Posibilitate de provizionare securizata;
- Implementare firewall de tip stateful;
- Oferire suport pentru implementare bazata pe zone de securitate;
- Throughput firewall: 1.5 Gbps;
- Throughput Threat prevention: 700 Mbps;
- Throughput IPSec VPN: 500 Mbps;
- Stocare internă de minimum 200 GB în tehnologie flash/SSD;
- Număr de sesiuni: 190.000, suport pentru: 9000 sesiuni pe secunda;
- Număr de politici definite: 2000;
- VLANs: 802.1q, 802.3ad, LACP;
- Funcții translate NAT de la IPv4 la IPv6 și reciproc, NAT64, NPTv6;
- Routing: OSPF, BGP, RIP, rutare statica, policy-based, PPPoE, Multicast PIM-SM / IGMP, BFD;
- Porturi: 4 x 1 Gbps Ethernet, 4x 1 Gbps Ethernet SFP, 4x 1/10 Gigabit Ethernet SFP+, 2x 1 Gbps Ethernet pentru functiile de HA;

- Management de tip out-of-band: 1x 1 Gbps Ethernet, 1x USB/microUSB;
- Posibilitate funcționare în mod high-availability;
- Doua surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.20 Firewall tip 4 - 2 bucăți

Cerinte:

- Posibilitate de provizionare securizata;
- Implementare firewall de tip stateful;
- Oferire suport pentru implementare bazata pe zone de securitate;
- Throughput firewall: 80 Gbps;
- Throughput Threat prevention: 10 Gbps;
- Throughput IPSec VPN: 50 Gbps;
- Stocare internă de minimum 450 GB în tehnologie flash/SSD;
- Număr de sesiuni: 50.000.000, suport pentru: 400.000 sesiuni pe secunda;
- Număr tuneluri IPsec VPN : 200.000;
- Utilizatori SSL VPN: 30.000;
- Număr de zone de securitate definite: 500;
- Număr de politici definite: 200.000;
- VLANs: 802.1q, 802.3ad, LACP;
- Funcții translație NAT de la IPv4 la IPv6 și reciproc, NAT64, NPTv6;
- Routing: OSPF, BGP, RIP, rutare statica, policy-based, PPPoE, Multicast PIM-SM / IGMP, BFD;
- Porturi: 24 x 1/10 Gbps Ethernet SFP+;
- Management de tip out-of-band: 2x 1 Gbps Ethernet, port USB;
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.21 Soluție tip "Secure Mail Gateway" - 2 bucăți

Cerinte:

- Arhitectura: posibilitate de implementare în mod MTA (blocare), BCC (monitorizare), TAP/SPAN;
- Capacitate procesare și inspectare: 400.000 e-mail-uri/zi;
- Porturi:
 - 2x 1 Gbps Ethernet;

- 1x 1 Gbps Ethernet pentru management;
- Stocare internă de minimum 600 GB în tehnologie SAS, protejată prin mecanisme de tip RAID;
- Oferă funcționalități de inspectare/analiza a documentelor atașate (executabile Microsoft Windows, Microsoft Office, PDF, Zip, conținut web, fișiere comprimate) cu posibilitate de sand-boxing (customizabil), analiza URL-urilor (reputație, analiza conținutului, etc), decriptarea parolilor (mecanisme euristice și bazate pe dicționare/cuvinte cheie);
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19".

3.5.4.5.4.22 Soluție tip "DNS Firewall" - 2 bucăți

Cerințe:

- Throughput: 10 Gbps;
- Conexiuni L4 pe secunda: 200.000 cps;
- Număr de conexiuni concurente L4: 10.000.000;
- Număr cereri L7 pe secunda: 600.000 rps;
- Conexiuni SSL (chei 2K): 4.000 tps;
- Throughput SSL (chei 2K): 8 Gbps;
- Compresie hardware: 5 Gbps;
- Porturi: 2x 10 Gbps Ethernet SFP+, 2x 1 Gbps Ethernet SFP;
- Stocare internă de minimum 500 GB în tehnologie SAS;
- Suport pentru:
 - furnizarea de răspunsuri de autoritate DNS îndreptând traficul către adresele IP corecte;
 - DNS SEC și pentru răspunsuri la hostname-uri balansate;
 - baza de date de geo locație în scopul direcțării utilizatorilor către cel mai apropiat data center;
 - balansarea pe baza următoarelor metrici: RTT, Hops, Topology, Completion Rate, Packet Rate, Virtual Server Capacity, Bits/second, Link Capacity;
 - mirroring pentru conexiunile non-SSL în configurație Active-Standby;
 - implementarea într-un mediu/topologie cu o singura sub-rețea (subnet), implementarea în mod bridge;
 - primirea de mesaje SOAP/XML de la instrumente externe pentru modificarea configurației controller-elor de aplicații;
 - generarea și afișarea unei hărți a rețelei pentru adresele IP și pool-urile serverelor virtuale;
 - agregarea link-urilor (802.3ad) și LACP (Link Aggregation Control Protocol);
 - spanning-tree - STP, RSTP (Rapid Spanning Tree Protocol), MSTP (multiple spanning tree protocol);

- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19”;

3.5.4.5.4.23 Soluție tip "ADC și WAF" - 4 bucăți

Cerințe:

- Accelerare hardware pentru SSL;
- Throughput: 20 Gbps;
- Număr de instanțe virtuale ADC: 10;
- Conexiuni L4 pe secunda: 400.000 cps;
- Număr de conexiuni concurente L4: 25.000.000;
- Număr cereri L7 pe secunda: 1.000.000 rps;
- Conexiuni SSL (chei 2K): 10.000 cps;
- Throughput SSL (chei 2K): 15 Gbps;
- Compresie hardware: 10 Gbps;
- Protocoale de rutare: OSPF, RIP, BGP;
- Porturi: 4x 10 Gbps Ethernet SFP+, 8x 1 Gbps Ethernet SFP;
- Stocare internă de minimum 500 GB în tehnologie SSD;
- Suport pentru:
 - Load Balancing L4/7 (policy based routing, dynamic content rewrite);
 - Balansare bazata pe algoritmi multipli: round-robin, weighted round-robin, least connection, shortest response;
 - Compresie, caching;
 - Balansare Layer 4: suport TCP/UDP, bazare pe parametri server (CPU, RAM, HDD), IP persistent, cookie persistent, hash cookie;
 - Balansare Layer 7: suport HTTP, HTTPS, FTP, SIP, RDP RTMP, content switching (HTTP Host, HTTP Request, HTTP Referrer), URL Redirect, DNS load balacing, content rewriting;
 - Protecție avansata pentru toate tipurile de amenințări din Top 10 OWASP, Cross-site scripting, SQL Injection, Session Hijacking, Cross-site Request Forgery;
 - Protecție automata pentru atacuri de tip Zero-Day;
 - Scanner de vulnerabilitati incorporat si posibilitate de integrare cu scannere externe;
 - Capabilități web security: white-listing, black-listing, IP Reputation, IP Geolocation;
 - Traducere HTTP/2 - HTTP 1.1;
 - Suport pentru integrare cu soluții PKI;
 - Suport pentru IPv6;

- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19";

3.5.4.5.4.24 Soluție de balansare a încărcării - 4 bucăți

Cerinte:

- Throughput: 10 Gbps;
- Conexiuni L4 pe secunda: 200.000 cps;
- Număr de conexiuni concurente L4: 10.000.000;
- Număr cereri L7 pe secunda: 600.000 rps;
- Conexiuni SSL (chei 2K): 4.000 tps;
- Throughput SSL (chei 2K): 8 Gbps;
- Compresie hardware: 5 Gbps;
- Porturi: 2x 10 Gbps Ethernet SFP+, 4x 1 Gbps Ethernet SFP;
- Stocare internă de minimum 500 GB în tehnologie SAS;
- Suport pentru:
 - Load Balancing L4/7 (policy based routing, dynamic content rewrite);
 - Balansare bazata pe algoritmi multipli: round-robin, weighted round-robin, least connection, shortest response;
 - Compresie, caching;
 - Balansare Layer 4: suport TCP/UDP, bazare pe parametri server (CPU, RAM, HDD), IP persistent, cookie persistent, hash cookie;
 - Balansare Layer 7: suport HTTP, HTTPS, FTP, SIP, RDP RTMP, content switching (HTTP Host, HTTP Request, HTTP Referrer), URL Redirect, DNS load balacing, content rewriting;
 - Suport pentru IPv6;
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare AC 220V redundante;
- Montabil în rack standard de 19";

3.5.4.5.4.25 Soluție tip HSM - 4 bucăți

Cerinte:

Echipamentul criptografic de tip HSM va asigura funcții de suport specifice asimilate autorităților de emitere de certificate digitale (CA) în regim de funcționare offline. Totodată permite asigurarea suportului criptografic hardware pentru funcționalități diverse integrate în aplicațiile dezvoltate și care rulează în arhitectură SOA, respectiv cel puțin pentru securizarea WebServices, în configurații de tip XML-Firewall, management de

identitate și de acces la resurse integrat la nivel de aplicație, semnare și/sau criptare de documente obiect sau de documente de tranzacție generate pe bază de tehnologie XML.

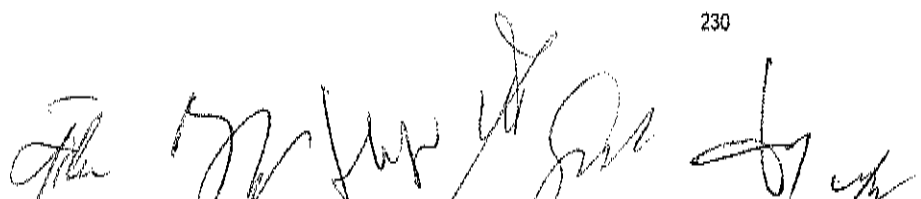
- Suport API: PKCS #11, Java JCE/JCA, Microsoft CAPI, Open SSL;
- Suport REST API pentru administrare;
- Suport pentru sisteme de operare multiple: Unix, Windows, Linux;
- Criptografie:
 - Asimetric: RSA, DSA, Elliptic Curve Cryptography, KCDSA;
 - Simetric: AES, AES-GCM, Triple DES, DES, RC2, RC4, RC5, CAST;
 - Hash digest: SHA-1, SHA-2, SM3;
- Certificare FIPS 140-2-Level 3 PED (password and multi-factor);
- Porturi: 4 x 1GBE;
- Suport IPv4 și IPv6;
- Posibilitate partiționare, număr partiții: 10;
- Performante:
 - RSA-2048: 10.000 tps;
 - ECC P256: 20.000 tps;
 - AES-CGM: 15.000 tps;
- Posibilitate funcționare în mod high-availability;
- Două surse de alimentare de tip hot-swap;
- Montabil în rack standard de 19".

3.6 Managementul utilizatorilor și accesul la sistem

Gestiunea utilizatorilor sistemului precum și gestiunea granulară a accesului acestora la aplicații / module / funcționalități vor fi realizate utilizând componenta gestiune identități și acces utilizatori prevăzută în cadrul proiectului. Această componentă se va integra și cu componenta PKI pentru a asigura autentificarea pe bază de certificat digital, suplimentar la autentificarea pe bază de combinație cont utilizator și parolă.

Cu excepția unor zone funcționale la nivelul componentei portal, ce permit accesul neautentificat, toate funcționalitățile sistemului vor fi disponibile doar utilizatorilor autentificați și autorizați, sistemul implementând o securitate bazată pe roluri, grupuri și permisiuni asociate cu o granularitate suficientă astfel încât să poată fi implementate politici flexibile și totodată scalabile de acces.

Sistemul informatic integrat va trebui să pună la dispoziție mecanismele necesare integrării la nivel național și la nivelul Uniunii Europene cu alte sisteme informatice gestionate de către alte autorități publice astfel încât să se asigure identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă în conformitate cu Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.



Regulamentul eIDAS tratează două domenii principale:

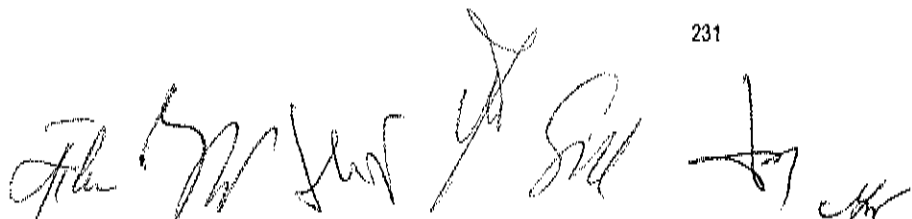
- Identificarea electronică;
- Prestarea serviciilor de încredere.

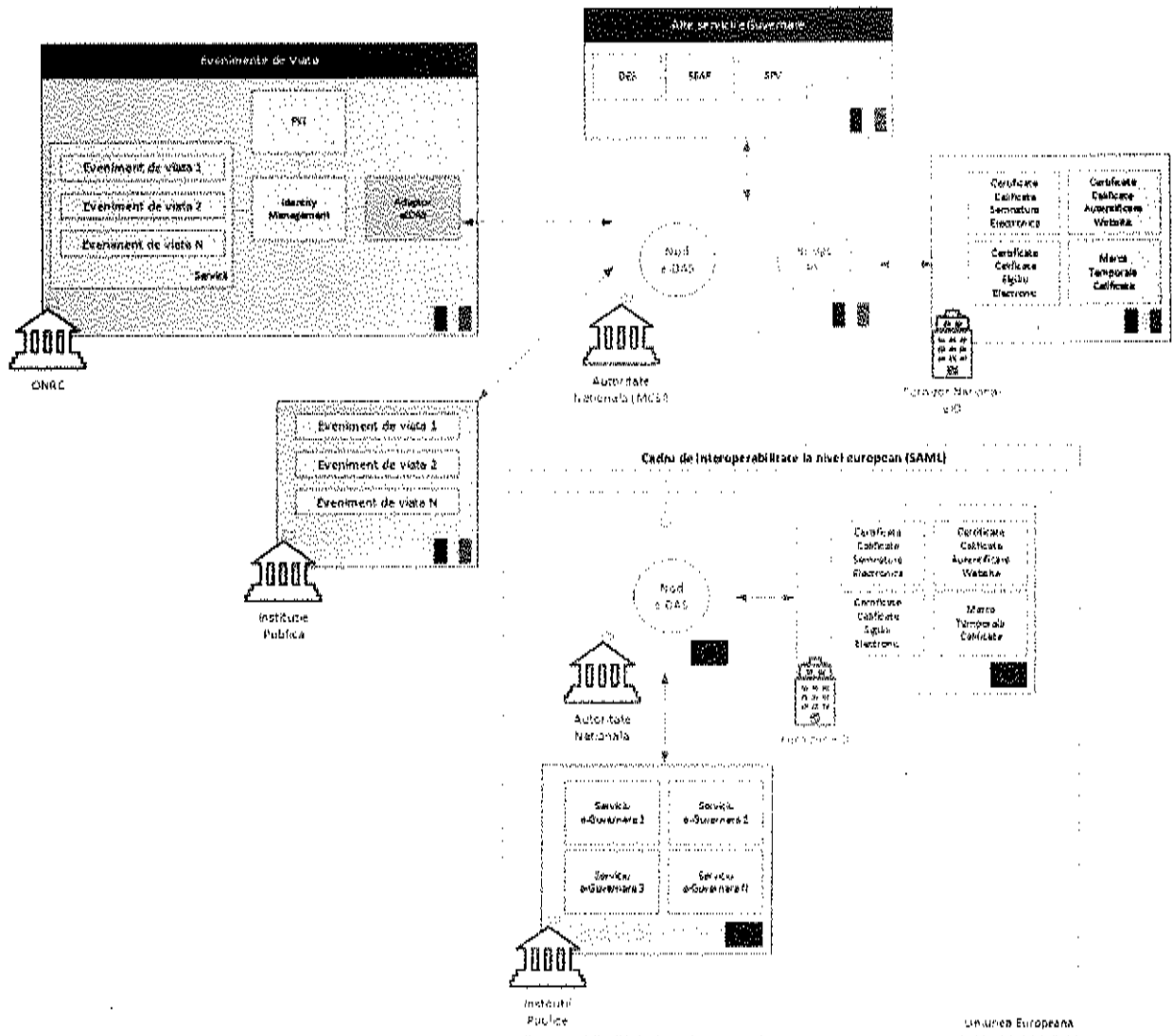
Regulamentul eIDAS asigură recunoaștere implicită a serviciilor de încredere la nivelul UE. Astfel, semnăturile electronice calificate create cu certificate digitale calificate emise de un Furnizor de servicii de încredere calificat au efectul juridic echivalent al unei semnături olografe și sunt recunoscute la nivelul tuturor statelor membre.

Interoperabilitatea dintre sistemele de identificare notificate de statele membre se realizează prin noduri (noduri eIDAS) ce reprezintă puncte de legătura care fac parte din arhitectura de interoperabilitate europeană pentru identificarea electronică. Un nod este implicat în identificarea transfrontalieră a persoanelor și are capacitatea să recunoască sau să transmită mai departe datele către alte noduri, prin faptul că face interoperabilitatea între mecanismele naționale de identificare electronică ale unui stat membru și serviciile de e-guvernare ale altor state membre. Cu privire la identificarea electronică, sunt definite 3 niveluri de siguranță: scăzut, substanțial și ridicat. Statele membre trebuie să notifice Comisiei Europene sistemele de identificare electronică naționale, incluzând nivelurile de securitate și emitentul sau emitenții mijloacelor de identificare electronică din cadrul sistemului (furnizori eID).

Sistemul denumit "nod" facilitează prin identificare și rutare, comunicarea bidirecțională dintre toate sistemele funcționale din cadrul arhitecturii dedicate asigurării serviciilor de e-Guvernare, oferind suport pentru interoperabilitatea cu celelalte sisteme similare din spațiul Uniunii Europene.

Totodată, nodul permite asigurarea punților de identificare (bridge), dintre toate sistemele care operează bidirecțional în cadrul arhitecturii informaționale ce stă la baza operaționalizării evenimentelor de viață, corelate cu identificarea bazată pe infrastructuri de chei publice (PKI), cu alte mecanisme de identificare acceptate în aplicațiile de e-guvernare și cu aplicațiile operaționale.



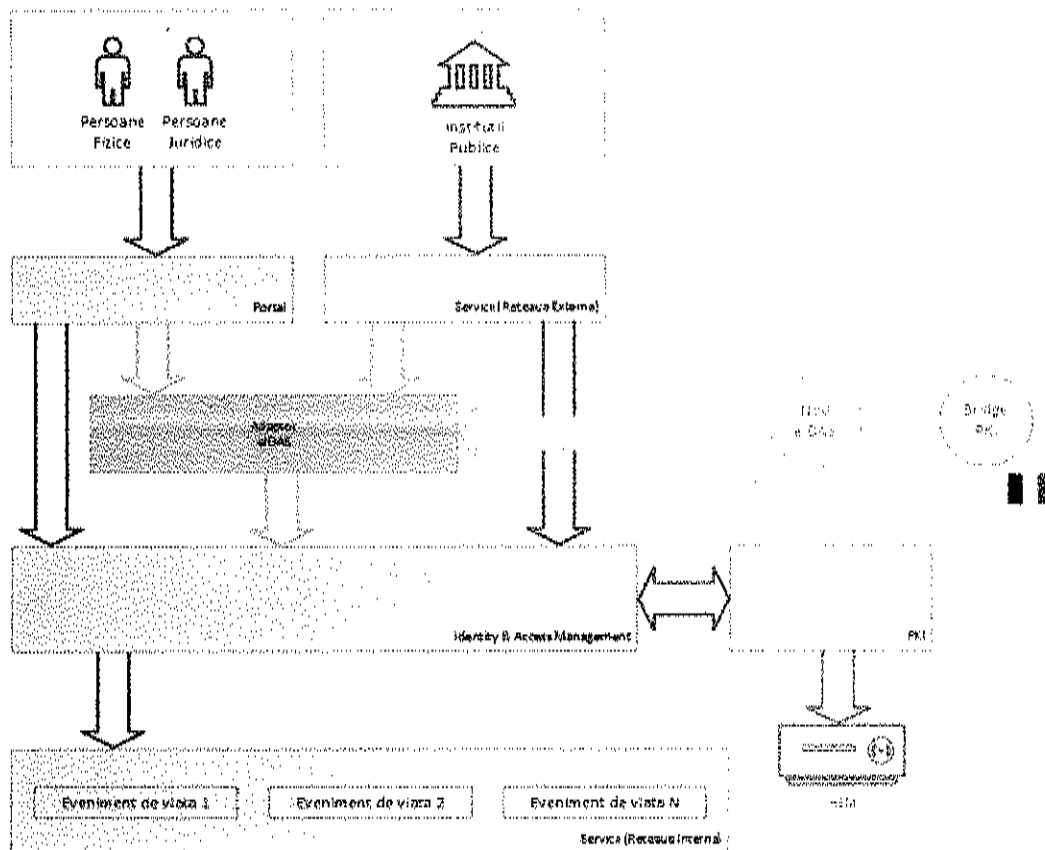


Figură: Interconectarea sistemului informatic integrat la nodul național eIDAS

Sistemul informatic integrat va trebui să implementeze un adaptor eIDAS ce va fi responsabil cu integrarea dintre propria infrastructură de PKI și de gestiune a identității și accesului și nodul național eIDAS. Adaptorul eIDAS va acționa ca o punte între propria infrastructură de gestiune a identității, de PKI (gestiune certificate), serviciile electronice (ca și aplicații de business) și cetățeni, instituții sau utilizatori proprii ONRC ce se vor autentifica și autoriza pentru acces securizat la serviciile electronice.

Din motive operaționale, sistemul informatic integrat trebuie să permită gestionarea identităților precum și implementarea Single Sign-On (SSO), în mod alternativ, utilizând exclusiv componentele de Identity & Access Management și PKI, având posibilitatea ulterioară de a cupla adaptorul eIDAS la sistem în vederea integrării cu nodul național eIDAS gestionat de către MTIC.

[Handwritten signatures]



Figură: Adaptorul eIDAS integrat la nivelul sistemului informatic integrat

Adaptorul eIDAS va trebui să implementeze la nivelul sistemului integrat următoarele funcționalități de bază:

- *Furnizor de identitate*: validare identitate utilizator, gestionarea nivelului de încredere conform nivelurilor eIDAS, federalizarea identității și suport pentru asigurarea Single Sign-On (SSO) cu serviciile electronice puse la dispoziție de către sistem;
- *Furnizor de semnătură electronică*: integrare cu infrastructura PKI și gestionarea cheilor într-un depozit securizat tip HSM. Utilizatorii identificați vor putea avea asociate unul sau mai multe certificate digitale pentru semnarea electronică a documentelor. Totodată, va trebui permisă semnarea documentelor utilizând interfețe tip web-based (remote signing), prin intermediul unui Web API disponibil;
- *Suport pentru integrare*: suport pentru SAML și OAuth/OpenID pentru implementarea Web SSO. Suport cel puțin pentru standardele PDF Advanced Electronic Signature (PAdES) și PKCS #1.

3.7 Securitatea sistemului

Informațiile gestionate în cadrul ONRC sunt informații publice, rolul instituțional al ONRC fiind tocmai acela de asigurare a publicității acestor informații. Există însă în cadrul sistemului informatic al ONRC și informații cu caracter personal aferente în general persoanelor cu calitate legală în cadrul profesionistului, care în

general nu sunt destinate publicității (CNP, adresă completă de domiciliu etc.). Având în vedere faptul că sistemul informatic propus are și componente cu expunere în internet (componenta de portal, serviciul web pentru interoperabilitate cu sisteme informatice externe și serviciul de schimb electronic de date), conform clasificării anterioare el se încadrează în categoria sistemelor informatice cu risc **MARE**.

Toate componentele funcționale ale sistemului informatic vor fi protejate de infrastructura dedicată de securitate prevăzută, astfel încât să fie asigurată o protecție avansată începând cu perimetrul rețelei (DMZ) și terminând cu terminalele de lucru ale utilizatorilor. Partea de securitate este compusă din echipamente de tip next generation firewall cu capabilități avansate de protecție împotriva atacurilor cibernetice, de soluții dedicate de protecție a email-urilor, împotriva atacurilor de tip Denial-of-Service (DoS) sau Web application firewall (WAF).

Componenta portal este principala interfață cu utilizatorii (persoane fizice și juridice) și este expus în internet, la fel ca și componenta de integrare (interoperabilitate) cu sisteme informatice externe și schimb electronic de date. Restul componentelor nu sunt expuse către exterior în internet, accesul la toate acestea realizându-se pentru utilizatori autentificați și totodată autorizați la nivelul componentei de gestiune acces și identitate utilizatori din cadrul proiectului. Datele operaționale nu pot fi accesate direct de către utilizatori, ci doar prin intermediul instrumentelor / aplicațiilor asociate prelucrării acestora, iar accesul la aceste instrumente / aplicații este permis doar utilizatorilor autentificați și autorizați în consecință.


Sistemul informatic permite utilizatorilor folosirea de certificate digitale la nivelul componentei PKI, aceasta fiind integrată cu componenta de gestiune acces și identitate utilizatori, astfel încât să poată fi implementat și Single-Sign-On la nivelul componentelor aplicative, prin utilizarea ori a certificatului digital la autentificare ori a unei combinații de tip utilizator / parolă. Totodată, sistemul este prevăzut și cu o componentă specializată pentru integrarea cu nodul național eIDAS gestionat de către MTIC, astfel încât să poată prelua solicitări de servicii electronice respectând caracteristicile tehnice definite la nivelul standardului de reglementare identități electronice și niveluri de încredere pentru servicii electronice.

3.7.1 Securitatea rețelei

Din punct de vedere al securității rețelei, noul sistem va fi inclus în zonele de securitate definite deja în cadrul organizației. Fiecare nod de procesare va fi plasat în zona de securitate corespunzătoare, în funcție de rolul pe care îl joacă în arhitectura sistemului. Echipamentele de securitate a comunicațiilor vor include regulile de securitate pentru nodurile noului sistem.

3.7.2 Securitatea datelor

Accesul la datele din sistem va fi permis numai utilizatorilor autentificați și autorizați și numai prin intermediul instanțelor de aplicații. Accesul la bazele de date va fi permis doar utilizatorilor autentificați și autorizați în acest sens, gestiunea accesului fiind implementată la nivelul componentei de gestiune identități și acces utilizatori.



3.7.3 Securitatea aplicațiilor

Fiecare aplicație a noului sistem va asigura protecția față de accesul neautorizat, prin mecanisme care permit autentificarea unică și autorizarea utilizatorilor pe baza de roluri și permisiuni. Aplicațiile vor permite accesul partajat la resurse, prin restricționarea accesului la nivelul modulelor funcționale.

Prin modulele funcționale ale aplicațiilor, utilizatorii vor avea vizibilitatea doar asupra datelor stocate în sursele de date la care au acces.

Aplicațiile vor asigura monitorizarea interacțiunii utilizatorului cu interfața grafică prin mecanisme de tip log și audit.

Echipamentele cu funcționalitate NetFlow sau IPFIX trebuie integrate în soluția existentă a Beneficiarului pentru a asigura managementul unitar fără a necesita costuri suplimentare din partea Beneficiarului.

Aplicațiile vor permite limitarea funcționalităților disponibile unui utilizator, în conformitate cu drepturile asociate.

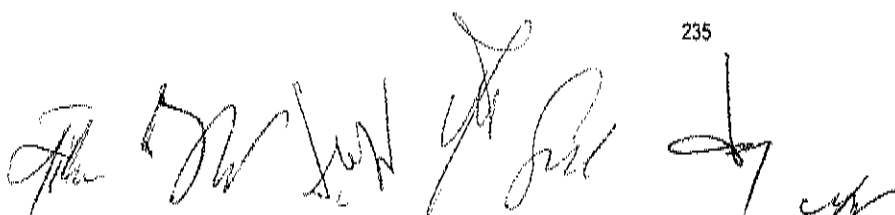
Trebuie inclusă o componentă care va permite operatorilor să aibă acces la informații complete de vizibilitate la nivelul fluxurilor de date dintre componentele diferitelor aplicații care rulează pe infrastructura din centrul de date pentru a putea înțelege modul în care aplicațiile comunică între ele și a crea o hartă cu interdependențele existente la nivelul aplicațiilor, precum și a putea identifica tipare de trafic atipice care pot semnaliza fie o eroare în configurarea politicilor de acces și securitate la nivelul infrastructurii de rețea, fie un potențial atac informatic.

Această componentă va permite construirea și simularea unor politici de acces și comunicare de tip whitelist în mod automat la nivelul rețelei din centrul de date. Platforma va avea un mecanism prin care politica definită pe baza datelor colectate să poată fi aplicată la nivelul mașinilor care rulează în centrul de date, indiferent de tipul acestora (virtuale, fizice) și de aplicația care rulează pe mașina respectivă. Prin intermediul acestei funcționalități platforma va permite segmentarea aplicațiilor la nivelul centrului de date având la bază informații în timp real despre funcționarea rețelei.

Componenta de vizibilitate va oferi informații complete despre componentele diferitelor aplicații din centrul de date, modul în care aceste componente comunică unele cu altele și interdependențele stabilite între aceste componente. Prin analizarea acestor informații platforma va fi capabilă să implementeze un model de politici de tip zero-trust la nivelul întregii rețele din centrul de date.

Componenta de vizibilitate trebuie să fie capabilă să analizeze în timp real toate comunicațiile realizate de toate componentele diferitelor aplicații la nivelul centrului de date. Colectarea datelor despre traficul realizat de diferitele componente ale aplicațiilor se va face folosind o serie de senzori software instalați la nivelul mașinilor virtuale sau fizice din centrul de date. Caracteristicile minimale ale acestor senzori sunt descrise mai jos:

- Senzorii trebuie să poată fi instalați atât manual cât și automat, folosind utilitare de management centralizat și automatizare (Puppet, Chef, Ansible). Ulterior instalării toate actualizările la nivelul senzorilor vor putea fi făcute din intermediul platformei de vizibilitate.
- Senzorii pot fi configurați pentru a nu consuma mai mult de un anumit procent de resurse de CPU la nivelul mașinii virtuale pe care rulează. Utilizarea suplimentară a resurselor de procesor indusă de sensor la nivelul mașinii virtuale pe care acesta rulează trebuie să fie sub 5%.



- Overhead-ul de trafic de rețea general de senzori trebuie să fie sub 1% din traficul total al rețelei de centru de date.
- Senzorii vor transmite către platforma de vizibilitate informații complete despre traficul general de aplicații care să permită analiza comportamentului aplicațiilor precum și monitorizarea deviațiilor de la comportamentul normal.
- Senzorii vor colecta header-ul tuturor pachetelor generate de aplicațiile de pe mașinile pe care rulează acești senzori, precum și informații de context despre fluxurile de trafic. Colectarea acestor informații se poate face și în situația în care payload-ul pachetului este captat. Senzorul nu va colecta informații din payload. Colectarea fluxurilor de trafic se va face fără sampling, pentru a nu pierde informații relevante.

Datele colectate prin intermediul senzorilor vor fi colectate de platforma centrală a componentei de vizibilitate. Platforma va stoca datele colectate de senzori și le va analiza folosind algoritmi complecși (inclusiv analiza comportamentală și algoritmi de tip machine-learning nesupravegheați) pentru a genera informații relevante despre aplicațiile din centrul de date. Platforma va folosi datele colectate și va interacționa cu senzorii instalați la nivelul mașinilor din centrul de date pentru a asigura următoarele funcționalități

1. Vizibilitate la nivelul aplicațiilor

Platforma va permite operatorilor să înțeleagă modul în care aplicațiile din centrul de date funcționează și interacționează, pentru a putea opera cu succes mediu informatic complex și posibilitatea definirii unor politici de segmentare a aplicațiilor din centrul de date. Este necesară monitorizarea continuă a aplicațiilor din centrul de date pentru a avea disponibilă în orice moment o hartă a aplicațiilor critice și a modului în care acestea interacționează. Această hartă va putea fi folosită pentru a permite evoluția în timp a mediului informatic, o dată cu dispariția sau transformarea unor aplicații existente și apariția de aplicații noi.

Platforma va realiza, folosind algoritmi interni, o categorisire a aplicațiilor în grupuri precum și identificarea automată a tiparelor de trafic între aceste grupuri de aplicații, precum și interdependențele între acestea.

Operatorii și administratorii sistemelor informatice vor putea să definească grupuri sau clustere de aplicații și să realizeze, în mod automat, grafice privind modul de comunicație între aceste grupuri de aplicații. În acest fel administratorii sistemului vor înțelege cu exactitate relațiile dintre aplicațiile din centrul de date și modul în care acestea comunică (porturi expuse, porturi apelate, etc).

Platforma va permite și integrarea de informații din surse externe (în mod minimă: load-balancer-e și CMDB) pentru a avea o imagine completă asupra modului în care diferitele aplicații comunică.

2. Vizualizarea și explorarea fluxurilor de comunicații

Platforma va permite explorarea tuturor fluxurilor de comunicații de la nivelul centrului de date prin intermediul unui motor de căutare care permite analizarea unui număr foarte mare de fluxuri de date (milioane de fluxuri) în timp foarte scurt (sub o secundă). Motorul de căutare va avea funcționalități avansate de filtrare a rezultatelor unei căutări precum și posibilitatea de a căuta informații folosind un modul de căutare vizual (funcționalități de tip drill-down pe elemente vizuale de trafic).

3. Simulare de politici de acces

Datele colectate de platforma vor putea fi folosite pentru a simula impactul pe care o politică de acces modificată o poate avea asupra traficului real din centrul de date. În felul acesta operatorii și administratorii sistemului informatic vor putea simula politicile de acces într-un mediu simulat,

folosind date istorice sau date in timp real, inaintea implementarii acestora in productie, pentru a nu afecta functionarea normala a aplicatiilor de productie si disponibilitatea acestora.

4. Generare automata de politici de acces si segmentarea aplicatiilor

Datele colectate de platforma cu privire la modul de comunicare intre aplicatiile din centrul de date va putea fi folosit pentru crearea in mod automat a unei politici de acces de tip whitelist care sa permita in mod efficient segmentarea comunicatiilor intre aplicatiilor din centrul de date. Platforma trebuie sa permita exportarea politicii de acces definite in mod automat intr-un format programabil (JSON, XML sau YAML).

5. Implementarea de politici de microsegmentare prin intermediul senzilor din sistemele de operare gazda

Platforma va putea distribui in mod automat, prin intermediul senzilor, reguli pentru firewall-ul sistemului de operare gazda al masinilor virtuale sau fizice monitorizate; pentru a putea realiza un model de micro-segmentare extrem de granular.

6. Implementarea de politici de microsegmentare prin intermediul senzilor din sistemele de operare gazda

Platforma va putea distribui in mod automat, prin intermediul senzilor, reguli pentru firewall-ul sistemului de operare gazda al masinilor virtuale sau fizice monitorizate pentru a putea realiza un model de micro-segmentare extrem de granular.

7. Identificarea unor comportamente deviate ale infrastructurii monitorizate

Sistemul va fi capabil sa detecteze in mod automat urmatoarele deviatii la nivelul fiecarui sistem de operare monitorizat (fizic, virtual sau cloud based):

- Inventarierea proceselor care ruleaza pe server, realizarea unui arbore al modului de executie al tuturor proceselor, identificarea de executii de procese care au potential malitios.
- Detectarea vulnerabilitatilor software prin monitorizarea in mod continuu a pachetelor si software-urilor instalate pe sistem precum si versiunile acestora pentru a identifica pachete sau software afectate de vulnerabilitati cunoscute.
- Detectarea situatiilor in care se incearca exfiltrarea datelor de pe sistemele monitorizate.

Platforma va permite integrarea cu alte sisteme prin intermediul de API-uri deschise, se va folosi o tehnologie API de tip REST sau echivalent. Mai mult dezvoltatorii software interni vor putea utiliza datele stocate de platforma si vor putea dezvolta propriile aplicatii folosind limbajele de programare Python sau Scala.

Platforma va fi ofertata pentru un numar de minim 200 de senzori.

3.7.4 Securitate fizică

Rack-urile cu echipamente vor fi prevăzute cu încuietori mecanice, pentru o protecție suplimentară. Pentru asigurarea protecției fizice a echipamentelor și pentru controlul accesului, în cadrul fiecărui centru de date



se va implementa o soluție de protecție antiefracție, precum și o soluție de control al accesului. Pentru protecția la incendiu se va instala un sistem de avertizare la început de incendiu, precum și un sistem de stingere cu gaz inert. Pentru asigurarea ventilației și a răcirii echipamentelor se va instala un sistem de răcire special, redundant. A se vedea secțiunea "Cerinte privind amenajarea și dotarea centrelor de date".

3.7.5 Confidențialitatea datelor

Accesul la datele stocate în bazele de date și în sistemele de fișiere partajate gestionate la nivelul echipamentelor de stocare se va putea realiza numai prin instanțe de servicii de aplicație, care vor accesa datele direct. Accesul la date va fi autorizat și auditat în mod riguros.

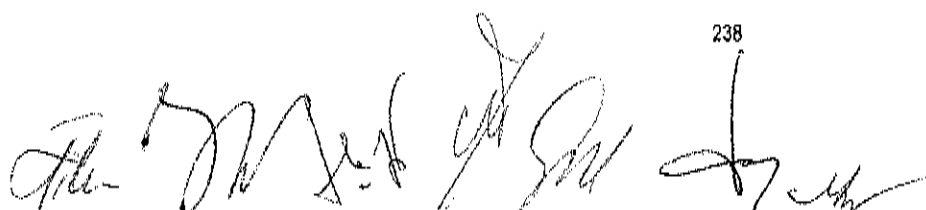
3.8 Capacitate și dimensionare date

- Componentele software prevăzute în proiect vor fi dimensionate / licențiate în funcție de cerințele specifice aferente fiecărei componente în parte din prezenta documentație cu respectarea următoarelor specificații minime aferente mediului de producție:

- o Componenta portal: minimum 10 instanțe (servere), fiecare instanță acoperind cel puțin 8 core-uri fizice;
- o Componenta server web: minimum 6 instanțe (servere), fiecare instanță acoperind cel puțin 4 core-uri fizice;
- o Componenta server de aplicații: minimum 36 de instanțe (servere), fiecare instanță acoperind cel puțin 6 core-uri fizice;
- o Componenta baza de date: minimum 20 de instanțe (servere), fiecare instanță acoperind cel puțin 8 core-uri fizice;
- o Componenta replicare date: minimum 20 de instanțe, fiecare instanță acoperind cel puțin 8 core-uri fizice;
- o Componenta integrare și schimb de mesaje: minimum 6 instanțe (servere), fiecare instanță acoperind cel puțin 4 core-uri fizice;
- o Componenta procese de business: minimum 4 instanțe (servere), fiecare instanță acoperind cel puțin 4 core-uri fizice;
- o Componenta ETL: minimum 4 instanțe (servere), fiecare instanță acoperind cel puțin 4 core-uri fizice;
- o Componenta raportare și analiza: minimum 150 utilizatori;
- o Componenta gestiune identități și acces utilizatori: minimum 2500 utilizatori;
- o Componenta integrare eIDAS: minimum 2 instanțe;
- o Componenta PKI: minimum 2500 utilizatori;
- o Componenta semnare electronica: minimum 2500 utilizatori;

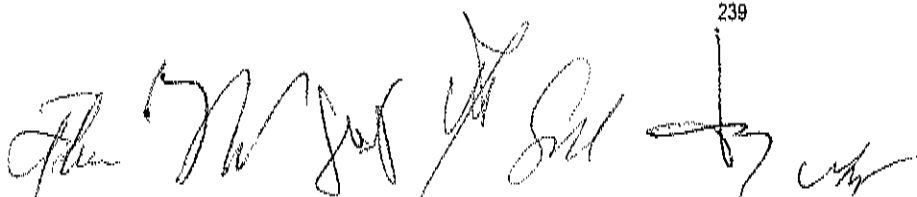
Ofertantul va include orice alte componente software sunt necesare pentru buna funcționare a celor livrate, de exemplu servere de aplicație, baze de date suplimentare etc.

238



Alocarea de resurse solicitata prin prezenta documentație este una minimală ce pleacă de la arhitectura sistemului actual și posibilitățile ulterioare de creștere a utilizării, ofertantul având posibilitatea de a propune o alocare suplimentară de resurse plecând de la cantitățile minimale prevăzute în documentație și obligația ca soluția furnizată să îndeplinească cerințele de performanță din aceasta documentație tehnică;

- Sistemul va fi dimensionat având în vedere următoarele date determinate de situația existentă și prognoza de creștere în următorii 5 ani:
 - Număr de utilizatori interni ai sistemului integrat: 2500;
 - Număr de utilizatori externi la nivel de portal: 500.000;
 - Număr de utilizatori interni pentru raportare și analiză: 150;
 - Număr utilizatori interni pentru call-center: 50;
 - Număr utilizatori interni pentru testare: 150;
- Volum de date:
 - Volumul actual al datelor din bazele de date RC, RL, BPI, REG, TAX și nomenclatoare: 7 TB;
 - Volumul datelor stocate în Sistemul de Arhivare Electronica: 20 TB;
 - Volumul metadatelor din Sistemul de Arhivare Electronica: 0,6 TB;
 - Numărul de file de documente scanate stocate în Sistemul de Arhivare Electronica: 137 milioane; toate documentele sunt într-un format ce nu permit căutări;
 - Numărul de file de documente scanate adăugate anual: 20 milioane;
- **Criterii de performanță/timpuri de răspuns:**
 - La dimensionarea componentelor hardware și software ale soluției se va avea în vedere asigurarea premiselor pentru obținerea unor criterii de performanță care să asigure eficiența activităților derulate de utilizatori. Astfel, **timpii de răspuns ai sistemului informatic la solicitări standard de acces la informație sau de scriere de informații nu vor depăși câteva secunde (maxim 3 secunde), la o încărcare maximă a sistemului** (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).
 - Pentru obținerea rapoartelor operaționale zilnice, timpii de răspuns nu vor depăși 20 de secunde. Pentru rapoarte statistice și de istoric, se vor asigura mijloace tehnice pentru minimizarea timpului de așteptare al utilizatorilor (de exemplu segmentarea cantității de date returnate și popularea ecranului cu primul set de date fără a aștepta transmiterea întregului set de date etc.);
 - Cerințele hardware și software din prezentul document vor fi considerate cerințe minimale. **Astfel, este responsabilitatea ofertantului să dimensioneze soluția din punct de vedere hardware și software astfel încât să fie respectate criteriile de performanță mai sus menționate în condițiile de încărcare și volum descrise în prezentul document;**



Ofertantul câștigător este responsabil atât cu livrarea, instalarea și configurarea echipamentelor hardware în site-uri (centre de date), a sistemelor software de bază dar și cu dezvoltarea componentelor personalizate ale sistemului.

Ofertantul câștigător va fi responsabil cu toate activitățile necesare pentru punerea în producție a sistemului incluzând: analiză detaliată, proiectare detaliată, dezvoltare de cod, testare unitară, testare de integrare, testare pentru punerea în producție, instalarea și configurarea pentru punerea în producție, migrarea datelor, sprijin pentru Beneficiar în vederea punerii în producție, garanție, management de proiect.

Codul sursă pentru toate aplicațiile dezvoltate și componentele noi dezvoltate în cadrul sistemului va fi predat către ONRC și va deveni proprietatea Beneficiarului.

Ofertantul câștigător va fi responsabil cu toate activitățile necesare pentru instalarea, configurarea și punerea în producție pentru toate componentele sistemului.

Nicio componentă software din cele oferite nu trebuie să aibă vreo limitare 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 nici alte limitări de licențiere sau de altă natură care să prevină folosirea acesteia în scopul pentru care a fost achiziționată.

În cazul în care echipamentele componente ale soluției tehnice vor fi furnizate de mai mulți producători, va fi asigurată integritatea și funcționalitatea întregului sistem. Funcționalitatea componentelor sistemului nu va fi în 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 sediile autorității contractante, conform anexa.

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

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

3.9 Cerințe de implementare

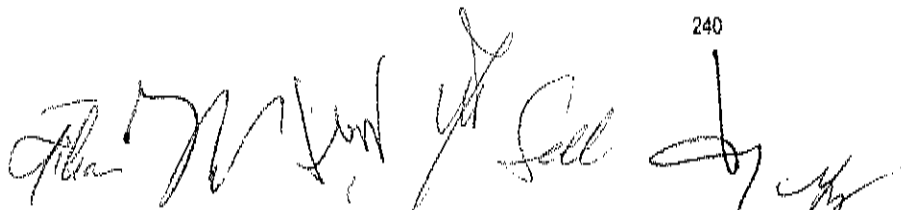
3.9.1 Servicii de management de proiect

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

Durata de implementare a sistemului informatic (de la semnarea contractului până la semnarea acceptanței finale) va fi de maxim 18 de luni de la data semnării contractului. Această perioadă include amenajarea camerei serverelor, livrarea, instalarea și punerea în funcțiune a echipamentelor precum și proiectarea, dezvoltarea, migrarea, testarea, instruirea și acceptanța sistemului.

Ofertanții vor avea în vedere următoarele termene maxime pentru finalizarea activităților de implementare:

240



- Amenajare spațiu tehnic Centru de date principal și Centru de date secundar – 2 luni și 26 zile de la semnarea contractului;
- Analiza – 5 luni și 25 zile de la semnarea contractului;
- Proiectare – 7 luni și 27 zile de la semnarea contractului;
- Livrare și instalare infrastructură hardware și software mediu de testare și dezvoltare – 6 luni și 16 zile de la semnarea contractului;
- Livrare și instalare infrastructură hardware și software mediu de producție – 8 luni și 10 zile de la semnarea contractului;
- Dezvoltare / testare prestator – 1 an 4 luni și 3 zile de la semnarea contractului;
- Migrare date – 1 an și 25 zile de la semnarea contractului;
- Testare funcțională și de integrare – 1 an 4 luni și 3 zile de la semnarea contractului;
- Instruire administratori și utilizatori – 1 an 5 luni și 7 zile de la semnarea contractului;
- Punere în funcțiune sistem (inclusiv datele migrate/incărcate) și obținere acceptanță finală – 1 an 6 luni de la semnarea contractului.

Totodată, în planul de proiect se va avea în vedere realizarea următoarelor recepții:

1. Cantitative – prin intermediul cărora se livrează produsele hardware, pachetele software standard și livrabilele serviciilor prestate din punct de vedere cantitativ.
2. Calitative – prin intermediul cărora Beneficiarul verifica parametrii de calitate ai livrărilor cantitative. Acestea pot fi:
 - a. Recepții calitative parțiale – sunt recepții calitative ce privesc anumite componente și/sau servicii ce fac obiectul contractului de achiziție și care pot fi individualizate. Sunt acceptate recepții calitative parțiale pentru:
 - Livrarea și instalarea produselor hardware - în urma testelor de acceptanță a instalării produselor hardware
 - Livrarea și instalare pachetelor software de bază – în urma testelor de acceptanță a instalării pachetelor software de baza
 - Serviciile de analiză – în urma aprobării documentului de analiza
 - Serviciile de proiectare – în urma aprobării documentului de proiectare
 - Serviciile de amenajare a spațiului tehnic – în urma testelor de acceptanță aferente spațiului tehnic
 - Servicii de dezvoltare și testare – în urma testării funcționale și de performanță a sistemului
 - Servicii de migrare date - în urma acceptării raportului de migrare date
 - Serviciile de instruire – în urma acceptării serviciilor de instruire prestate
 - b. Recepție finală – care este realizată după finalizarea tuturor activităților proiectului și punerea în funcțiune a întregului sistem informatic.

Ofertantul are obligația să respecte următoarele termene maxime pentru realizarea recepțiilor calitative în cadrul proiectului:

Denumire produs/serviciu	Livrabile furnizate (minim)	Document recepție calitativă	Termen maxim de recepție calitativă (în ani, luni, zile de la semnarea contractului)
Amenajare spațiu tehnic pentru ambele centre de date	Proces verbal recepție cantitativă spațiu tehnic amenajat Raport privind amenajarea spațiului tehnic Scenarii de testare a spațiului tehnic	Proces verbal recepție calitativă spațiu tehnic	2 luni și 26 zile
Infrastructură hardware	Infrastructură hardware Raport instalare și configurare infrastructură hardware Scenarii de testare a infrastructurii hardware	Proces verbal recepție calitativă infrastructură hardware	3 luni și 23 zile respectiv 5 luni și 18 zile (mediu de testare și dezvoltare respectiv mediu de producție)
Produce software standard	Produce software standard Raport instalare și configurare produse software standard Scenarii de testare a produselor software standard	Proces verbal recepție calitativă produse software standard	6 luni și 16 zile respectiv 8 luni și 10 zile (mediu de testare și dezvoltare respectiv mediu de producție)
Servicii de analiza	Document analiză de business Scenarii de testare funcțională și de testare integrare	Proces verbal recepție calitativă servicii analiza	5 luni și 25 zile
Servicii de proiectare	Document proiectare detaliata Scenarii de testare non-funcțională Standarde de dezvoltare Arhitectura module/aplicatii Strategia de integrare	Proces verbal recepție calitativă servicii proiectare	7 luni și 27 zile
Servicii de dezvoltare și testare	Kit de instalare Procedura de instalare	Proces verbal recepție calitativă servicii dezvoltare și testare	1 an 4 luni și 3 zile

	Manuale de utilizare și instalare Ghid de testare funcțională și de testare integrare Rezultatele testelor interne ale Prestatorului și ale testerului extern		
Servicii de migrare	Rapoarte privind migrarea datelor	Proces verbal recepție calitativa servicii migrare	1 an și 25 zile
Servicii de instruire	Materiale instruire utilizatori Materiale instruire administratori Rapoarte privind participarea la cursurile de instruire	Proces verbal recepție calitativă servicii instruire	1 an 5 luni și 7 zile
Sistem informatic integrat	Raport de punere în funcțiune a sistemului informatic (GOLIVE) Codul sursa al aplicațiilor dezvoltate Procedura de compilare a codului sursa Rapoartele de monitorizare și control al proiectului Certificat de garanție pentru sistemul informatic	Proces verbal de recepție calitativă finală	1 an 6 luni

Având în vedere finanțarea contractului prin Proiectul intitulat "Sistem electronic integrat al ONRC consolidat și interoperabil destinat asigurării serviciilor de e-guvernare centrate pe evenimente de viață (ONRC v2.0)", SMIS 123634, durata contractului poate fi dimensionată astfel încât aceasta să se încadreze în durata, calendarul și termenii Contractului de finanțare nr. 6/2.3.1/04.04.2019, încheiat între Oficiul Național al Registrului Comerțului și Ministerul Fondurilor Europene, cu modificările ulterioare.

Livrabilele se predau beneficiarului pe baza de procese verbale de recepție cantitativă. Recepțiile calitative se realizează pe baza proceselor verbale de recepție calitativa aferente livrabililor menționate în tabelul de mai sus și a inspecțiilor / verificărilor realizate de către beneficiar în conformitate cu prevederile prezentului document.

Ofertanții au obligația de a evidenția toate milestone-urile și activitățile importante, duratele acestora și resursele ce vor fi alocate, în cadrul unui grafic de proiect ce va fi inclus în oferta tehnică.

3.9.1.1 Planificare, monitorizare și 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 furnizării livrabililor și ale acceptării acestora de către

Autoritatea Contractanta, responsabilitățile cu privire la fiecare activitate în parte, precum și persoanele responsabile din cadrul echipei de proiect pentru realizarea fiecărei activități.

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

- ședință lunara de evaluare a stadiului întregului proiect
- ședințe regulate de evaluare a diferitelor zone funcționale ale proiectului
- ședințe de evaluare la finalizarea unor etape de proiect
- ședințe de evaluare a riscului
- ședințe ad-hoc de rezolvare a unor probleme specifice

Aceste ședințe vor fi conduse de către managerul de Proiect, iar rezultatele ședințelor vor fi documentate în Minute de Ședință care vor fi păstrate în cadrul Dosarului de Proiect.

Ofertantul are obligația de a întocmi rapoarte lunare în care va detalia cel puțin următoarele:

- rezultate realizate, resurse utilizate în perioada de raportare, progresele înregistrate în derularea proiectului
- dificultăți întâmpinate în etapa respectivă și soluții aplicate pentru îndreptarea acestora
- recomandări, aspecte financiare, precum și planificarea activităților (acțiuni, riscuri, resurse, livrabile etc.) pentru perioada următoare

3.9.1.2 Raportarea

Ofertantul declarat câștigător trebuie să transmită Beneficiarului cel puțin următoarele rapoarte:

- Rapoarte periodice prezentate de către Managerul de Proiect către Comitetul de Conducere al proiectului
- Rapoarte de Excepție (rapoarte ad-hoc care vor fi elaborate ori de câte ori vor apare excepții de la activitățile planificate, excepții 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.

3.9.1.3 Metodologia de proiect

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

Ofertantul va detalia metodele și instrumentele folosite pentru:

- managementul proiectului
- monitorizarea evoluției proiectului
- managementul calității
- managementul riscurilor

- managementul schimbării
- managementul comunicării

Monitorizarea evoluției proiectului

Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanță care va fi utilizat în cadrul proiectului pentru recepțiile/acceptanțele parțiale și recepția/acceptanța finală. Se va prezenta planul împărțit pe etape precum și formularele aferente recepțiilor/acceptanțelor parțiale și recepțiilor/acceptanțelor finale.

Managementul calității

Calitatea în mediul de proiect se definește ca fiind totalitatea cerințelor de ordin tehnic, funcțional, a obiectivelor cantitative și calitative ale proiectului, precum și metodologia și procedurile de management de proiect stabilite la nivelul proiectului, care trebuie atinse și respectate pentru finalizarea cu succes a proiectului.

Ofertantul va avea în vedere cel puțin furnizarea următoarelor livrabile pe durata implementării:

- Livrabile de management (planuri, proceduri, rapoarte):
 - Echipa de proiect și Comitetul de conducere al proiectului;
 - Planul proiectului;
 - Rapoarte de monitorizare și control al proiectului;
- Livrabile tehnice ale proiectului:
 - Documentul de analiză de business – a proceselor existente și a celor care vor fi implementate;
 - Documentul de proiectare detaliată hardware/software – ce include arhitectura sistemului și aspectele non-funcționale;
 - Documentația tehnică a sistemului informatic (format electronic)
 - Scenarii de testare funcțională și non-funcțională (format electronic);
 - Echipamentele hardware și software standard contractate și livrate;
 - Documentul care certifică instalarea și configurarea echipamentelor hardware;
 - Documentul care certifică corectitudinea funcționalităților dezvoltate în cadrul sistemului informatic;
 - Documentul care certifică instalarea și configurarea finală a sistemului informatic (format electronic);
 - Documentul care certifică instruirea utilizatorilor sistemului informatic (format electronic);
 - Documentul care certifică instruirea personalului care va utiliza/administra echipamentele hardware și software;
 - Kitul de instalare a aplicațiilor dezvoltate (include release note și instrucțiuni de instalare)
 - Codul sursa al aplicațiilor dezvoltate, biblioteci, inclusiv fișierele de configurare din cadrul tuturor componentelor sistemului, atât pentru software-ul dezvoltat cât și pentru configurarea celorlalte componente hardware/software care sunt diferite de configurația standard de instalare; Codul sursa documentat al aplicațiilor până la nivel de clasa (Java), funcții și proceduri stocate;

- Materiale de instruire (format electronic);
- Manuale de utilizare/administrare/configurare ale sistemului informatic (format electronic);
- Proceduri de lucru cu / de administrare a sistemul(ui) informatic (format electronic);
- Procedura detaliata de instalare și configurare pentru fiecare aplicație (format electronic);
- Orice ce alte documente sau instrumente necesare pentru buna funcționare a sistemului;
- Certificate de garanție.

Cerințe minime de calitate pentru fiecare livrabil:

- pentru echipamente:
 - tip
 - cerințe tehnice
 - standarde
 - dimensiuni
 - consum energetic etc.
- pentru software:
 - cerințe funcționale
 - gradul de precizie
 - interoperabilitatea
 - respectarea cerințelor
 - securitatea
 - conformitatea
 - cerințe tehnice
 - cerințe de capacitate, timp de răspuns
- pentru servicii
 - cerințe, specialiști, activități
 - specificațiile livrabilelor rezultante

Procedura de management al calității va conține 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 propunerii tehnice 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 ședințe 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 și documentate în Registrul Riscurilor, împreună cu modul în care acestea pot fi ținute sub control. De asemenea, se vor prevedea măsuri de rezervă pentru

situația în care riscul devine activ. Registrul Riscurilor și planurile asociate pentru controlul acestor riscuri vor fi revăzute în mod regulat în timpul ședințelor 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. Managerul de Proiect al furnizorului va fi responsabil de actualizarea Registrului de Riscuri.

Furnizorul va fi responsabil pentru livrarea unui sistem informatic integrat și funcțional, care să includă toate funcționalitățile prevăzute și care să permită atingerea tuturor obiectivelor specifice ale proiectului, conform cerințelor din Caietul de Sarcini, prevederilor legale și obiectivelor stabilite de instituție în cadrul capitolului Obiective.

Furnizorul 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, furnizorul 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.

Ofertantul va prezenta procedura de management a riscurilor, registrul inițial al riscurilor care conține cele mai importante riscuri identificate de acesta și măsurile propuse de remediere, precum și formularele care vor fi utilizate în cadrul acestui proces pe durata contractului. Se vor identifica riscuri din categorii diferite, care necesită abordări diferite, inclusiv pe baza experienței proprii.

Managementul schimbării

În cadrul oricărui 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 derulării sale anumite procese de lucru, cerințe tehnice și funcționale sau priorități să se modifice. Este esențial ca în astfel de situații proiectul să se poată adapta acestor schimbări, iar aceasta poate însemna modificarea diferitelor planuri, specificații și livrabile ale proiectului pe durata implementării proiectului.

Toate aceste schimbări vor fi gestionate prin intermediul Procedurii de Management al Schimbării.

Schimbările 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.) și se vor stabili cele mai bune strategii pentru gestionarea lor. Schimbările care au implicații asupra livrabilelor proiectului vor fi documentate și supuse aprobării Comitetului de Conducere al proiectului.

Ofertantul va prezenta în cadrul propunerii tehnice și modalitatea de tratare a schimbărilor în cadrul contractului. Se va prezenta procedura de management al schimbărilor precum și formularele care vor fi utilizate în cadrul acestui proces pe durata contractului.

Managementul comunicării

Ofertantul trebuie să prezinte în cadrul proiectului modalitatea (metodologia) prin care se va realiza comunicarea între participanții la contract.

3.9.2 Servicii de implementare

3.9.2.1 Analiza

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

- formularul/formularele care trebuie să fie utilizate pentru fiecare livrabil
- descrierea conținutului fiecărui livrabil
- modul în care trebuie să fie interpretat conținutul livrabilelor

Echipa de analiză a Prestatorului trebuie să analizeze cerințele conform cadrului normativ, fluxurilor și proceselor operaționale, procedurilor de sistem și operaționale, sistemului de management al calității, controlului intern managerial, managementului riscurilor, managementului strategic și operațional, modificărilor legislative, cazuisticii solicitanților etc, împreună cu experții Beneficiarului pentru a înțelege corect nevoile proiectului înainte de proiectarea și dezvoltarea noilor funcționalități.

Sedintelor de analiza vor putea fi înregistrate audio, ca parte a întocmirii minutei sedintei. Minutele sedintelor vor fi întocmite în format editabil de reprezentanți ai Furnizorului și vor fi aprobate de Beneficiar.

Livrabilele de analiză includ descrierea componentelor care trebuie dezvoltate/adaptate. Livrabilele acestei etape sunt cel puțin următoarele:

- Document de analiză de business - cu specificațiile funcționale pentru componentele dezvoltate/adaptate.
- Planul de testare, incluzând cazuri și scenarii de testare funcționale și respectiv de integrare, pentru componentele dezvoltate/adaptate conform cerințelor din prezentul proiect.

Livrabilul poate fi supus adaptării în funcție de evoluția cadrului normativ, a fluxurilor și proceselor operaționale, procedurilor de sistem și operaționale, sistemului de management al calității, controlului intern managerial, managementului riscurilor, managementului strategic și operațional, modificărilor legislative, cazuisticii solicitanților, etc, cu condiția ca, în cazul în care modificarea survenită afectează o zonă funcțională deja documentată pentru care serviciile de implementare sunt în curs, să fie utilizată procedura de management al schimbării pentru gestionarea impactului asupra proiectului.

În vederea derulării etapelor de proiectare respectiv dezvoltare software, livrabilele mai sus menționate vor fi aprobate de către persoanele responsabile din cadrul ONRC.

3.9.2.2 Proiectarea software

Serviciile de proiectare software se vor realiza pe baza documentelor rezultate și aprobate în faza de analiză software și a cerințelor din documentația de atribuire. Etapa de proiectare va fi urmată de etapa de dezvoltare.

Livrabilele acestei etape sunt cel puțin: Documentul de proiectare detaliată – include Modelul funcțional și de date, Scenarii de testare funcțională și non-funcțională, Standarde de dezvoltare, Arhitectura module/aplicatii, Strategia de integrare.

În vederea derulării etapei de dezvoltare software, livrabilul menționat va fi aprobat de către persoanele responsabile din cadrul ONRC.

3.9.2.3 Dezvoltare software

Serviciile de dezvoltare software se vor realiza pe baza documentelor rezultate și aprobate în fazele de analiză și proiectare software. Aceste servicii includ dezvoltarea și integrarea efectivă a funcționalităților, conform specificațiilor aprobate în faza de analiză. Etapa de dezvoltare se va încheia cu testarea internă realizată de Furnizor, în vederea livrării către ONRC a funcționalităților dezvoltate în cadrul proiectului.

Livrabilele acestei etape sunt cel puțin următoarele:

- Codul sursa documentat al aplicației până la nivel de clasa (Java), funcții și proceduri stocate;
- Codul sursa al aplicațiilor dezvoltate, biblioteci, inclusiv fișierele de configurare din cadrul tuturor componentelor sistemului, atât pentru software-ul dezvoltat cât și pentru configurarea celorlalte componente hardware/software care sunt diferite de configurația standard de instalare;
- Codul sursa al aplicațiilor.
- Codul fișierelor de configurare;
- Rezultatele testelor Prestatorului;
- Procedura de compilare a codului sursa;
- Procedura detaliată de instalare și configurare pentru fiecare aplicație;
- Manuale de utilizare
- Manuale de administrare.

Înainte de predarea unui release nou (sau a unui patch) spre testare către ONRC, Prestatorul va realiza propria etapă de testare internă, ca parte a procedurilor sale de asigurare a calității.

3.9.2.4 Instalarea și configurarea soluției

Ofertantul va fi responsabil pentru realizarea soluției oferite asigurând:

- compatibilitate maximă cu soluția existentă;
- valorificarea infrastructurii existente;
- garantarea unei maxime disponibilități.

Ofertantul va asigura următoarele servicii:

Implementarea soluției

Implementarea subsistemelor/soluțiilor va cuprinde cel puțin următoarele faze/activități:

- transportul și manipularea componentelor hardware până la sediul beneficiarului, după caz;
- furnizarea cerințelor necesar a fi asigurate de beneficiar pentru instalarea în bune condiții;
- realizarea planului detaliat al activităților ce vor fi realizate și agrearea acestuia cu beneficiarul, în vederea evitării oricărei întreruperi în funcționarea aplicațiilor din producție;

- analiza cerințelor, pregătirea specificațiilor funcționale și validare de către beneficiar;
- proiectarea detaliată a soluțiilor solicitate și validare de către beneficiar. După validarea acestui document de către Beneficiar se va trece la executarea serviciilor necesare aferente;
- instalarea și configurarea tuturor produselor software, după caz;
- instalarea și configurarea tuturor echipamentelor în scopul implementării soluției, după caz;
- realizarea tuturor configurărilor necesare pentru asigurarea tuturor serviciilor solicitate;
- dezvoltarea soluției software;
- realizarea testării funcționale a soluției pe mediul de dezvoltare/testare;
- configurarea produselor software existente în scopul implementării soluțiilor, după caz;
- realizarea tuturor configurărilor necesare pentru asigurarea tuturor serviciilor solicitate;
- actualizarea configurațiilor ca urmare a unor modificări survenite pe cel puțin unul din sistemele din locațiile implementate;
- realizarea testării funcționale a sistemului implementat pe mediul de dezvoltare/testare la fiecare modificare de configurație;
- livrarea documentelor cu specificațiile pentru soluțiile implementate;
- livrarea procedurilor de lucru detaliate pentru serviciile implementate;
- livrarea procedurilor de back-up și restore, după caz.

Ofertantul va asigura serviciile de instalare / configurare în afara orelor programului de lucru ale ONRC, cel puțin pentru activitățile care implică oprirea/întreruperea sistemelor productive ale ONRC, reconfigurările aferente testării și orice alte configurări care implică sistemul aflat în producție.

Metodologia de implementare propusă trebuie să fie de tip iterativ.

Instalare / configurare subsisteme/soluții

Ofertantul va fi responsabil pentru realizarea subsistemelor/soluțiilor asigurând:

- compatibilitate cu soluția existentă;
- valorificarea infrastructurii existente;
- garantarea unei maxime disponibilități.

Serviciile de instalare/configurare vor cuprinde:

- instalare software aplicativ la nivel central și teritorial după caz;
- configurare și monitorizare.

3.9.2.5 Testarea și testele de acceptanță

Realizarea cu succes a testelor este condiție pentru obținerea acceptanței finale asupra soluțiilor livrate.

Planul de testare va fi propus de Furnizor și agreat de Beneficiar. **Beneficiarul va achiziționa serviciul de testare printr-o procedura de achiziție publică separată iar furnizorul respectiv va avea responsabilitatea implementării și rulării testelor din planul de testare aprobat de Beneficiar.**

Testele care vor fi efectuate de prestatorul extern de testare vor include, dar nu se vor limita la următoarele:

- Testare funcțională pe date relevante – intra în responsabilitatea beneficiarului și furnizorul va asigura suportul pe durata testării
- Testare de performanță (timp de răspuns corespunzător profilului de utilizator) – intra în responsabilitatea beneficiarului și furnizorul va asigura suportul pe durata testării
- Teste de stres (volum de date, număr de utilizatori concurenți) – intra în responsabilitatea beneficiarului și furnizorul va asigura suportul pe durata testării
- Testare de integrare – intra în responsabilitatea beneficiarului și furnizorul va asigura suportul pe durata testării
- Testare software automatizată – intra în responsabilitatea beneficiarului și furnizorul va asigura suportul pe durata testării
- Testare de securitate a întregului sistem (cel puțin 2 iterații până la punerea în funcțiune a întregului sistem integrat) – intra în responsabilitatea beneficiarului și furnizorul va asigura suportul pe durata testării
- Orice alte teste relevante care cresc gradul de satisfacție a utilizatorului final (ergonomia interfeței cu utilizatorul, evaluarea utilizabilității, personalizarea, confidențialitatea, securitatea datelor, reducerea duplicării activităților, suport tehnic, instruire, etc.)

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

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

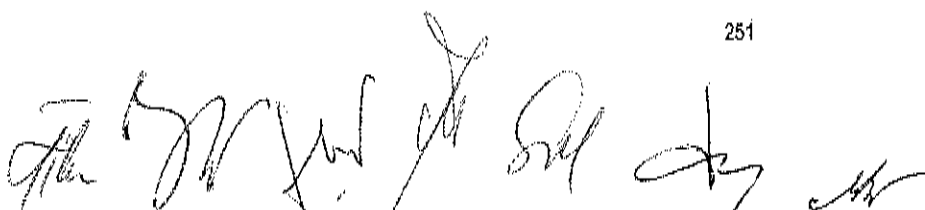
Beneficiarul (cu asistența Prestatorului) va rula toate scenariile pentru testele de acceptanță ale componentei livrate. Testele de acceptanță se vor derula în conformitate cu Planul de Testare.

3.9.2.6 Intrarea în producție

Ofertanții trebuie să prezinte planul care va fi utilizat la trecerea în producție a sistemului. Totodată, trebuie avute în vedere și activitățile de import / migrare conținut din sistemele productive existente astfel încât la intrarea în producție, sistemul să fie pe deplin funcțional.

Planul prezentat trebuie să țină cont de legăturile logice între subsisteme astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activităților zilnice a angajaților Beneficiarului.

3.9.3 Servicii de mentenanță, garanție și suport



Prestatorul va asigura garanția de minimum 36 luni de la punerea în funcțiune a sistemului pentru toate funcționalitățile acestuia, care trebuie să rămână minime pe întreaga perioadă de garanție.

Pentru infrastructura hardware, perioada minimă de garanție solicitată va fi de asemenea de minimum 36 luni de la livrarea echipamentelor.

Prestatorul va include în ofertă serviciile de mentenanță de la producători pentru tot software-ul livrat aferent tuturor mediilor (producție, test, dezvoltare etc.), pentru 12 luni de la acceptanța calitativă a acestora.

Toate bunurile livrate vor fi noi, neutilizate și dintre cele mai recente sau actuale modele și vor încorpora toate îmbunătățirile recente în design și materiale. Cele mai recente sau actuale modele și toate îmbunătățirile recente încorporate în design și materiale sunt cele disponibile în perioada care începe cu 6 luni înainte și până la începerea livrării la fața locului pentru fiecare categorie de articole. Prestatorul va demonstra cele menționate mai sus printr-un certificat al producătorului care indică data producției pentru fiecare categorie de articole.

În perioada de garanție, Prestatorul se obligă să asigure constatarea defecțiunilor hardware și remedierea defectelor on-site.

Defecte hardware

Termenul de răspuns la solicitări este de maxim 1 oră de la data și ora reclamării acesteia de către beneficiar, iar termenul de remediere pentru defecte ale infrastructurii hardware este de maxim 6 ore de la data și ora reclamării acesteia de către beneficiar, în cazul în care disfuncționalitatea blochează accesul utilizatorilor externi ONRC (de exemplu portalul de servicii electronice și serviciile de schimb de date) și de maxim 15 ore în cazul în care defectele afectează sisteme cu impact strict intern în cadrul ONRC.

Defecte software

Pe durata garanției se va asigura și rezolvarea defectelor soluției software implementate.

Timpii de rezolvare sunt definiți mai jos în funcție de gravitatea incidentului apărut:

Nivel Criticitate	Timp de răspuns	Timp soluționare temporară	Timp soluționare finală
Critic	1 oră	6 ore	15 ore
Mediu	6 ore	15 ore	30 ore
Minor	15 ore	45 ore	80 ore

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 funcționalități 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.

Ofertantul are obligația de a asigura serviciile de suport și garanție de luni până vineri/zile de lucru nelucratoare declarate ca fiind lucratoare în sistemul administrației publice, în intervalul orar 8-18 și sâmbăta-duminică/ la cerere pentru tipurile de incidente Critice. Prin ore / zile se înțelege ore lucrătoare / zile lucrătoare.

Depășirile timpilor de răspuns/soluționare 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 depășirea termenului de răspuns și a termenului de remediere aferente defectelor hardware ce afectează utilizatorii externi ai ONRC, se vor aplica 3 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de remediere a defectelor hardware care afectează sistemele cu impact intern în cadrul ONRC se vor aplica 2 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare aferente defectelor software critice, se vor aplica 3 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare a defectelor software medii se vor aplica 2 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare a defectelor software minore se va aplica 1 punct de penalizare pentru fiecare oră de depășire a termenului.

Un punct de penalizare valorează 0,0001 % din valoarea contractului.

Garanția se va asigura fără costuri suplimentare din partea ONRC.

Remedierea defectelor hardware se va face la sediile 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 situația în care este necesară transportarea echipamentelor în afara sediilor ONRC, toate mijloacele de stocare a datelor vor fi reținute de către beneficiar (Hard-discurile vor fi scoase din echipamente și păstrate la sediul ONRC).
- La finalizarea fiecărei intervenții în cadrul perioadei de garanție se va întocmi o fișă de intervenție care va conține următoarele detalii: data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției (reparație/inlocuire), durata de intervenție și confirmarea recepției prin semnăturile Prestatorului și beneficiarului.
- Perioada de garanție se va majora cu timpul de nefuncționare al echipamentelor/subsistemelor informatice în intervalul de reparare a acestora.

Pe durata mentenanței se va asigura rezolvarea incidentelor soluției software implementate.

Timpii de rezolvare sunt definiți mai jos în funcție de gravitatea incidentului apărut:



Handwritten signatures and a stamp. The stamp is a rectangular box containing the number 253.

Nivel Criticitate	Timp de răspuns	Timp soluționare temporară	Timp soluționare finală
Critic	1 oră	3 ore	6 ore
Mediu	3 ore	6 ore	12 ore
Minor	6 ore	12 ore	24 ore

Tipurile incidentelor:

- Critic:** una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate, iar impactul acestui incident duce la imposibilitatea utilizării sistemului.
Pentru acest tip de incident care au ca efect oprirea funcționării sistemelor și/sau activității sau serviciilor instituției, ofertantul va oferi asistență permanentă, 24/7.
- Mediu:** impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor funcționalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.
- Minor:** impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.

Ofertantul are obligația de a asigura serviciile de mentenanță 24/7, astfel: de luni până vineri/ zile de lucru nelucratoare declarate ca fiind lucratoare în sistemul administrației publice, în intervalul orar 8-18 și pentru zilele de sâmbătă, duminică și sărbători legale în intervalul orar 9-13.

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

- Pentru depășirea termenului de răspuns și a termenului de soluționare aferente defectelor software critice, se vor aplica 6 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare a defectelor software medii se vor aplica 4 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare a defectelor software minore se va aplica 2 punct de penalizare pentru fiecare oră de depășire a termenului.

Un punct de penalizare valorează 0,0001 % din valoarea contractului.

Mentananta se va asigura fără costuri suplimentare din partea ONRC.

Înștiințarea cu privire la o disfuncționalitate a sistemului informatic implementat va fi realizată de către beneficiar prin următoarele metode (care vor fi puse la dispoziție de către furnizor o dată cu punerea în funcțiune a sistemului):

- Automat printr-un mecanism intern la nivelul fiecărui modul/aplicație, gestionate centralizat într-un modul general și personalizabil de administrare și gestiune a incidentelor

254



- Aplicație informatică de gestiune a incidentelor REDMINE sau alt sistem similar aflat în proprietatea achizitorului sau al furnizorului în perioada de garanție și mentenanță, disponibil 24 ore x 7 zile
- Utilizând sistemul de poștă electronică (la o adresă de poștă electronică dedicată pusă la dispoziție de către furnizor), disponibil 24 ore x 7 zile.
- Printr-un apel telefonic al ONRC la un număr dedicat pus la dispoziție de către furnizor, disponibil 24 ore x 7 zile
- Prin transmiterea unui fax de către ONRC la un număr de fax dedicat pus la dispoziție de către furnizor, disponibil 24 ore x 7 zile.

Achizitorul își rezervă dreptul ca oricând pe perioada contractului, cât și în perioada de garanție și mentenanță, să instaleze orice componentă dezvoltată sau modificată de către prestator, urmărind procedurile, manualele și/sau detaliile de instalare realizate de prestator. Pentru orice neclaritate, diferență, omisiune, etc, prestatorul este obligat să actualizeze corespunzător documentele de instalare și/sau suport.

Mentenanță corectivă a sistemului:

a. Furnizorul va realiza aplicarea de update-uri / upgrade-uri necesare bunei funcționări a produselor de bază/adaptate utilizate în cadrul sistemului și rezultate din sesiunile de monitorizare-analiză-rezolvare regulate și aprobate de către beneficiar

b. Furnizorul va realiza modificări asupra sistemului pentru a adresa propunerile de îmbunătățire a performanței și disponibilității sistemului rezultate din sesiunile de monitorizare-analiză-rezolvare regulate și aprobate de către beneficiar


c. Furnizorul va asigura:

- suport telefonic cu privire la modul de funcționare a soluțiilor implementate
- asistența tehnică pentru soluțiile livrate
- asistența tehnică pentru personalul Beneficiarului
- monitorizare de la distanță a soluțiilor instalate și configurate (identificarea și monitorizarea funcționării) urmate de aplicarea în mod proactiv, după informarea Beneficiarului, a diverselor măsuri corective pentru asigurarea continuării funcționării la parametrii optimi)
- reinstalare/ reconfigurare, necesară pe parcursul operării soluțiilor implementate pentru menținerea nivelului de consistență la nivel de software (ca versiuni, patch-level, update-level, configurări etc.). În cazul produselor software standard (licențe), aceste activități vor fi realizate de Prestator doar în cazul în care Autoritatea are asigurat suportul de la producător
- reinstalări de produse software dezvoltate/comerciale în cazul instalării unor versiuni în centrul principal/local care impun reinstalarea acestora
- aplicarea update-urilor și patch-urilor produselor software comerciale / functionalități dezvoltate

Mentenanță evolutivă a sistemului:

a. Furnizorul va realiza întreținerea componentelor dezvoltate ale sistemului astfel încât acestea să fie aliniate cu ultima versiune pe baza specificațiilor rezultate din etapele de analiză/adaptare a sistemului, a cerințelor legislative și a recomandărilor în domeniu. În scopul acestor servicii intră întreținerea tuturor

255



interfețelor, modulelor, componentelor, aplicațiilor dezvoltate față de modificările apărute pentru asigurarea funcționalităților specifice cazurilor de utilizare implementate în cadrul sistemului.

b. Furnizorul va desfășura următoarele activități (fără a se limita la acestea) aferente construirii mediului de producție și a mediului de test:

- 1) Proiectarea extensiei sistemului informatic existent cu subsistemul „nou” atât din punct de vedere arhitectura a sistemului cât și din punctul de vedere a activităților de dezvoltare necesare pentru adaptarea componentelor „existente” în vederea reutilizării în cadrul subsistemului „nou”
- 2) Adaptarea, instalarea și configurarea subsistemului „nou” care include:
 - a. Instalarea / configurarea middleware-ului pe infrastructura existentă
 - b. Adaptarea/modificarea componentelor dezvoltate în sistemul „existent” pentru a fi reutilizate în sistemul „nou”
 - c. Instalarea / configurarea componentelor dezvoltate
- 3) Pentru fiecare modificare se va face o testare funcțională completă a soluției, care se va încheia, după caz, cu un raport de testare.
- 3) Furnizarea de servicii de instruire (hands on) către echipa Autorității Contractante astfel încât aceasta să poată prelua operarea subsistemului „nou” extins. Oferta trebuie să conțină propunerea realistă a Prestatorului în privința zilelor de instruire necesare pentru echipa Autorității Contractante.
- 4) Adăugarea funcționalităților minim necesare pentru lansarea în producție a subsistemului „nou” (analiza noilor cerințe, proiectarea, dezvoltarea și instalarea noilor release-uri)

Transfer de cunoștințe către echipa Beneficiarului

a. Documentarea tuturor procedurilor de administrare/întreținere și încărcarea acestora în baza de cunoștințe a beneficiarului

b. Prezentarea către echipa beneficiarului a modificărilor asupra procedurilor atunci când acestea apar.

3.9.4 Instruirea personalului ONRC

Activitățile de instruire vor fi desfășurate de către Prestator pentru fiecare subsistem în parte și trebuie să creeze competențele necesare în rândul angajaților ONRC, astfel încât la finalul implementării instituția să nu fie dependentă de furnizorul de tehnologie pentru operarea sistemului.

Ofertantul va prezenta un program de instruire pentru toate serviciile de instruire menționate mai jos, cu precizarea următoarelor informații:

- descrierea programului de instruire, a tematicii și a conținutului acestora;
- detalii de organizare a programului de instruire
- descrierea rezultatelor așteptate;
- resurse puse la dispoziție de Prestator;
- resurse necesare din partea ONRC.

256



De asemenea, ofertantul va prezenta în oferta care va fi depusă descrierea detaliată a procedurilor de instruire pe care le propune în cadrul proiectului care vor evidenția în mod obligatoriu următoarele:

- modalitatea de planificare a instruirii;
- modalitatea de desfășurare a instruirii;
- modalitatea de evaluare a rezultatelor instruirii;
- modalitatea de evaluare a performanțelor instructorilor.

ONRC, împreună cu prestatorul, vor stabili de comun acord modalitatea de instruire pe baza planificării proiectului și disponibilității cursanților.

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

ONRC va stabili, la nivel intern, lista participanților la cursurile de instruire și va comunica Managerului de Proiect din partea Prestatorului această listă.

Desfășurarea instruirii

Instruirea se va desfășura conform planului de instruire stabilit și agreat contractual. Instruirea se va ține în limba română, utilizând metode interactive combinate cu metode clasice, de către instructori din partea Prestatorului. Acesta va asigura infrastructura hardware, software și suportul de curs în limba română.

Instruirea se va face pe baza suportului de curs în format electronic, livrat de Prestator fiecărui participant. Acest suport de curs va conține exemple practice pentru o mai bună înțelegere a modului de funcționare și administrare a sistemului, precum și alte detalii legate de acesta.

Încheierea instruirii se va efectua prin testarea participanților. În urma acestei testări se va efectua certificarea/atestarea participanților. Certificarea/atestarea participanților va avea loc pentru toate persoanele care au depășit media minimă pentru admitere, stabilită în prealabil înaintea începerii testării. Testarea se va face pe formulare tipizate, cu întrebări de tip grilă și răspuns liber.

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

Ședințele de instruire constau din:

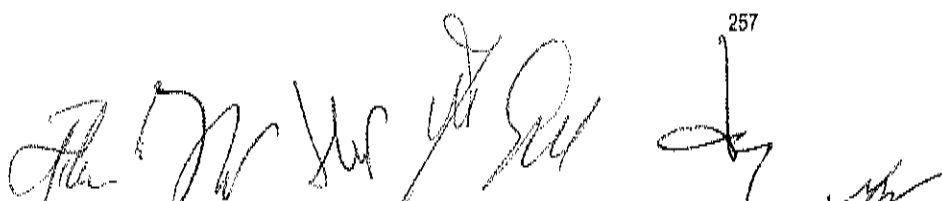
- prezentarea conceptelor de către instructor;
- ședințe practice, pentru mai bună înțelegere și utilizare a sistemului / produselor software (sisteme de operare, sisteme de gestiune a bazelor de date etc.) / echipamentelor hardware;

Instruirea utilizatorilor se va face pe un mediu de test ce va utiliza o bază de date test.

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

Prestatorul va asigura logistica și instruirea administratorilor, dezvoltatorilor și utilizatorilor finali ai sistemului informatic (o parte dintre aceștia), astfel:

257



3.9.4.1 Instruire pentru administrarea sistemului informatic – pentru 68 de administratori ai sistemului informatic integrat, respectiv 8 administratori baze de date/serv. aplic. și 60 administratori de sistem/security

Cursurile vor cuprinde tematici precum administrarea sistemului, administrarea bazelor de date, monitorizarea performanțelor, asistența utilizatorilor, etc

Echipele de implementare/administrare a ONRC va fi instruita de către Prestator astfel încât să poată asigura funcționarea sistemului cu o asistență minimă din partea Prestatorului sau independent de acesta, începând cu perioada post-implementare.

Cursurile vor avea loc la București, într-o locație asigurată de Prestator, dotată corespunzător necesar susținerii cursurilor, fără a fi necesară și asigurarea de servicii de cazare și transport pentru cursanți.

În plus, ofertantul trebuie să includă în propunerea tehnică și 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.

Număr de sesiuni de instruire: 4, fiecare având 5 zile.

Sesiunile de instruire vor avea o audiență de 17 persoane fiecare.

În total se vor instrui 68 de administratori ai sistemului informatic integrat.

3.9.4.2 Instruire pentru echipa de dezvoltatori a ONRC – pentru 22 de dezvoltatori de aplicații, respectiv 12 dezvoltatori de aplicații și 10 dezvoltatori de aplicații - integrare

Echipele de dezvoltatori de aplicații a ONRC va fi instruita de către Prestator astfel încât să poată asigura adaptarea sistemului dezvoltat cu o asistență minimă din partea Prestatorului sau independent de acesta, începând cu perioada post-implementare.

Cursurile vor avea loc la București, într-o locație asigurată de Prestator dotată corespunzător necesar susținerii cursurilor, fără a fi necesară și asigurarea de servicii de cazare și transport pentru cursanți.

Număr de sesiuni de instruire: 2, fiecare având 5 zile.

Sesiunile de instruire vor avea o audiență de 11 persoane fiecare.

În total se vor instrui 22 de dezvoltatori de aplicații.

3.9.4.3 Instruire pentru utilizarea sistemului informatic integrat – pentru 460 de utilizatori finali

Acest tip de instruire este destinat viitorilor utilizatori ai sistemului informatic și se va derula după finalizarea testării funcționale a sistemului implementat, incluzând tematici cu privire la utilizarea noului sistem implementat, după cum urmează:

- Cursuri destinate utilizatorilor finali (RC)
- Cursuri destinate utilizatorilor finali (BPI)
- Cursuri destinate utilizatorilor finali (RL)
- Cursuri destinate celorlalte categorii de utilizatorilor finali

258



Instruirea va fi de tip „train the trainer”, utilizatorii instruiți de către Prestator asigurând, la rândul lor, instruirea celorlalți utilizatori.

Număr de sesiuni de instruire: minim 1, maxim 23, fiecare având 5 zile.

Sesiunile de instruire vor avea o audiență de minim 20 persoane fiecare. Numărul de utilizatori finali instruiți vor fi detaliați după faza de contractare. În total se vor instrui 460 de persoane din rândul utilizatorilor cu privire la utilizarea sistemului informatic integrat.

Instruirea va cuprinde și un modul cu privire la securitatea informației și a sistemului informatic, precum și la protejarea datelor cu caracter personal și la legislația aplicabilă.

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

Cursurile vor avea loc la București, într-o locație asigurată de Prestator dotată corespunzător necesar susținerii cursurilor, fără a fi necesară și asigurarea de servicii de cazare și transport pentru cursanți.

Sesiunile de curs se pot desfășura și în paralel, pe cât posibil, după consultarea și aprobarea acestora în colaborare cu Autoritatea Contractantă, pentru a nu bloca activitățile operaționale ale ONRC/ORCT, cu încadrarea în termenele impuse de obligația respectării datei de finalizare a proiectului.

3.10 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 sau altor organizații;
- Surse de mediu legislativ – factori care provin din contextul legislativ național/comunitar/internațional (legislația actuală aplicabilă) și evoluția legislației naționale/comunitare/internaționale;
- Surse externe (la nivel european, național) – factori ce sunt determinați de specificațiile stabilite pentru platformele BRIS, IRI, BEREC (Buletinul electronic al registrului comerțului), EBOCS, SAE;
- Surse de ordin tehnic – factori care provin din constrângeri (limitări) de tip tehnic, inclusiv la nivelul datelor existente sau al formatului acestora.

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	Măsuri de atenuare ale riscului
1	Se schimbă Project Managerul din echipa proiectului pe durata derulării acestuia Probabilitate: mică	Impact: semnificativ Consecințe: apariția unor disfuncționalități în gestionarea proiectului și în coordonarea echipei de proiect. Acțiuni preventive: La formarea echipei se desemnează un PM care a mai fost implicat în proiecte din același domeniu sau cel

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
		<p>puțin din aceeași sferă și care are o stabilitate cunoscută în cadrul structurii organizatorice a ONRC. Desemnarea unui adjunct care să cunoască toate aspectele operaționale ale proiectului și care să poată prelua aceasta funcție în cazul indisponibilității managerului de proiect desemnat inițial.</p> <p>Responsabili: Director General ONRC</p>
2	<p>Descompletarea echipelor pe durata ciclului de viața al proiectului</p> <p>Probabilitate: medie</p>	<p>Impact: mediu</p> <p>Consecințe: un posibil impact semnificativ asupra activităților proiectului, livrabilelor cheie, finalizării etapelor proiectului. Pierderea unor abilitați cheie în momente critice.</p> <p>Acțiuni corective: Înlocuirea personalului cât mai curând posibil, permiterea unei perioade de tranziție, atunci când este posibil.</p> <p>Acțiuni preventive: Pregătirea și derularea unui program intern de instruire.</p> <p>Responsabili: manager de proiect ONRC, Director general ONRC</p>
3	<p>Rezistența personalului beneficiarului la schimbare</p> <p>Probabilitate: medie</p>	<p>Impact: mediu</p> <p>Consecințe: Probleme operaționale. Beneficiile sistemului nu pot fi valorificate complet din cauza folosirii practicilor vechi de lucru.</p> <p>Acțiuni corective: problema va fi escaladată către Comitetul Director al Proiectului. Ar putea fi necesare programe de instruire suplimentare.</p> <p>Acțiuni preventive: obținerea angajamentului conducerii beneficiarului că personalul său va fi informat despre importanța proiectului.</p> <p>Responsabili: manager de proiect ONRC, Director general ONRC</p>
4	<p>Modificări în aria de cuprindere a proiectului</p> <p>Probabilitate: medie</p>	<p>Impact: mediu</p> <p>Consecințe: Posibile reevaluări ale obiectivului, costurilor și/sau etapelor proiectului.</p> <p>Acțiuni corective: Reprogramarea componentelor non-critice ale proiectului pentru etapa ulterioară. Acest proces va fi desfășurat în concordanță cu procedura de control a modificărilor.</p>

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
		<p>Acțiuni preventive: Asigurarea acordului tuturor factorilor decizionali importanți în privința acoperirii sistemului din faza inițială a proiectului.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
5	<p>Lipsa cooperării din partea utilizatorilor</p> <p>Probabilitate: mica</p>	<p>Nivelul de implicare a utilizatorilor este esențial atât pentru succesul sistemului cât și pentru acceptanța finală.</p> <p>Impact: mediu</p> <p>Consecințe: costuri suplimentare pentru proiect, cauzate de eventuala apariție a unor noi cerințe. Definierea eronată a unor cerințe funcționale.</p> <p>Acțiuni corective: Escaladarea către nivelurile conducerii superioare și obținerea unui angajament puternic din partea Comitetului Director.</p> <p>Acțiuni preventive: Utilizatorii trebuie implicați în activitățile proiectului. Dacă este necesar se vor efectua analize ale proiectului.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
6	<p>Nu se respecta termenul de implementare tehnică al proiectului.</p> <p>Probabilitate: medie</p>	<p>Impact: mediu</p> <p>Consecințe: imposibilitatea respectării termenului de implementare specificat în Contractul de finanțare</p> <p>Acțiuni preventive: Respectarea perioadei de analiză pentru stabilirea tuturor detaliilor pentru desfășurarea dezvoltării în parametri stabiliți. Verificarea periodică a taskurilor în derulare.</p> <p>Acțiuni corective: stabilirea măsurilor pentru recuperarea timpului pierdut în etapele anterioare. Încheierea de acte adiționale la contractul de finanțare.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
7	<p>Produsul nu respectă întocmai cerințele clientului</p> <p>Probabilitate: medie</p>	<p>Riscul apare atunci când Prestatorul nu a înțeles exact ce dorește clientul sau când nu sunt respectate specificațiile funcționale ale proiectului.</p> <p>Impact: Semnificativ</p>

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
		<p>Acțiuni preventive: Validarea etapelor intermediare astfel încât să se poată observa cât mai rapid orice deviație și pentru a se putea lua măsurile necesare pentru corectarea acestora.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
8	<p>Produsul final conține bug-uri</p> <p>Probabilitate: medie</p>	<p>Impact: Mediu</p> <p>Acțiuni preventive: stabilirea unei etape de testare internă a fiecărei componente, apoi a unei testări integrate.</p> <p>Acțiuni corective: Asigurarea unei marje de timp pentru rezolvarea bug-urilor, existenta unei echipe de testare care să descopere toate bug-urile existente.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
9	<p>Domeniu nou pentru dezvoltatori</p> <p>Probabilitate: medie</p>	<p>Fiind un produs inovator pe piață, dezvoltatorii sistemului pot avea dificultăți în a-și desfășura munca.</p> <p>Impact: Mare</p> <p>Acțiuni preventive: Se vor căuta dezvoltatori sau consultanți care au mai lucrat pe proiecte asemănătoare. Se va asigura buna înțelegere a procesului general de către dezvoltatori.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
10	<p>Neagrearea unui plan formal pentru testarea funcțională a sistemului informatic, bazat pe scenarii clare de testare, ceea ce poate duce la prelungirea excesiva a perioadei de testare, sau la apariția unor noi cerințe introduse sub formă de observații de testare. Prolungirea perioadelor de testare afectează și planificarea activităților experților pentru managementul proiectului.</p> <p>Probabilitate: medie</p>	<p>Impact: Mediu</p> <p>Acțiuni preventive: Stabilirea unei strategii de testare și acceptanță imediat după demararea proiectului de implementare a soluției informatice.</p> <p>Planul de contingenta pentru protejarea proiectului dacă acțiunile preventive eșuează: Întocmirea unor scenarii de testare și acceptanță agreeate de ambele părți, care să ușureze activitatea de testare. Validarea de către ONRC a strategiei de testare și acceptanță pentru sistemul informatic.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
11	<p>Existența unor divergențe de opinie de natură tehnică între experții ONRC și experții tehnici ai Prestatorului, care să determine întârzierea finalizării unor activități din proiect.</p> <p>Probabilitate: medie</p>	<p>Impact: Mediu</p> <p>Acțiuni preventive: Stabilirea exacta a responsabilităților și a nivelului de autoritate pentru fiecare din experții / specialiștii celor două organizații. Derularea unor întâlniri în care să fie prezentate și discutate opiniile experților și specialiștilor celor două organizații. Derularea unei sesiuni de instruire preliminară pentru prezentarea tehnologiilor utilizate în proiect.</p> <p>Acțiuni corective: Implicarea managerului de proiect al ONRC și a managerului de proiect al prestatorului pentru medierea eventualelor dispute.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator</p>
12	<p>Epidemia de boală coronavirus 2019 (COVID-19) poate afecta capacitatea de prestare a serviciilor la sediile Autorității Contractante.</p> <p>Probabilitate: medie</p>	<p>Impact: Mare</p> <p>Consecințe: întârzierea îndeplinirii activităților conform graficului.</p> <p>Acțiuni preventive: Autoritatea Contractantă va lua măsurile recomandate în vederea reducerii impactului pandemiei COVID-19. Se vor desfășura de la distanță orice activități posibile. Pentru toate activitățile de la sediile Autorității Contractante se vor respecta măsurile în vigoare.</p>
13	<p>Criza financiară provocată de epidemia de boală coronavirus 2019 (COVID-19) poate afecta capacitatea de derulare a achizițiilor internaționale de echipamente și produse software.</p> <p>Probabilitate: medie</p>	<p>Impact: Mare</p> <p>Consecințe: Dacă Ofertanții nu reușesc să obțină finanțări naționale/internaționale nu se vor putea plasa comenzile de echipamente.</p> <p>Acțiuni preventive: Derularea procedurilor de achiziție echipamente fără întârzieri în etapa de recepție, pentru a diminua nevoia de finanțare a proiectului. Diminuarea sumei de finanțat între momentul recepției și plata finală.</p> <p>Responsabili: manager de proiect ONRC / manager de proiect prestator / Director general ONRC</p>

Ofertantul va identifica și alte riscuri față de cele principale, arătate mai sus. În oferta se vor prezenta recomandări/proponeri de reducere sau eliminare a riscurilor care ar putea afecta implementarea proiectului (inclusiv a riscurilor prezentate mai sus).

3.11 Cerințe specifice

Pentru toate componentele software dezvoltate și/ sau pentru toate aplicațiile software propuse pentru desfășurarea contractului, Prestatorul va respecta următoarele cerințe:

- Toate licențele software necesare implementării sistemului vor fi perpetue, cu drept de utilizare ONRC pentru totdeauna de la momentul plății, respectiv orice componenta software furnizată va putea să fie folosită în mod legal pentru o perioadă nedefinită de timp, în care funcționalitățile minimale solicitate trebuie să rămână active, pentru sistemele oferite, conform cerințelor din prezentul document. Nu se accepta alte tipuri de licențiere software, inclusiv nu se acceptă următoarele: leasing, închiriere, licențiere temporară indiferent de perioada de timp oferită dacă este limitată, licențiere cloud, etc.
- Nu se vor accepta aplicații sau sisteme care interacționează cu entități din afara rețelei ONRC, inclusiv nu se accepta sisteme care să interacționeze cu sistemele producătorilor, sisteme de tip cloud public (extern ONRC), etc. Excepție fac cazurile în care pentru buna funcționare și mentenanța aplicațiilor și componentelor oferite și pentru buna îndeplinire a cerințelor tehnice, este nevoie de interacțiunea cu site-urile producătorilor sau alte site-uri (de exemplu: site-uri de update-uri pentru sistemul de operare sau aplicații, site-uri de unde este nevoie de componente sau versiuni noi ale aplicațiilor furnizate, site-uri de firmware, BIOS, drivere, knowledge base ale producătorilor de echipamente – în orice situație este obligatoriu ca aceste site-uri să fie cele oficiale indicate de producători). De asemenea, la excepții se încadrează și conectivitatea specifică sistemului, așa cum este prezentată în acest document.

Atât pe parcursul desfășurării contractului, cât și în timpul perioadei de garanție și a asigurării suportului pentru platforma software, ONRC își rezerva dreptul să verifice oricând orice livrabil realizat de Ofertantul declarat câștigător, inclusiv cod sursa, proceduri de instalare, modificări în sisteme, documentație, etc. Pentru orice neconcordanță, Ofertantul declarat câștigător este obligat să remedieze problema semnalată și eventual să actualizeze documentele aferente.

Criteriile de acceptanță de la fiecare nivel de testare vor fi stabilite în acord cu Autoritatea Contractantă într-un plan de testare care va fi propus de Ofertantul declarat câștigător și validat de Autoritatea Contractantă, astfel încât să se asigure conformitatea implementării soluției cu specificațiile funcționale stabilite.

Recepții și teste de acceptanță:

- Pentru recepții vor fi avute în vedere prevederile din capitolul **Modalitate de plată**;
- Vor avea loc recepții cantitative și calitative ale componentelor sistemului informatic (echipamente hardware, produse software, alte componente software, analiză, proiectare, dezvoltare, testare, migrare, instruire);
- Punerea în funcțiune a infrastructurii hardware, produselor software și a platformei de virtualizare respectiv recepția calitativă se vor face prin teste de bază a funcționării acestora;
- Recepția finală a sistemului informatic va avea loc prin testarea întregului sistem integrat pe baza unui plan de testare agreat. Testarea se va face și pe baza de date de producție după ce s-a terminat migrarea datelor pe noua structură.

- Acceptarea codului sursă pentru sistemul informatic (module/aplicatii) se va face cu demonstrarea funcționării acestuia, respectiv se va efectua cel puțin cinci modificări, se vor compila, se vor instala și se va demonstra ca funcționează corect pe mediu de producție al Beneficiarului.
- Pentru testele de acceptanță vor fi avute în vedere prevederile din capitolul **Testarea și testele de acceptanță**.

3.12 Evaluarea performanței Contractantului

Performanța Contractantului va fi evaluată de către Autoritatea Contractantă pe durata implementării proiectului pe baza indicatorilor de performanță menționați în Anexa 1 a prezentului caiet de sarcini. Performanța finală a Contractantului va fi calculată ca medie aritmetică a acestor indicatori prin rotunjire la 0 zecimale, conform funcției ROUND din Microsoft Excel – ROUND(formula, 2). 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 pe durata derulării Contractului.

4 Descrierea cerințelor pentru experții cheie

Prestatorul va asigura o echipa formata din experții solicitați care vor fi responsabili de realizarea activităților din cadrul contractului în conformitate cu cerințele beneficiarului.

ONRC va oferi suport tehnic pentru implementare prin intermediul propriului personal, din rândul angajaților din domeniile IT, juridic, RC, RL, BPI, economic sau alte domenii de business și suport, după caz, care va pune la dispoziția Prestatorului tehnic informațiile necesare despre infrastructura existentă și, de asemenea, cu privire la sursele și specificul datelor existente în cadrul organizației sau alte informații relevante pentru buna derulare a proiectului.

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

Din punct de vedere al resurselor umane necesare pentru operarea sistemului informatic, aceștia vor fi angajații ONRC din domeniile IT, juridic, RC, RL, BPI, economic, managementul instituției, alte domenii de business și suport, după caz.

4.1 Responsabilitățile experților cheie

4.1.1 Manager de proiect – 1 persoană

Responsabilități:

- Activități specifice de management de proiect (legat de obiectul contractului)

- Punct principal de contact în relația cu beneficiarul
- Managementul proiectului în ansamblul sau, managementul ariei de cuprindere, managementul schimbărilor, planificarea generală a proiectului, managementul riscurilor, managementul problemelor, managementul comunicării
- Asigurarea resurselor proiectului
- Managementul, organizarea, alocarea și planificarea echipei de proiect
- Urmărirea respectării tuturor termenelor conform planului de proiect
- Realizarea rapoartelor periodice/ad-hoc ale proiectului.
- Elaborarea planurilor de calitate
- Verificarea și asigurarea calității livrabilelor

4.1.2 Manager de proiect adjunct – 1 persoană

Responsabilități:

- Activități specifice de management de proiect (legat de obiectul contractului)
- Punct secundar de contact în relația cu beneficiarul
- Rezolvarea problemelor în scopul evitării situațiilor de criza
- Urmărirea respectării tuturor termenelor conform planului de proiect
- Analiza modalității prin care livrabilele proiectului corespund cerințelor de business
- Verificarea și asigurarea calității livrabilelor

4.1.3 Expert arhitect soluție – 1 persoană

Responsabilități:

- Definirea, împreună cu Expertul coordonare dezvoltare aplicații software, a soluțiilor detaliate pentru noile subsisteme
- Definirea arhitecturii de integrare a componentelor sistemului
- Activități de implementare, asistența și suport tehnic
- Identificarea riscurilor și problemelor tehnice și a soluțiilor de rezolvare

4.1.4 Expert coordonare analiză – 1 persoană

Responsabilități:

- Coordonează activitățile de analiză a cerințelor de business, elaborare a documentelor de specificații funcționale și a scenariilor de testare
- Activități de implementare, asistența și suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanță a sistemului

4.1.5 Expert analist de business – 3 persoane

Responsabilități:

- Analiza cerințelor de business
- Realizarea documentelor de specificații funcționale și a scenariilor de testare
- Activități de implementare, asistenta și suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanță a sistemului

4.1.6 Expert coordonare dezvoltare software – 1 persoană

Responsabilități:

- Coordonează activitățile de dezvoltare de software
- Asigura suport tehnic în activitățile de implementare
- Rezolva disfuncționalități software (bug-uri)
- Asigura suport tehnic în perioada de garanție
- Crearea/ actualizarea documentațiilor

4.1.7 Expert dezvoltare aplicații software – 6 persoane

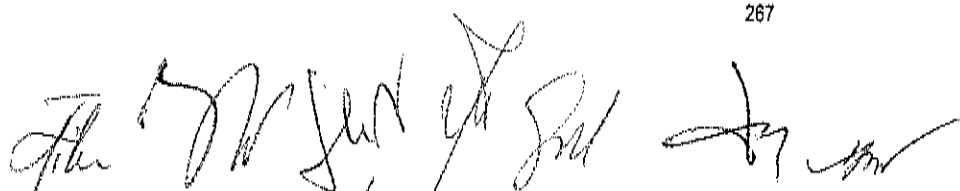
Responsabilități:

- Activități specifice de dezvoltare de aplicații software, pe baza documentelor de analiza, specificații funcționale, specificații tehnice, arhitectura sistem
- Testare unitara (interna)
- Suport în activitățile de implementare
- Rezolvare disfuncționalități software (bug-uri)
- Asigurare suport tehnic în perioada de garanție
- Crearea/ actualizarea documentațiilor

4.1.8 Expert coordonare testare – 1 persoană

Responsabilități:

- Coordonarea activităților de testare
- Activități specifice testării de aplicații software
- Implementarea planurilor, scenariilor și cazurilor de test,
- Activități de testare componente și testare funcțională,
- Întocmirea și livrarea rapoartelor de testare și implementare.



4.1.9 Expert testare – 2 persoane

Responsabilități:

- Activități specifice testării de aplicații software
- Implementarea planurilor, scenariilor și cazurilor de test,
- Activități de testare componente și testare funcțională,
- Întocmirea și livrarea rapoartelor de testare și implementare.

4.1.10 Expert implementare software – 2 persoane

Responsabilități:

- Activități specifice de instalare și configurare a produselor software oferite
- Crearea și actualizarea documentațiilor de administrare a produselor software
- Activități de implementare, asistența și suport tehnic

4.1.11 Expert baza de date – 1 persoană

Responsabilități:

- Activități specifice de instalare și administrare de baze de date în arhitecturi redundante;
- Activități specifice replicării datelor din baza de date;
- Asistența și suport tehnic;
- Testarea bazelor de date;
- Dezvoltarea soluției de migrare baze de date
- Crearea/ actualizarea documentațiilor de administrare;

4.1.12 Expert replicări date/ETL – 1 persoană

Responsabilități:

- Activități specifice de instalare și configurare componente de replicare date sau ETL;
- Proiectarea și implementarea proceselor de replicare date sau ETL din baza de date a SII ONRC în baza de date a sistemului implementat, ținând cont de cerințele caietului de sarcini;
- Asistența și suport tehnic;
- Testarea componentelor de replicare date sau ETL;
- Crearea și actualizarea documentațiilor de administrare a componentelor de replicare date sau ETL;

4.1.13 Expert infrastructură/virtualizare – 1 persoană

Responsabilități:

- Activități specifice implementării infrastructurii / sistemului de virtualizare aferente sistemului;

- Asistența și suport tehnic;
- Adaptări/actualizări/îmbunătățiri/extinderi/ configurări ale sistemului de virtualizare;
- Testarea sistemului de virtualizare;
- Crearea/ actualizarea documentațiilor de administrare;

4.1.14 Expert comunicații – 1 persoană

Responsabilități:

- Activități specifice proiectării și implementării din punct de vedere securitate a comunicațiilor sistemului informatic implementat, atât din punct de vedere software, cât și hardware;
- Activități de proiectare, instalare și configurare rețele de comunicație redundante
- Asistența și suport tehnic;
- Crearea/ actualizarea/ verificarea documentațiilor.

4.1.15 Expert testare de securitate -- 1 persoană

Responsabilități:

- Activități specifice testării de securitate a sistemelor informatice
- Testează eficiența controalelor de securitate implementate în proiect
- Identifica vulnerabilitățile existente la nivelul sistemului
- Implementarea planurilor, scenariilor și cazurilor de test,
- Activități de testare componente și testare funcțională,
- Întocmirea și livrarea rapoartelor de testare și implementare

4.1.16 Expert securitatea informației – 1 persoană

Responsabilități:

- Realizarea soluției de securitate în etapa de analiza;
- Configurarea din punct de vedere al securității a sistemelor informatice;
- Consultanța de specialitate pentru echipa de proiect în timpul derulării proiectului;
- Realizarea planului de securitate a sistemului informatic;
- Realizarea planurilor de continuitate și recuperare în caz de dezastru;
- Instrucțiuni pentru administratorii sistemului informatic și pentru utilizatorii sistemului informatic;
- Întocmirea și livrarea rapoartelor de testare și implementare

4.1.17 Expert instruire – 1 persoană

Responsabilități:

269



- Derularea activităților de instruire utilizatori;
- Pregătirea materialelor de curs și a testelor în strânsă legătură cu restul echipei;
- Pregătirea raportului de curs.

4.1.18 Expert amenajare centru de date – 1 persoane

Responsabilități:

- Activități specifice de amenajare/ instalare/ operare a centrelor de date
- Consultanta de specialitate pentru echipa de proiect în timpul derulării proiectului
- Adaptarea planului de proiect (și a proiectului) la elementele specifice apărute în timpul amenajării/ instalării/ operării centrului de date
- Testarea echipamentelor de protecție specifice centrului de date
- Realizarea documentelor specifice centrului de date, inclusiv pentru operațiile de operare, întreținere, mentenanță
- Instrucțaj pentru responsabilii centrului de date

4.1.19 Experti responsabili cu amenajare centru de date (numarul de persoane va fi stabilit de ofertant)

Responsabilități/competențe profesionale dobândite conform supliment descriptiv al certificatului de absolvire pentru ocupațiile:

Inginer sisteme de securitate fizică cod COR 215222 cu următoarele competențe:

- Organizarea activitatilor de instalare a sistemelor tehnice de securitate;
- Instalarea sistemelor tehnice de detectie si alarmare la efracție si control al accesului;
- Instalarea sistemelor tehnice de detectare, semnalizare si alarmare la incendiu;
- Instalarea sistemelor tehnice de televiziune cu circuit inchis (TVCI);
- Realizarea sistemelor tehnice de monitorizare;
- Asigurarea testarii, evaluarii si punerii in functiune a echipamentelor si sistemelor tehnice de detectie si alarmare la efracție si control al accesului;
- Asigurarea testarii, evaluarii si punerii in functiune a echipamentelor si sistemelor tehnice de detectare, semnalizare si alarmare la incendiu;
- Asigurarea testarii, evaluarii si punerii in functiune a echipamentelor si sistemelor tehnice de televiziune cu circuit inchis;
- Asigurarea testarii, evaluarii si punerii in functiune a echipamentelor si sistemelor tehnice de monitorizare;
- Asigurarea mentenantei si service-ului pentru sistemele tehnice de detectie si alarmare la efracție si control al accesului;
- Asigurarea mentenantei si service-ului pentru sistemele tehnice de detectare, semnalizare si alarmare la incendiu;
- Asigurarea mentenantei si service-ului pentru sistemele tehnice de televiziune cu circuit inchis;
- Asigurarea mentenantei si service-ului pentru sistemele tehnice de monitorizare;
- Instruirea beneficiarului asupra utilizarii si intretinerii sistemului.

Tehnician pentru sisteme tehnice de detecție, supraveghere video și monitorizare, control acces cod COR 352130 cu următoarele competențe:

- Montarea tubulaturii pentru sistemele tehnice de securitate
- Realizarea cablajului necesar sistemelor tehnice de securitate
- Pregătirea lucrărilor de instalare a sistemelor tehnice de securitate
- Instalarea sistemelor de detectare, semnalizare și alarmare la incendiu
- Instalarea sistemelor tehnice de detecție, efracție și control al accesului
- Instalarea sistemelor tehnice de monitorizare
- Instalarea sistemelor tehnice de televiziune cu circuit închis (TVCI)
- Punerea în funcțiune a sistemelor de detectare, semnalizare și alarmare la incendiu
- Punerea în funcțiune a sistemelor tehnice de detecție, efracție și control al accesului
- Punerea în funcțiune a sistemelor tehnice de monitorizare
- Punerea în funcțiune a sistemelor tehnice de televiziune cu circuit închis (TVCI)
- Asigurarea mentenanței și service-ului pentru sistemele de detectare, semnalizare și alarmare la incendiu
- Asigurarea mentenanței și service-ului pentru sistemele tehnice de detecție, efracție și control al accesului
- Asigurarea mentenanței și service-ului pentru sistemele de monitorizare
- Asigurarea mentenanței și service-ului pentru sistemele de televiziune cu circuit închis (TVCI)
- Aplicarea normelor de sănătate și securitate în muncă
- Menținerea unor relații de muncă eficiente
- Aplicarea normelor de protecție a mediului

Tehnician pentru sisteme tehnice de detecție, alarmare și stingere incendiu cod COR 742106 cu următoarele competențe:

- Aplicarea prevederilor legale referitoare la sănătatea și securitate în muncă;
- Aplicarea normelor de protecție a mediului;
- Organizarea activității de instalare a sistemelor și instalațiilor de limitare și stingere a incendiilor;
- Instalarea sistemelor și instalațiilor de limitare și stingere a incendiilor;
- Punerea în funcțiune a sistemelor și instalațiilor de limitare și stingere a incendiilor;
- Efectuarea verificării curente de stare a sistemelor și instalațiilor de limitare și stingere a incendiilor;
- Asigurarea mentenanței sistemelor și instalațiilor de limitare și stingere a incendiilor.

Electrician autorizat pentru executarea/verificarea instalațiilor electrice cu autorizare de tip B, grad II, cod COR 741101 cu următoarele competențe:

- confecționarea și montajul instalațiilor de paratrasnet și a prizei de pamant;
- măsurarea parametrilor la instalațiile electrice,
- montajul instalațiilor electrice aferente utilajelor termice și tehnico-sanitare,
- montajul instalațiilor electrice interioare și exterioare de uz general,
- remedierea defecțiunilor aparute la instalațiile electrice,
- aprovizionarea cu materiale a locului de muncă.

Frigotehnist pentru instalații frigorifice/sisteme de condiționare a aerului, cod COR 712701 cu următoarele competențe

- instalarea
- întreținerea
- punerea și scoaterea în/din funcțiune
- diagnosticarea deficiențelor de funcționare
- remedierea deficiențelor uzuale
- supravegherea instalațiilor frigorifice

4.2 Cerințe minime obligatorii ale experților cheie

Numărul minim de persoane necesar pentru fiecare categorie de experți este menționat în dreptul acesteia. Fiecare dintre persoanele propuse trebuie să îndeplinească integral toate cerințele minime aferente expertului (profilului de persoana) pentru care au fost nominalizate. Nu se accepta îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.

4.2.1 Manager de proiect – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind managementul de proiect dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.2 Manager de proiect adjunct – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind managementul de proiect dovedite prin certificare în domeniu recunoscută la nivel național / internațional
- Experiență specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.3 Expert arhitect soluție – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe în domeniul arhitecturilor de tip Enterprise orientate pe servicii, dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Competențe privind o metodologie de dezvoltare software, dovedite prin certificare în domeniu recunoscută la nivel național/internațional



- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.4 Expert coordonare analiză – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind analiza de business dovedite prin certificare în domeniu recunoscută la nivel național/internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.5 Expert analist de business – 3 persoane

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind analiza de business dovedite prin certificare în domeniu recunoscută la nivel național/internațional
- Experiență specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.6 Expert coordonare dezvoltare software – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind crearea de arhitecturi pentru soluții software de tip Enterprise dovedite prin certificare în domeniu recunoscută la nivel național sau internațional
- Competențe privind dezvoltarea de software dovedite prin certificare în domeniu recunoscută la nivel național sau internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.7 Expert dezvoltare aplicații software – 6 persoane

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind dezvoltarea de software dovedite prin certificare în domeniu obținute la nivel național sau internațional (pentru absolvenții de studii superioare la facultăți cu profil informatic/calculatoare, este suficientă diploma de absolvire)

- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic care a inclus o soluție de dezvoltare aplicații software pe tehnologia oferită, în cadrul căruia a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

4.2.8 Expert coordonare testare – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind testarea sistemelor informatice, dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.9 Expert testare – 2 persoane

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind testarea sistemelor informatice, dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.10 Expert implementare software – 2 persoane

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe în domeniul IT pentru cel puțin 2 din următoarele domenii: sisteme de operare / aplicații software / portal / servere de aplicație, dovedite prin certificări recunoscute la nivel național / internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic care a inclus o soluție de implementare software pe tehnologia oferită, în cadrul căruia a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

4.2.11 Expert baza de date – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind administrarea bazelor de date în configurație cluster dovedite prin certificare în domeniu recunoscută la nivel național/ internațional
- Competențe privind optimizarea performanței bazelor de date dovedite prin certificare în domeniu recunoscută la nivel național/ internațional

- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic care a inclus o soluție de baze de date pe tehnologia oferită, în cadrul căruia a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

4.2.12 Expert replicări date/ETL – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind implementarea sistemelor de replicare a datelor sau a instrumentelor ETL dovedite prin certificare recunoscută la nivel național/internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic care a inclus o soluție de replicare date/ETL pe tehnologia oferită, în cadrul căruia a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

4.2.13 Expert infrastructură/virtualizare – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe în domeniul sistemelor de operare de tip Enterprise, dovedite prin certificare recunoscută la nivel național/ internațional
- Competențe privind sistemul de virtualizare oferit în cadrul acestei proceduri, dovedite prin certificare recunoscută la nivel național/ internațional
- Competențe în domeniul sistemelor hyperconvergente, dovedite prin certificare recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.14 Expert comunicații – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind implementarea, administrarea și depanarea tehnologiilor avansate de rutare și switching, dovedite prin certificare recunoscută la nivel național/ internațional
- Competențe privind administrarea și gestiunea securitatea rețelelor dovedite prin certificare recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.15 Expert testare de securitate – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent

- Competențe privind testarea de securitate a sistemelor informatice, dovedite prin certificare recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract în cadrul căruia au fost desfășurate activități de testare a securității sistemelor informatice și în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.16 Expert securitatea informației – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind securitatea datelor și a sistemelor informatice, dovedite prin certificare recunoscută la nivel național/ internațional
- Experiență specifică în cel puțin un proiect sau contract de evaluare a unor sisteme informatice în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.17 Expert instruire – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind instruirea, dovedite prin diplomă/certificare de formator recunoscută la nivel național/ internațional sau echivalent
- Experiență specifică în cel puțin un proiect sau contract de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract

4.2.18 Expert amenajare centru de date – 1 persoană

- Absolvent studii superioare finalizate cu diploma de licență sau echivalent
- Competențe privind amenajarea/ instalarea și operarea centrelor de date (Data Room), dovedite prin prezentarea oricărui acreditări/certificări recunoscute la nivel național/internațional în specialitatea ATS (Accredited Tier Specialist) sau echivalent
- Experiență specifică în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

4.2.19 Experti responsabili cu amenajare centru de date (numarul de persoane va fi stabilit de ofertant)

Responsabilii trebuie sa detina cel putin urmatoarele specializari:

- responsabil tehnic cu executia sistemelor de conditionare a aerului – certificat provizoriu de AGFR – în baza Notificării Ministrului Mediului Nr 17694/ss/29.12.2008 și a Ordinului Ministrului Mediului Nr 756/2011.
- tehnician pentru sisteme tehnice de detecție, supraveghere video și monitorizare, control acces și de comunicații – se va prezenta certificatul de absolvire și

suplimentul descriptiv al certificatului în conformitate cu Legea 333/2003 și HG 301/2012

- tehnician pentru sisteme tehnice de detecție, alarmare și stingere incendiu - se va prezenta certificatul de absolvire și suplimentul descriptiv al certificatului în conformitate cu OMAI 87/2010
- inginer sisteme de securitate – se va prezenta certificatul de absolvire și suplimentul descriptiv al certificatului în conformitate cu Legea 333/2003 și HG 301/2012
- inginer sisteme de detecție, alarmare și stingere incendiu – se va prezenta certificatul de absolvire și suplimentul descriptiv al certificatului în conformitate cu OMAI 87/2010
- electrician autorizat ANRE tip B, gradul II se va prezenta autorizația de electrician de tip B în conformitate cu Ordinul nr. 116 din 20.12.2016 pentru modificarea anexei la ordinul președintelui autorității naționale de reglementare în domeniul energiei nr. 11/2013 privind aprobarea regulamentului pentru autorizarea electricienilor, verificatorilor de proiecte, responsabililor tehnici cu execuția, precum și a experților tehnici de calitate și extrajudiciari în domeniul instalațiilor electrice

Pentru experții responsabili cu amenajare centru de date se accepta și nominalizarea unui singur expert pentru mai multe poziții.

În conformitate cu principiul recunoașterii reciproce, autoritatea contractantă accepta documente echivalente celor solicitate la nivelul documentației de atribuire, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Pentru experții responsabili cu amenajare centru de date, ofertantul va descrie în propunerea tehnică momentul în care vor interveni în implementarea viitorului contract, precum și modul în care operatorul economic ofertant și-a asigurat accesul la serviciile acestora, fie prin resurse proprii, caz în care vor fi prezentați experții în cauză, fie prin externalizare, situație în care se vor descrie aranjamentele contractuale realizate în vederea obținerii serviciilor respective, nominalizarea și prezentarea de documente precum autorizația/atestatul/certificatul urmând a fi solicitate pe parcursul derulării contractului.

Operatorul economic străin trebuie să întreprindă, acolo unde legislația națională impune, demersurile necesare pentru a putea prezenta pe parcursul derulării contractului autorizațiile recunoscute de autoritățile române.

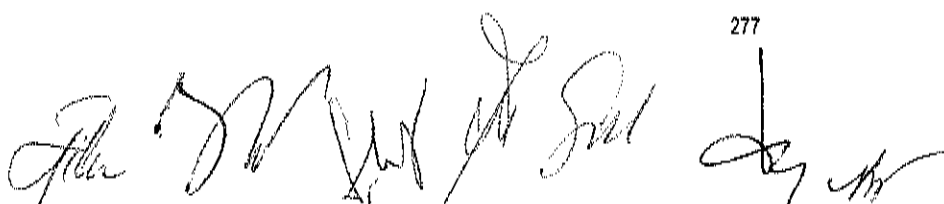
Prin sintagma "același tip de activități" se înțelege și faptul că expertul a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract.

Pentru experții cheie de la pct. 4.2.1. până la pct. 4.2.18 din caietul de sarcini, se acceptă nominalizarea unui anumit expert pentru o singură poziție în cadrul contractului.

Prestatorul va asigura un număr suficient de experți non-cheie pentru realizarea proiectului, suplimentând resursele alocate activităților pe perioada derulării contractului, fără însă a solicita modificarea valorii acestuia. Experții non cheie vor trebuie să lucreze sub îndrumarea experților cheie.

Ofertanții trebuie să prezinte în oferta tehnică, pentru fiecare expert solicitat de la pct. 4.2.1. până la pct. 4.2.18 din caietul de sarcini, următoarele informații/documente:

277



- numele persoanei propuse pentru fiecare poziție (de exemplu pentru dezvoltator software sunt cerute minim 6 poziții și pentru fiecare dintre acestea trebuie nominalizată câte o persoană);
- declarația de disponibilitate semnată de persoana propusă (în cazul în care aceasta nu este angajat al Prestatorului);
- Curriculum Vitae (CV), aferent fiecărei persoane propuse în cadrul echipei, semnat de către fiecare titular în parte și datat;
- Copiile documentelor justificative relevante care demonstrează îndeplinirea cerințelor referitoare la studiile, expertiza și experiența specifică relevantă solicitată și prezentată în CV, cum ar fi:
 - Diplome de studii, certificări, alte diplome relevante;
 - Recomandări emise de beneficiarul final al proiectului, semnate sau contrasemnate de către Autoritatea Contractantă/beneficiarul privat în calitate de beneficiar final, sau alte documente edificatoare, din care să reiasă denumirea, beneficiarul și perioada de realizare a proiectelor/contractelor în care a acumulat experiența solicitată și activitățile prestate de către persoana propusă precum și rolul deținut în proiect, care să evidențieze experiența profesională specifică similară.

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

În cazul în care ofertantul, în cadrul ofertei depuse, nu menționează cel puțin următoarele elemente pentru a demonstra experiența minimă în proiecte a personalului propus, oferta acestuia va fi respinsă:

- Denumirea, beneficiarul și perioada de realizare a proiectelor în care a acumulat experiența solicitată
- Activitățile prestate de către persoana propusă precum și rolul deținut în proiect

Autoritatea Contractantă are dreptul de a verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți și de a solicita și alte documente/ informații care să clarifice experiența similară respectivă.

În urma verificării exactității informațiilor și a dovezilor furnizate de către ofertanți, Autoritatea Contractantă poate solicita și alte documente/informații care să clarifice experiența profesională solicitată. De asemenea, Autoritatea Contractantă își rezervă dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experiența profesională, în vederea confirmării celor prezentate de către ofertanți.

Persoanele propuse vor fi de preferat vorbitori de limba română la un nivel avansat. În cazul persoanelor care nu sunt vorbitori de limba română, prestatorul va pune la dispoziție interpreți/ traducători autorizați în vederea comunicării cu personalul autorității contractante și în vederea traducerii livrabililor ce trebuie predate autorității contractante în limba română. Ofertantul declarat câștigător este responsabil de acoperirea tuturor cheltuielilor referitoare la interpreți/ traducători/ traduceri.

Pentru persoanele propuse care au calitatea de salariați ai ofertantului, se va prezenta în mod obligatoriu orice document prin care să se demonstreze relația contractuală dintre persoanele nominalizate și ofertant (extras Revisal/ contract de muncă, etc.). În cazul în care se propune personal care nu este salariat al Prestatorului, fiecare astfel de personal va completa și va semna o declarație de disponibilitate semnată de

titular, cu referire strictă la obiectul contractului ce face obiectul prezentei proceduri(Formulare: **Model declarație de disponibilitate**).

Pe parcursul derulării contactului de achiziție publică, modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează conform prevederilor art. 162 din Anexa 1 (Normele metodologice) la HG nr. 395/2016.

Astfel, înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează numai cu acceptul autorității contractante, și nu reprezintă o modificare substanțială, așa cum este aceasta definită în art. 221 din Lege, decât în următoarele situații:

a) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin criteriile de calificare/selecție prevăzute în cadrul documentației de atribuire;

b) noul personal de specialitate nominalizat pentru îndeplinirea contractului nu obține cel puțin același punctaj ca personalul propus la momentul aplicării factorilor de evaluare.

În situațiile prevăzute anterior, contractantul are obligația de a transmite pentru noul personal documentele solicitate prin documentația de atribuire fie în vederea demonstrării îndeplinirii criteriilor de calificare/selecție stabilite, fie în vederea calculării punctajului aferent factorilor de evaluare.

Ofertantul se obligă să respecte legislația în vigoare care reglementează condițiile la locul de muncă conform modelului din secțiunea Formulare: **Model declarație referitoare la condițiile de muncă și de protecția muncii**.

5 Modul de întocmire a ofertei

Propunerea tehnică va fi elaborată astfel încât să rezulte că sunt îndeplinite în totalitate cerințele aferente Caietului de sarcini. Propunerea tehnică trebuie să reflecte asumarea de către ofertant a tuturor cerințelor și obligațiilor prevăzute în Caietul de sarcini.

Propunerea tehnică:

1. Ofertantul va prezenta o singură ofertă cu respectarea cerințelor Caietului de Sarcini.
2. Propunerea tehnică va fi întocmită în conformitate cu solicitările din caietul de sarcini, acestea fiind considerate minime și obligatorii.
3. Ofertantul are obligația de a face dovada conformității sistemului informatic oferit cu toate specificațiile tehnice cuprinse în caietul de sarcini.
4. Prezentarea modului de îndeplinire a cerințelor funcționale și tehnice solicitate în caietul de sarcini. Ofertantul va prezenta sub forma tabelara, explicațiile, valorile și documentele doveditoare pentru toate caracteristicile solicitate în caietul de sarcini (matrice de complianță).
5. Ofertantul va detalia modul în care echipamentele, componentele și produsele software oferite răspund la fiecare dintre cerințele enumerate în parte, specificând în clar identificatorul unic producător asociat fiecărui echipament, numărul de echipamente oferite pentru fiecare tip de echipament, configurația,




funcționalitățile și opțiunile acestora. Separat, vor fi prezentate de asemenea și funcționalitățile suplimentare, dacă este cazul. Nu se acceptă echipamente scoase din fabricație sau la finalul ciclului de vânzare. Se acceptă livrarea doar de echipamente noi.

6. 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.
7. Ofertantul va include în mod obligatoriu detalierea modalității de îndeplinire a tuturor specificațiilor tehnice aferente produselor software de bază/aplicații/echipamentelor hardware, consumabilelor de proces și, după caz, ale instalațiilor/utilajelor tehnice prevăzute în ofertă, sub formă de fișe tehnice din care să rezulte îndeplinirea cerințelor funcționale precizate în caietul de sarcini, respectiv documente care provin de la producători/organisme de certificare și inspecție/laboratoare de încercare, etc., din care să rezulte modul de îndeplinire a cerințelor;
8. Ofertantul va prezenta condițiile de vânzare, garanție și punere în funcțiune a tuturor produselor software de bază/aplicații/echipamentelor hardware, consumabilelor de proces și, după caz, ale instalațiilor/utilajelor tehnice prevăzute în ofertă.
9. Dacă Ofertantul este reprezentat de o asocierie, atunci se vor prezenta rolurile fiecărui membru al asocierii. Membrii asocierii își vor asuma în mod solidar răspunderea pentru realizarea tuturor activităților contractului. În cazul subcontractării, se va prezenta modul de abordare și gestionare a relației cu subcontractorii, în raport cu activitățile subcontractate.
10. Ofertantul va depune prin intermediul SEAP o înregistrare audio-video a sesiunii demonstrative, semnată cu semnătură electronică extinsă, până la data și ora limită de depunere a ofertelor, precizată în anunțul de participare.
11. Alte informații considerate semnificative de ofertant sau orice alte constrângeri, pentru evaluarea corespunzătoare a propunerii tehnice.
12. Ofertele ne-sustenabile/care nu pot fi fundamentate, de natură să nu asigure satisfacerea cerințelor din caietul de sarcini, vor fi respinse ca neconforme.

Notă - condiții generale și particulare:

1. Prin depunerea unei oferte, ofertantul acceptă în prealabil condițiile generale și particulare care guvernează acest contract, după cum sunt acestea prezentate în Documentația de atribuire, ca singură bază a acestei proceduri de atribuire, indiferent care sunt condițiile proprii de vânzare ale ofertantului.
2. Ofertanții au obligația de a analiza cu atenție documentația de atribuire și să pregătească oferta conform tuturor instrucțiunilor, formularelor, prevederilor contractuale și Caietului de sarcini conținute în această documentație.
3. Niciun cost suportat de operatorul economic pentru pregătirea și depunerea ofertei nu va fi rambursat. Toate aceste costuri vor fi suportate de către operatorul economic ofertant, indiferent de rezultatul procedurii.



4. Presumpția de legalitate și autenticitate a documentelor prezentate: ofertantul își asumă răspunderea exclusivă pentru legalitatea și autenticitatea tuturor documentelor prezentate în original și/sau copie în vederea participării la procedură.
5. Analizarea de către comisia de evaluare a documentelor prezentate de ofertanți nu angajează din partea acestora nicio răspundere sau obligație față de acceptarea acestora ca fiind autentice sau legale și nu înlătură răspunderea exclusivă a ofertantului sub acest aspect.
6. Specificațiile tehnice definite în cadrul prezentului caiet de sarcini corespund necesităților și exigențelor Autorității Contractante.
7. Orice referire la producători / mărci / tipuri / standarde / procedee / producție specifică /origine / certificări prezentate în caietul de sarcini sunt menționate doar pentru identificarea cu ușurință a tipului de produs/serviciu/certificare și vor fi considerate ca purtând mențiunea "sau echivalent".
8. Potențialii ofertanți pot vizita amplasamentele Beneficiarului pentru a obține datele necesare pentru elaborarea ofertei însoțită de o persoană desemnată din partea Autorității Contractante. Planificarea vizitei se va face la numărul de fax: +4021.316.0808 sau adresa de e-mail: valentin.vladu@onrc.ro. Potențialii ofertanți care intenționează să viziteze amplasamentele trebuie să transmită, cu cel puțin 2 zile lucrătoare înainte de data stabilită pentru vizita amplasamentului/amplasamentelor, o scrisoare prin care își anunță intenția de a participa la vizită. Participanții la vizita amplasamentelor sunt responsabili cu asigurarea mijloacelor de transport în vederea efectuării vizitei.

6 Criterii de atribuire

Criteriul de atribuire este "cel mai bun raport calitate-preț".

ALGORITM DE CALCUL

Evaluarea ofertelor se va face în ordinea descrescătoare a punctajului total obținut din punctajul tehnic și financiar, pe baza ponderilor prezentate în fișa de date a achiziției, pentru fiecare dintre criteriile respective.

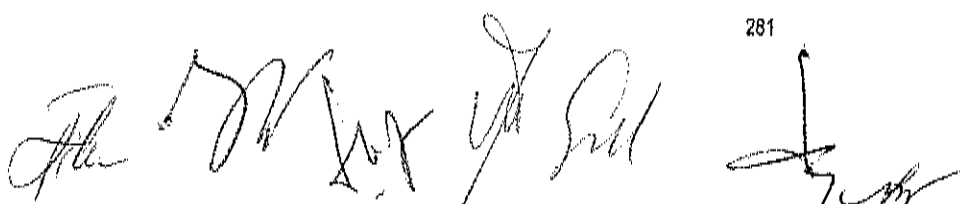
Oferta care obține cel mai mare număr de puncte va fi declarată câștigătoare.

Evaluarea ofertelor se va realiza pe baza următoarelor criterii și a punctajul aferent obținut de fiecare oferta evaluata.

Punctajul total acordat pentru fiecare ofertă se calculează pe baza formulei:

Punctaj Total Ofertant A = Punctaj „Prețul ofertei” Ofertant A + Punctaj “ Termen de executie contract” Ofertant A + Punctaj „Propunerea tehnică - Perioada de garanție a sistemului integrat” Ofertant A + Punctaj „Propunerea tehnică - Perioada Mentenanta software” Ofertant A + Punctaj „Propunerea tehnică - Capabilități soluție tehnică – Baza de date” Ofertant A + Punctaj „Propunerea tehnică - Experiența profesionala a personalului” Ofertant A + Punctaj „Propunerea tehnică – Planul de proiect” Ofertant A

281



Criteriile de evaluare sunt:

Nr. crt.	Factori de evaluare	Pondere %
1.	F1. Prețul ofertei	40
2.	F2. Termen de execuție contract	5
3.	F3. Perioada de garanție a sistemului integrat	6
4.	F4. Perioada Mentenanta software	16
5.	F5. Propunere tehnică – Capabilități soluție tehnică – Baza de date	18
6.	F6. Propunerea tehnică – Experiența profesionala a personalului	12
7.	F7. Propunerea tehnică – Planul de proiect	3
<i>Total</i>		100

Notă: în vederea comparării unitare a ofertelor, toate prețurile vor fi exprimate în cifre cu două zecimale și toate calculele se vor face cu rotunjire la 2 zecimale, conform funcției ROUND din Microsoft Excel – ROUND(formula, 2) – pentru fiecare din calculele aferente evaluării ofertelor. Funcția ROUND se va aplica pentru întreaga formulă de calcul, pentru fiecare etapa a calculului.

Pentru factorul F7, evaluarea se va face în funcție de calificativul foarte bine/bine/acceptabil/minim.

Clasamentul ofertelor se stabilește prin ordonarea descrescătoare a punctajelor respective, oferta câștigătoare fiind cea de pe primul loc, respectiv cea cu cel mai mare punctaj maxim total rezultat în urma aplicării criteriului de atribuire cel mai bun raport calitate-preț.

Departajarea ofertelor cu punctaj egal, situate pe primul loc: în cazul în care vor exista punctaje egale, autoritatea contractantă va departaja oferta castigatoare după punctajul maxim total obținut la criteriul prețul ofertei (fiind factorul cu ponderea cea mai mare). Dacă și după aceasta departajare există egalitate se vor departaja după punctajul obținut la Capabilități soluție tehnică - Baza de date. Dacă și după aceasta există egalitate se vor departaja după punctajul maxim obținut la criteriul -Mentenanță software. Dacă și după aceasta departajare există egalitate se vor departaja după punctajul obținut la criteriul Experiența profesională a ofertantului. Dacă și după aceasta departajare există egalitate se vor departaja după punctajul obținut la criteriul - Perioada de garanție a sistemului oferat. Dacă și după aceasta departajare există egalitate se vor departaja după punctajul obținut la criteriul Termen de execuție contract. Dacă și după aceasta departajare există egalitate se vor departaja după punctajul obținut la criteriul Planul de proiect. În cazul în care persista egalitatea, pentru departajare Autoritatea va solicita operatorilor economici în cauză, noi propuneri financiare..

6.1 Descrierea modalității de punctare a factorului de evaluare "Prețul ofertei" (F1)

Factor de evaluare	Modalitate de punctare	Punctaj maxim
--------------------	------------------------	---------------

1. Prețul ofertei	Punctajul financiar se acordă astfel: a. Pentru cel mai mic dintre prețurile oferite se acordă 40 de puncte; b. Pentru alt preț decât cel prevăzut la litera a) se acordă punctaj astfel:	40 puncte
	Punctaj Financiar Ofertant A = Preț minim ofertat ÷ Preț Ofertant A × 40	
	Se vor compara prețurile fără TVA prezentate în propunerea financiară.	

6.2 Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică -- Termen de execuție contract" (F2)

Număr maxim de puncte: 5 puncte.

Factor de evaluare	Modalitate de punctare	Punctaj maxim
1. Termen de execuție contract	<p>Pentru oferta/ofertele care prezintă o reducere cu 90 de zile a termenului de execuție a contractului față de termenul maxim prevăzut în caietul de sarcini, se va acorda punctajul maxim.</p> <p>Pentru ofertarea unui termen de execuție a contractului redus cu mai mult de 90 zile nu se acordă punctaj suplimentar.</p> <p>Pentru restul ofertelor admisibile, punctele se vor calcula utilizând următoarea formulă: Algoritm de calcul: $P \text{ termen } (n) = \text{Termen}(n) / \text{Termen } (90 \text{ zile}) \times 5 \text{ puncte}$, unde: P termen (n) - punctajul obținut de către oferta admisibilă aflată în evaluare; Termen (90 zile) – numărul de zile de reducere a termenului de execuție a contractului pentru care se acordă punctajul maxim, respectiv 90 de zile; Termen (n) – numărul de zile de reducere a termenului de execuție a contractului prezentat în oferta admisibilă aflată în evaluare.</p> <p>Nota 1: Termenul de execuție a contractului este de maxim 18 luni. (în cazul ofertării unui termen de execuție a contractului de peste 18 luni oferta va fi considerată neconformă).</p> <p>2. Nu se acordă punctaj intermediar pentru intervale mai mici de</p>	5 puncte

	1 zi. 3. Pentru un termen de executare a contractului de 18 luni se acorda zero puncte.	
--	--	--

6.3 Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică – Perioada de garanție a sistemului integrat" (F3)

Număr maxim de puncte: 6 puncte.

Factor de evaluare	Modalitate de punctare	Punctaj maxim
1. Perioada de garanție (PG) a sistemului integrat	Pentru oferta/ofertele care prezintă o garanție extinsă gratuită mai mare (hardware, software de bază și aplicații) cu 24 de luni față de durata minimă prevăzută în Caietul de sarcini (36 luni) se acorda punctajul maxim.	6 puncte
	Pentru restul ofertelor admisibile, punctele se vor calcula utilizând următoarea formulă: Algoritm de calcul: punctajul se acordă proporțional, astfel: $P(n) = PG(n)/PG(\text{maxim}) \times 6$ puncte, unde $P(n)$ – Punctajul obținut de oferta "n" $PG(n)$ – Perioada de garanție extinsă gratuită prezentată în oferta admisibilă aflată în evaluare. $PG(\text{maxim})$ – Perioada de garanție extinsă gratuită maximă pentru care se acorda punctaj, respectiv de 24 de luni	
	Nota: 1) Perioada de garanție – durata minimă solicitată în Caietul de sarcini este de 36 de luni de la data semnării procesului verbal de punere în funcțiune, iar cea maximă pentru care se acorda punctaj este de 60 de luni de la data semnării procesului verbal de punere în funcțiune. 2) Sub termenul de 36 luni ofertele vor fi declarate neconforme. 3) Pentru o perioadă de garanție gratuită mai mare de 60 luni ofertele nu vor fi punctate suplimentar. 4) Pentru o garanție de 36 de luni se acorda zero puncte. 5) PG va fi exprimată în luni calendaristice, fără zecimale. Nu se acordă punctaj intermediar pentru intervale mai mici de 1 luna.	

6.4 Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică – Perioada mentenanța software" (F4)

Număr maxim de puncte: 16 puncte.

Factor de evaluare	Modalitate de punctare	Punctaj maxim
1. Mentenanța software	<p>Mentanța se referă la activitatea de monitorizarea proactivă a funcționării sistemului dezvoltat, la depanarea erorilor din cadrul aplicației (corectiva) prin aplicarea de corecții (patches) precum și la modificări ale aplicației (evolutiva) datorită unor schimbări legislative care pot conduce la necesitatea modificării aplicațiilor conform cerințelor caietului de sarcini.</p> <p>Pentru oferta/ofertele care prezintă o mentenanță software gratuită egală sau mai mare cu 48 de luni față de durata minimă prevăzută în Caietul de sarcini (12 luni) se acordă punctajul maxim 16 puncte.</p> <p>Pentru restul ofertelor admisibile, punctele se vor calcula utilizând următoarea formulă:</p> <p>Algoritm de calcul:</p> <p>punctajul se acordă proporțional, astfel:</p> $P_{\text{mentenanță}}(n) = \frac{\text{Ment_oferta}}{\text{Ment_max}} \times 16$ <p>unde:</p> <p>$P_{\text{mentenanță}}(n)$ este punctajul obținut de oferta "n" pentru durata serviciului de mentenanță gratuită extinsă al ofertei evaluate.</p> <p>Ment_oferta este durata mentenanței gratuite extinse din cadrul ofertei pentru care se face evaluarea</p> <p>Ment_max este durata maximă extinsă a mentenanței gratuite oferite (exprimată în luni), respectiv 48 luni.</p> <p>Nota:</p> <ol style="list-style-type: none"> 1) Perioada de mentenanță minimă solicitată în Caietul de sarcini este de 12 de luni de la data semnării procesului verbal de punere în funcțiune, iar cea maximă ce poate fi punctată este de 60 de luni de la data semnării procesului verbal de punere în funcțiune. 2) Sub termenul de 12 luni ofertele vor fi declarate neconforme. 3) Pentru o perioadă de mentenanță gratuită mai mare de 60 luni ofertele nu vor fi punctate suplimentar. 4) Pentru o mentenanță de 12 de luni se acordă zero puncte. 5) Perioada de mentenanță gratuită va fi exprimată în luni 	16 puncte

	calendaristice, fără zecimale. Nu se acordă punctaj intermediar pentru intervale mai mici de 1 luna.	
--	--	--

6.5 Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică – Capabilități soluție tehnică – Baza de date" (F5)

Număr maxim de puncte: 18 puncte.

Factor de evaluare	Modalitate de punctare	Punctaj maxim
1. Baza de date	<p>Pentru asigurarea unei toleranțe la defecte hardware sau nefuncționare planificată, scalabilitate și disponibilitate crescută a sistemului prin:</p> <ul style="list-style-type: none"> - instalarea unei singure baze de date pe mai multe noduri într-o arhitectură de tip cluster activ-activ; - acces concurrent, simultan de pe toate nodurile cluster-ului pentru orice obiect al bazei de date; - modificarea automată și dinamică a parametrilor de memorie astfel încât baza de date să se adapteze permanent la tipul de încărcare OLTP sau de tip DW, oferind astfel cele mai bune performanțe; - asigurarea balansării încărcării între noduri la nivelul cererilor și execuțiilor astfel încât tranzacțiile începute pe un nod vor putea fi reluate transparent și automat pe unul din nodurile rămase funcțional, după ce nodul inițial devin indisponibil, astfel încât utilizatorii finali nu vor simți nici o modificare în buna funcționare a aplicației, - reorganizarea, mutarea și redefinirea de fișiere de date, tabele și indecși fără blocarea activității utilizatorilor la datele aflate în curs de modificare, indiferent de dimensiunea acestora; - permiterea diferitelor metode de indexare a datelor, cum ar fi indexarea de tip B-Tree, bitmap, bazată pe funcții sau chiar definirea de tabelele de tip index în care datele să fie ordonate după o anumita coloana; - ajustarea dinamică și automată a parametrilor de memorie astfel încât dimensionarea sa fie realizată în concordanță cu tipul de operații ce se desfășoară la un moment dat; - utilizarea unor mecanisme de asigurare a consistenței datelor în 	18 puncte

	<p>situația nefavorabilă a unui incident, cum ar fi interogarea directă a tabelelor care să prezinte datele exact cum erau la un moment anterior în timp, anularea unei tranzacții sau restaurare rapida a datelor;</p> <ul style="list-style-type: none"> - să ofere nativ mecanisme care să permită interogarea istoricului modificărilor unei tabele, indiferent de tipul activităților (DDL sau DML) - recuperarea rapida în urma erorilor umane prin posibilitatea de a recupera online rânduri sau tabele șterse de utilizatori fără a necesita date de backup sau dezvoltarea de proceduri utilizator ; - partiționarea logica a tabelelor mari în scopul reducerii timpului de acces la date, folosind mai multe criterii de partiționare (interval, funcții hash sau listă de valori) precum și posibilitatea de a partiționa tabelele legate prin chei referențiale; - toleranță la defecte hardware sau nefuncționare planificată astfel încât să fie oferită o disponibilitate de tip 24x7 în cazul apariției unei defecțiuni hardware sau software la unul din serverele clusterului de baza de date; - balansarea încărcării între noduri la nivelul cererilor și execuțiilor pe baza de date cluster și posibilitatea de a interoga memoria cache de pe celelalte noduri, oferind o încărcare uniforma a clusterului; - în cazul apariției unor erori hardware sau software în clusterul de baza de date, acestea trebuie sa fie tratate automat de mecanismele interne ale bazei de date astfel încât reconectarea la nodul sau nodurile ramase disponibile să se facă în mod transparent față de aplicații și utilizatori; - posibilitatea de a adăuga la nevoie servere de baze de date suplimentare în cluster, servere care vor fi active imediat și vor prelua din încărcarea bazei de date, fără a necesita oprirea serviciilor la nivel de cluster; - mecanisme avansate de backup, complet sau de tip incremental, care să permită backup-ul întregii instanțe de baze de date, fără oprirea acesteia, dar și mecanisme de restaurare care să poată fi folosite în funcție de nevoie, independent pentru fiecare baza de date, individual la nivel de fișier de date, la nivel de tabelă și chiar de bloc de date; - comprimarea automata a backup-urilor, fie ele complete sau de tip incremental, indiferent de tipul de date stocate în baza de date, 	
--	---	--

	<p>inclusiv pentru cele binare de tip BLOb (Binary Large Object);</p> <p>- posibilitatea de a marca anumite fișiere de date care nu se mai modifica, ca fiind de tip „read-only” în vederea excluderii acestora din operațiile ulterioare de backup (complet sau incremental) ale bazei de date,</p> <p>se acordă 18 puncte.</p> <p>Ofertanții vor descrie în detaliu în cadrul ofertei modul de funcționare a componentelor sistemului cu referire la aspectele supuse evaluării pentru acest criteriu de atribuire.</p> <p>În cazul în care descrierea tehnică din ofertă este incompletă (adică nu acoperă toate aspectele solicitate respectiv funcționalitățile oferite de componentele propuse), nu se acorda punctajul aferent în cadrul acestui criteriu de atribuire.</p>	
--	--	--

6.6 Descrierea modalității de punctare a factorului de evaluare “Propunerea tehnică - Experiența profesională a personalului” (F6)

Prin acest factor se va realiza evaluarea experienței profesionale a persoanelor propuse pentru anumite poziții de experți solicitate în Caietul de sarcini. Persoanele pentru care se va face evaluarea vor avea responsabilitatea realizării efective a activităților și proceselor de execuție aferente derulării contractului. Factorul de evaluare este experiența profesională a personalului ofertantului concretizată în numărul de proiecte în care personalul a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

Număr maxim de puncte: 12.

Acordarea punctajului „Experiența profesională a personalului” se va face în felul următor:

Expert cheie	Număr maxim de puncte
Manager de proiect	2
Expert arhitect soluție	2
Expert coordonare analiza	2
Expert coordonare dezvoltare software	2
Expert coordonare testare	2
Expert securitatea informatiei	2
Total	12

Punctajul aferent experienței persoanelor propuse ca experți-cheie pentru pozițiile Expert arhitect soluție, Expert coordonare analiza, Expert coordonare dezvoltare software, Expert coordonare testare și Expert securitatea informației se va acorda astfel pentru fiecare în parte:

- a) pentru experiența persoanei propuse constând în implicarea între 2 și 4 proiecte sau contracte de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract se acordă 1/4 din punctajul maxim alocat poziției respective;
- b) pentru experiența persoanei propuse constând în implicarea între 5 și 7 proiecte sau contracte de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract se acordă 1/2 din punctajul maxim alocat poziției respective;
- c) pentru experiența persoanei propuse constând în implicarea în minim 8 proiecte sau contracte de dezvoltare/ implementare/ extindere sistem informatic în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract se acordă punctajul maxim alocat poziției respective.

Punctajul aferent experienței persoanei propuse pentru poziția de Manager de proiect se va acorda astfel:

- a) pentru experiența persoanei propuse constând în implicarea între 2 și 4 proiecte în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract se acordă 1/4 din punctajul maxim alocat poziției respective;
- b) pentru experiența persoanei propuse constând în implicarea între 5 și 7 proiecte în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract se acordă 1/2 din punctajul maxim alocat poziției respective;
- c) pentru experiența persoanei propuse constând în implicarea în minim 8 proiecte în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract se acordă punctajul maxim alocat poziției respective.

Nu se accepta persoane propuse pe poziții de experți fără nici un fel de experiență, respectiv fără demonstrarea implicării în cel puțin un proiect sau contract în care a îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.

Nu va fi punctată experiența profesională a unor persoane propuse pe poziții de experți suplimentare față de cele menționate în tabelul de mai sus, chiar dacă acestea îndeplinesc cerințele minimale și dovedesc experiența similară așa cum este descrisă în acest caiet de sarcini.

Pentru demonstrarea experienței profesionale solicitate, Ofertanții trebuie să prezinte în cadrul ofertei tehnice documente relevante: recomandări emise de beneficiarul final al proiectului, semnate sau contrasemnate de către Autoritatea Contractantă/beneficiarul privat în calitate de beneficiar final al proiectului sau alte documente edificatoare semnate de acesta.

Pentru fiecare document propus, se vor prezenta datele de contact actualizate ale beneficiarului final al proiectului (denumire, adresă poștală, adresă electronică, telefon, fax), astfel încât reprezentanții legali sau

289



Împuțerniciți ai beneficiarului final să fie în măsură să confirme cele prezentate în documentul/documentele propus(e) [(recomandare/recomandări sau alt(e) document(e)).

În acest sens, ofertantul va prezenta datele respective în cadrul documentului relevant propus pentru demonstrarea experienței profesionale solicitate sau în cadrul unui document centralizator separat, ce va cuprinde datele menționate la paragraful anterior.

În urma verificării informațiilor și a dovezilor furnizate de către ofertanți, Autoritatea Contractantă poate solicita și alte documente/informații care să clarifice experiența profesională solicitată. De asemenea, Autoritatea Contractantă își rezerva dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experiența profesională, în vederea confirmării celor prezentate de către ofertanți.

Punctajul va fi acordat numai pentru proiectele sau contractele pentru care documentele prezentate dovedesc experiența solicitată pentru fiecare persoană propusă pentru o anumită poziție de expert.

6.7 Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică – Planul de proiect" (F7)

Prin acest criteriu se va realiza evaluarea gradului de corectitudine și adaptare al planului de implementare a contractului prin raportare la nevoile proiectului.

Număr maxim de puncte: **3 puncte.**

Acordarea punctajului „Demonstrarea gradului de corectitudine și adaptare al planului de implementare a contractului, la nevoile proiectului” se va face în felul următor:

Element evaluat	Calificativ	Punctaj
În cadrul planului propus pentru implementarea contractului: 1. Au fost identificate punctele cheie de control / jaloanele ("milestones"), dar acestea se încadrează în cel puțin două dintre următoarele cazuri: - sunt relevante în cea mai mare parte / în totalitate prin raportare la cerințele caietului de sarcini și modalitatea efectivă de realizare a activităților; - sunt poziționate în cea mai mare parte / în totalitate corect în timp (în graficul de implementare a contractului); - sunt corelate corespunzător în cea mai mare parte / în totalitate cu succesiunea logică și cronologică a activităților prezentată în graficul de implementare a contractului, cu respectarea metodologiei propuse de implementare a contractului; 2. Principalele activități au fost explicitate în graficul de implementare a contractului și sunt detaliate în subactivități. 3. Drumul critic este aliniat în cea mai mare parte cu metodologia de management a serviciilor IT&C propusă pentru implementarea contractului. 4. Resursele alocate sunt corelate corespunzător în cea mai mare parte / în totalitate cu duratele activităților și efortul estimat pentru acestea, prezentate în planul de proiect.	Foarte bine	3

290



<p>În cadrul planului propus pentru implementarea contractului:</p> <p>1. Au fost identificate punctele cheie de control / jaloanele ("milestones"), dar acestea se încadrează în cel puțin două dintre următoarele cazuri:</p> <ul style="list-style-type: none"> - sunt parțial (în mică măsură) semnificative / relevante prin raportare la cerințele caietului de sarcini și modalitatea efectivă de realizare a activităților; - sunt poziționate în mod parțial (în mică măsură) corect în timp (în graficul de implementare a contractului); - sunt corelate corespunzător în mod parțial (în mică măsură) cu succesiunea logică și cronologică a activităților prezentată în graficul de implementare a contractului, cu respectarea metodologiei propuse de implementare a contractului; <p>2. Principalele activități au fost explicitate în graficul de implementare a contractului și sunt detaliate în subactivități.</p> <p>3. Drumul critic este aliniat parțial cu metodologia de management a serviciilor IT&C propusă pentru implementarea contractului.</p> <p>4. Resursele alocate sunt corelate parțial cu duratele activităților și efortul estimat pentru acestea, prezentate în planul de proiect.</p>	Bine	2
<p>În cadrul planului propus pentru implementarea contractului:</p> <p>1. Au fost identificate punctele de cheie de control / jaloanele ("milestones"), dar acestea se încadrează în cel puțin unul dintre următoarele cazuri:</p> <ul style="list-style-type: none"> - nu sunt semnificative / relevante prin raportare la cerințele caietului de sarcini și modalitatea efectivă de realizare a activităților; - nu sunt poziționate corect în timp (în graficul de implementare a contractului); - nu sunt corelate corespunzător cu succesiunea logică și cronologică a activităților prezentată în graficul de implementare a contractului, sau nu respectă metodologia propusă de implementare a contractului; <p>2. Principalele activități au fost explicitate în graficul de implementare a contractului, dar acestea nu sunt detaliate în subactivități.</p> <p>3. Drumul critic nu este aliniat cu metodologia de management a serviciilor IT&C propusă pentru implementarea contractului.</p> <p>4. Resursele alocate nu sunt corelate cu duratele activităților și efortul estimat pentru acestea, prezentate în planul de proiect.</p>	Acceptabil	1

Ofertantul va prezenta gradul de corectitudine și adaptare a planului de implementare a contractului prin raportare la nevoile proiectului conform Anexe 2 - Formular propunere tehnică.

7 Cerințe pentru sesiunea demonstrativă

Având în vedere complexitatea sistemului ce trebuie implementat și importanța respectării termenului de implementare menționat în prezentul document, asumat și prin contractul de finanțare, Autoritatea Contractantă va solicita ofertanților prezentarea în cadrul unei sesiuni demonstrative ce se va desfășura la sediul Autorității Contractante modalitatea prin care soluțiile software oferite incluse în oferta tehnică răspund nativ (out-of-the-box, respectiv prin funcționalități deja existente în cadrul produselor software oferite, fără a necesita servicii suplimentare de dezvoltare software) la unele cerințe minime din caietul de sarcini.

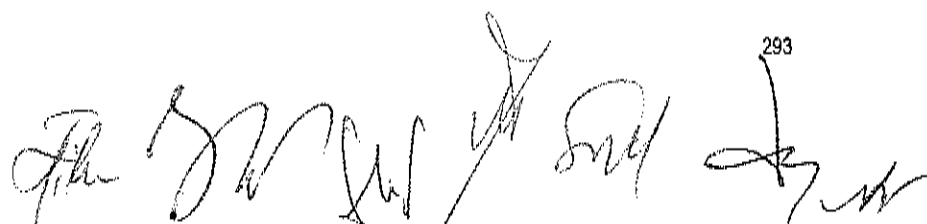
Cerințele minime ce vor fi prezentate în cadrul sesiunii demonstrative – Generator de formulare (online și offline) care răspund nativ (out-of-the-box, respectiv prin funcționalități deja existente în cadrul produselor software oferite, fără a necesita servicii suplimentare de dezvoltare software) la unele cerințe minime din caietul de sarcini.

UC1 – Crearea unui formular

Descriere	Utilizatorii (cu drepturi de creare) accesează software-ul și încep procesul de creare a unui formular pentru o anumită procedură în 3 moduri diferite: <ol style="list-style-type: none">1. Prin crearea formularului de la zero.2. Prin crearea formularului pe baza formularelor existente stocate în instrument.3. Prin crearea formularului din șabloane implicite.
Actori	<ol style="list-style-type: none">1. Administrator local de date.2. Utilizator de bază (gestionar formular).
Precondiții	<ol style="list-style-type: none">1. Furnizarea accesului la software.2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul).3. UC: Desemnarea administratorului de date locale.4. UC: Înregistrarea altor utilizatori.
Flux de bază: Creați un formular de la zero	<ol style="list-style-type: none">1. Utilizatorul de bază (gestionarul formularelor) se conectează la software.2. Utilizatorul de bază (gestionarul formularului) indică faptul că el / ea dorește să creeze un formular în pagina inițială a instrumentului.3. Utilizatorul de bază (gestionar formular) selectează opțiunea de a crea un formular de la zero (opțiune implicită).4. Utilizatorul de bază (gestionarul formularului) introduce numele formularului (care va constitui identificatorul său unic), indică tipul de procedură pe care îl va acoperi și limbile formularului.5. Utilizatorul de bază (gestionarul formularului) adaugă secțiuni ale formularului și câmpuri pentru fiecare secțiune, după cum este necesar, inclusiv definirea regulilor de validare și a dependențelor pentru fiecare câmp de date selectat.6. Utilizatorul de bază (gestionarul formularului) salvează formularul (fie pentru editarea ulterioară a formularelor, fie pentru finalizarea creării formularului) și indică starea formularului (schită, activ sau arhivat).

<p>Flux alternativ A:</p> <p>Creați un formular reutilizând un formular existent</p>	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularului) selectează opțiunea de a reutiliza un formular existent pentru a crea un formular nou. 2. Utilizatorul de bază (gestionarul formularelor) este redirecționat către o pagină care conține toate formularele create. Utilizatorul le poate sorta și filtra în funcție de criterii specifice de pe ecran sau poate efectua o căutare. 3. Utilizatorul de bază poate căuta printre formularele existente adăugând cuvinte cheie într-un șir de căutare sau filtrând pe baza altor caracteristici stocate ale formularului, precum data creării, procedura acoperită, numele de utilizator al creatorului formularului etc. 4. Utilizatorul de bază (gestionarul formularelor) selectează formularul care urmează să fie refolosit din formularele salvate. 5. Utilizatorul de bază (gestionarul formularului) introduce numele noului formular (care va constitui identificatorul său unic), selectează tipul de procedură pe care îl va acoperi și selectează locația de stocare către care trebuie trimise răspunsurile la formular. 6. Utilizatorul de bază (gestionarul formularului) modifică formularul după cum este necesar. 7. Utilizatorul de bază (gestionarul formularului) salvează formularul (fie pentru editarea ulterioară a formularelor, fie pentru a finaliza crearea formularului) și indică starea formularului (schită, activ sau arhivat).
<p>Flux alternativ B:</p> <p>Reutilizați un șablon existent</p>	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularelor) selectează opțiunea de a crea un formular dintr-un șablon existent. Utilizatorul de bază este redirecționat către o pagină care conține toate șabloanele disponibile. Utilizatorul le poate sorta și filtra în funcție de criterii specifice de pe ecran sau poate efectua o căutare. 2. Utilizatorul de bază (gestionarul formularului) caută printre șabloane adăugând cuvinte cheie într-un șir de căutare sau alte caracteristici stocate ale formularului, cum ar fi procedura acoperită, limbile disponibile etc. 3. Utilizatorul de bază (gestionarul formularului) selectează șablonul pe care dorește să îl folosească pentru a crea noul formular. Utilizatorul de bază (gestionarul formularelor) poate vedea formularele existente create pe baza șablonului selectat. Utilizatorul de bază (gestionarul formularului) continuă cu crearea unui formular bazat pe șablonul selectat, noul formular este creat. 4. Utilizatorul de bază (gestionarul formularului) adaugă secțiuni și câmpuri la formular după cum este necesar. 5. Utilizatorul de bază (gestionarul formularului) salvează formularul (fie pentru editarea ulterioară a formularelor, fie pentru finalizarea creării formularului) și indică starea formularului (schită, activ sau arhivat).
<p>Post-condiții</p>	<ol style="list-style-type: none"> 1. Formularul este creat cu un identificator unic. 2. Formularul este stocat. 3. Formularul poate fi refolosit, editat, tradus sau publicat (dacă starea este activă).

293



UC2 – Editarea un formular

Descriere	Utilizatorul de bază (gestionarul formularului), creatorul formularelor create anterior (dar nu în stare activă) poate continua editarea conținutului și structurii formularului și poate edita temele, stilurile, culorile, fonturile și grafica formularelor salvate.
Actori	Utilizator de bază (gestionare formular)
Precondiții	<ol style="list-style-type: none"> 1. Furnizarea accesului la software. 2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul). 3. UC: Numirea administratorului de date locale. 4. UC: Înregistrarea altor utilizatori. 5. UC: Crearea unui formular.
Flux de bază:	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularelor) se conectează la software. 2. Utilizatorul de bază (gestionarul formularului) caută formularul de editat. 3. Utilizatorul de bază (gestionarul formularului) selectează formularul de editat. 4. Utilizatorul de bază (gestionarul formularului) face clic pe opțiunea de editare. 5. Utilizatorul de bază (gestionarul formularului) intră în fereastra ediției în cazul în care el / ea este capabil să editeze conținutul, structura și imaginile. 6. Utilizatorul de bază (gestionarul formularului) salvează modificările formularului și indică starea formularului (schită, activ sau arhivat). 7. Utilizatorul de bază (gestionarul formularului) salvează formularul (fie pentru editarea ulterioară a formularelor, fie pentru a finaliza crearea formularului) și indică starea formularului (schită, activ sau arhivat).
Post-condiții	<ol style="list-style-type: none"> 1. Formularul creat este editat. 2. Formularul este salvat. 3. Formularul este indicat ca „activ” (dacă utilizatorul l-a activat). 4. Formularul poate fi refolosit, editat, tradus sau publicat (dacă starea este activă).


UC3 – Traducerea unui formular

Descriere	Utilizatorii de bază (gestionarii formularelor) și administratorii de date locale vor putea traduce câmpurile formularelor și mesajele informative printr-un serviciu de traducere automat sau manual.
Actori	<ol style="list-style-type: none"> 1. Administrator local de date 2. Utilizatori de bază (gestionar formular)

Precondiții	<ol style="list-style-type: none"> 1. Furnizarea accesului la software. 2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul). 3. UC: Desemnarea administratorului de date locale. 4. UC: Înregistrarea altor utilizatori de la aceeași autoritate. 5. UC: Crearea unui formular. 6. UC: Editarea unui formular.
Flux de bază: Folosirea unui serviciu de traducere automată	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularelor) se conectează la software. 2. Utilizatorul de bază (gestionarul formularelor) accesează formularele existente. 3. Utilizatorul de bază (gestionarul formularelor) alege să adauge același formular într-o altă limbă printr-un serviciu de traducere automată. 4. Utilizatorul de bază (gestionarul formularelor) alege o limbă din lista celor 24 de limbi oficiale ale UE, precum și islandeză și norvegiană. 5. Utilizatorul de bază (gestionarul formularelor) primește traducerea automată furnizată de instrument. 6. Utilizatorul de bază (gestionarul formularului) examinează versiunea tradusă a formularului și o editează după cum este necesar. 7. Utilizatorul de bază (gestionarul formularului) salvează modificările formularului și indică starea formularului / formularelor (schiță, activ sau arhivat). 8. Utilizatorul de bază (gestionarul formularului) inițiază publicarea formularului indicat ca „activ”.
Flux alternativ A: Traduceți manual formularul	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularului) accesează formularul. 2. Utilizatorul de bază (gestionarul formularelor) alege să adauge manual un formular în altă limbă. 3. Utilizatorul de bază (gestionarul formularului) umple din nou câmpurile noii versiuni a formularului în noua limbă. 4. Utilizatorul de bază (gestionarul formularului) examinează noua versiune a formularului și o editează după cum este necesar. 5. Utilizatorul de bază (gestionarul formularului) salvează modificările. 6. Utilizatorul de bază (gestionarul formularului) salvează modificările formularului și indică starea formularului (schiță, activ sau arhivat).
Post-condiții	<ol style="list-style-type: none"> 1. Formularele sunt traduse. 2. Formularul poate fi refolosit, editat sau publicat (dacă starea este activă).

UC4 – Publicarea unui formular

295



Descriere	Utilizatorii (cu drepturi de creație) publică un formular.
Actori	<ol style="list-style-type: none"> 1. Administrator local de date. 2. Utilizator de bază (gestionar formular).
Precondiții	<ol style="list-style-type: none"> 1. Furnizarea accesului la software. 2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul). 3. UC: Desemnarea administratorului de date locale. 4. UC: Înregistrarea altor utilizatori. 5. UC: Crearea unui formular 6. UC: Editarea unui formular 7. UC: Traducerea unui formular 8. UC: Căutarea unui formular
Flux de bază: Publicarea unui formular după crearea unui formular	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularelor) se conectează la software. 2. Utilizatorul de bază (gestionarul formularelor) creează un formular. 3. Utilizatorul de bază (gestionarul formularului) stabilește starea formularului creat la „activ”. 4. Utilizatorul de bază (gestionarul formularului) inițiază publicarea formularului (posibil doar dacă formularul este indicat ca „activ”), făcându-l disponibil pentru utilizarea sa practică (trimiterea informațiilor) pe orice site web.
Flux alternativ A: Publicarea unui formular după editarea unui formular	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularelor) se conectează la software. 2. Utilizatorul de bază (gestionarul formularului) face clic pe căutarea de pe pagina principală. 3. Utilizatorul de bază (gestionarul formularelor) este redirecționat către o pagină care conține toate formularele create. Utilizatorul le poate sorta și filtra în funcție de criterii specifice de pe ecran sau poate efectua o căutare. 4. Utilizatorul de bază poate căuta printre formularele existente adăugând cuvinte cheie într-un șir de căutare sau filtrând pe baza altor caracteristici stocate ale formularului, precum data creării, procedura acoperită, numele de utilizator al creatorului formularului etc. 5. Utilizatorul de bază (gestionarul formularelor) selectează formularul care urmează să fie editat din formularele salvate („editarea” este posibilă numai pentru formularele care nu sunt „active”). 6. Utilizatorul de bază (gestionarul formularului) editează formularul care urmează să fie publicat și setează starea formularului la „activ”.

	<p>7. Utilizatorul de bază (gestionarul formularului) salvează modificările aduse formularului care urmează să fie publicat.</p> <p>8. Utilizatorul de bază (gestionarul formularului) vizualizează formularul care urmează să fie publicat.</p> <p>9. Utilizatorul de bază (gestionarul formularului) inițiază publicarea formularului (posibil doar dacă formularul este indicat ca „activ”), făcându-l disponibil pentru utilizarea sa practică (trimiterea informațiilor) pe orice site web.</p>
<p>Flux alternativ B:</p> <p>Publicarea unui formular după traducerea unui formular</p>	<p>1. Utilizatorul de bază (gestionarul formularelor) se conectează la software.</p> <p>2. Utilizatorul de bază (gestionarul formularului) face clic pe căutarea de pe pagina principală.</p> <p>3. Utilizatorul de bază (gestionarul formularelor) este redirecționat către o pagină care conține toate formularele create. Utilizatorul le poate sorta și filtra în funcție de criterii specifice de pe ecran sau poate efectua o căutare.</p> <p>4. Utilizatorul de bază poate căuta printre formularele existente adăugând cuvinte cheie într-un șir de căutare sau filtrând pe baza altor caracteristici stocate ale formularului, precum data creării, procedura acoperită, numele de utilizator al creatorului formularului etc.</p> <p>5. Utilizatorul de bază (gestionarul formularelor) selectează formularul care urmează să fie tradus din formularele salvate.</p> <p>6. Utilizatorul de bază (gestionarul formularului) completează traducerea formularului după cum este necesar și indică starea formularului ca „activ”.</p> <p>7. Utilizatorul de bază (gestionarul formularului) salvează modificările aduse formularului tradus.</p> <p>8. Utilizatorul de bază (gestionarul formularului) vizualizează formularul tradus care urmează să fie publicat.</p> <p>9. Utilizatorul de bază (gestionarul formularului) inițiază publicarea formularului (posibil doar dacă formularul este indicat ca „activ”), făcându-l disponibil pentru utilizarea sa practică (trimiterea informațiilor) pe orice site web.</p>
<p>Flux alternativ C:</p> <p>Publicarea unui formular după ce căutați un formular</p>	<p>1. Utilizatorul de bază (gestionarul formularelor) se conectează la software.</p> <p>2. Utilizatorul de bază (gestionarul formularului) face clic pe căutarea de pe pagina principală.</p>

297



	<p>3. Utilizatorul de bază (gestionarul formularelor) este redirecționat către o pagină care conține toate formularele create. Utilizatorul le poate sorta și filtra în funcție de criterii specifice de pe ecran sau poate efectua o căutare.</p> <p>4. Utilizatorul de bază poate căuta printre formularele existente adăugând cuvinte cheie într-un șir de căutare sau filtrând pe baza altor caracteristici stocate ale formularului, precum data creării, procedura acoperită, numele de utilizator al creatorului formularului etc.</p> <p>5. Utilizatorul de bază (gestionarul formularelor) selectează formularul care urmează să fie publicat din formularele salvate. Formularele care urmează să fie publicate fără a fi necesare mai întâi editarea vor fi în stare „activă”.</p> <p>6. Utilizatorul de bază (gestionarul formularului) vizualizează formularul tradus care urmează să fie publicat.</p> <p>7. Utilizatorul de bază (gestionarul formularului) inițiază publicarea formularului (posibil doar dacă formularul este indicat ca „activ”), făcându-l disponibil pentru utilizarea sa practică (trimiterea informațiilor) pe orice site web.</p>
Post-condiții	<ol style="list-style-type: none"> 1. Formularul este disponibil pentru utilizarea sa practică (transmiterea informațiilor) pe orice site web în care formularul va fi disponibil cetățenilor și / sau întreprinderilor. 2. Va include un mecanism de control în cadrul generatorului de formulare. Acest mecanism va valida: <ul style="list-style-type: none"> • Statutul formularului (adică activ și nu expirat); și • Regulile de validare a datelor pe câmp. <p>Un astfel de mecanism implică faptul că, indiferent de tipul de stocare implementat (intern sau extern), formularele completate vor fi mai întâi transferate și validate de către generatorul de formulare înainte de transferul acestuia în locația de stocare selectată.</p> <p>În cazul în care formularul nu mai este activ, va fi afișat un mesaj de eroare și conținutul nu va fi transferat în locația de stocare.</p> <p>În cazul în care regulile comerciale (validarea datelor) nu sunt respectate, va fi afișat un mesaj de eroare descriptiv, iar conținutul nu va fi transferat la locația de stocare.</p> <p>Dacă nu sunt găsite erori sau dacă erorile legate de regulile de afaceri (validarea datelor) sunt corectate, conținutul formularului va fi transferat la locația de stocare (baza de date) selectată.</p>

UC5 – Gestionarea setărilor formularelor stocate

Descriere	Administratorii locali de date și utilizatorii de bază (gestionarii formularelor) vor putea gestiona setările formularelor, cum ar fi setările generale, setările elementelor de text, setările pentru participanți și acces, notificările și setările de gestionare a datelor și setările de control al publicării. Utilizatorii de bază (vizualizatori de formulare) vor putea vizualiza doar setările formularelor.
Actori	<ol style="list-style-type: none"> 1. Utilizator de bază (gestionar formular) 2. Utilizator de bază (vizualizator formular) 3. Administrator local de date
Precondiții	<ol style="list-style-type: none"> 1. Furnizarea accesului la software. 2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul). 3. UC: Desemnarea administratorului de date locale. 4. UC: Înregistrarea altor utilizatori de la aceeași autoritate. 5. UC: Crearea unui formular.
Flux de bază: Management pentru utilizator de bază (gestionar formular)	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularelor) se conectează la software. 2. Utilizatorul de bază (gestionarul formularelor) intră în pagină cu lista formularelor create. 3. Utilizatorul de bază (gestionarul formularului) selectează formularul care urmează să fie gestionat. 4. Utilizatorul de bază (gestionarul formularului) accesează pagina de setări separate pentru fiecare formular pentru a configura setările generale, elementele de text, participanții la formular și setările de acces, notificările și setările de gestionare a datelor și setările de control al publicării. 5. Utilizatorul de bază (gestionarul formularului) salvează modificările la setări.
Flux alternativ A: Management pentru utilizator de bază (vizualizator formular)	<ol style="list-style-type: none"> 1. Utilizatorul de bază (vizualizator formular) intră în pagină cu lista formularelor create. 2. Utilizatorul de bază (vizualizator formular) selectează formularul care urmează să fie gestionat. 3. Utilizatorul de bază (vizualizator formular) accesează o pagină de rezumat în care poate vizualiza setările generale, setările elementelor de text, utilizatorii, jurnalul de activitate și setările de acces, notificările și setările de gestionare a datelor și setările de control al publicării formularelor.
Flux alternativ B:	<ol style="list-style-type: none"> 1. Administratorul de date locale intră în pagină cu lista formularelor create.

Management pentru administratorul local de date	<p>2. Administratorul local de date selectează formularul care urmează să fie gestionat.</p> <p>3. Administratorul local de date accesează pagina de setări separate pentru fiecare formular pentru a configura setările generale, elementele de text, participanții la formular și setările de acces, notificările și setările de gestionare a datelor și setările de control al publicării.</p> <p>4. Administratorul local de date salvează modificările la setări.</p>
Post-condiții	<p>1. Setările formularelor sunt previzualizate.</p> <p>2. Setările formularelor sunt configurate.</p> <p>3. Starea formularelor este actualizată.</p>

UC6 – Analiza datelor

Descriere	<p>Generatorul de formulare va colecta și afișa informații despre utilizarea instrumentului într-un tablou de bord cu statistici disponibil utilizatorilor săi. Sursele de date ale statisticilor vor consta din răspunsurile la formularele create cu instrumentul și din jurnalele de activitate din cadrul instrumentului de generare a formularelor. Pentru a pregăti statistici, datele sunt agregate și anonimizate, lăsând doar indicatori statistici la nivel înalt.</p>
Actori	N / A (proces automatizat de generatorul de formulare)
Precondiții	<p>1. Furnizarea accesului la software.</p> <p>2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul).</p> <p>3. UC: Gestionarea utilizatorilor.</p> <p>4. UC: Crearea unui formular.</p> <p>5. UC: Editarea unui formular.</p> <p>6. UC: Traducerea unui formular.</p> <p>7. UC: Publicarea unui formular.</p> <p>8. UC: Gestionarea setărilor formularelor stocate.</p>
Flux de bază:	<p>1. Utilizatorul se conectează la software.</p> <p>2. Generatorul de formulare procesează datele statistice disponibile la intervale regulate (de exemplu, zilnic) sau la cerere.</p> <p>3. Generatorul de formulare preia informații din răspunsurile la formularele publicate și din jurnalele activității de generare a formularelor (de exemplu, date privind numărul de formulare create, numărul de interogări primite etc.).</p>

300



	<p>4. Generatorul de formulare anonimizează toate datele disponibile, eliminând orice informații de identificare personală (atât asupra respondenților, cât și a utilizatorilor instrumentului).</p> <p>5. Generatorul de formulare agregă datele pe baza dimensiunilor necesare (de exemplu, tipul procedurii, utilizarea șabloanelor, utilizarea câmpurilor de date, tipurile de activitate ale utilizatorilor etc.)</p> <p>6. Generatorul de formulare prezintă informațiile procesate în tabloul de bord al statisticilor pentru a fi accesate de toți utilizatorii.</p> <p>7. Utilizatorii instrumentului pot accesa date statistice cantitative specifice.</p> <p>8. Datele statistice sunt trimise la punctul final cu transferuri sincrone de date.</p> <p>9. Utilizatorii pot descărca raportul de statistici în mai multe formate (de exemplu, Microsoft Excel, valori separate prin virgulă etc.).</p>
Post-condiții	<ol style="list-style-type: none"> 1. Date statistice actualizate privind performanța generatorului de formulare. 2. Raport actualizat descărcabil al datelor statistice. 3. Datele statistice actualizate privind performanța generatorului de formulare sunt trimise la punctul final.

UC7 – Căutarea unui formular

Descriere	<p>Utilizatorii (cu drepturi de creare) accesează software-ul și încep procesul de creare a unui formular pentru o anumită procedură în 3 moduri diferite:</p> <ol style="list-style-type: none"> 1. Prin crearea formularului de la zero. 2. Prin crearea formularului pe baza formularelor existente stocate în instrument. 3. Prin crearea formularului din șabloane implicite.
Actori	<ol style="list-style-type: none"> 1. Administrator local de date. 2. Utilizator de bază (gestionar formular).
Precondiții	<ol style="list-style-type: none"> 1. Furnizarea accesului la software. 2. Definirea setărilor sistemelor de stocare, de gestionare a conținutului și / sau de gestionare a cazurilor (dacă este cazul). 3. UC: Desemnarea administratorului de date locale. 4. UC: Înregistrarea altor utilizatori .
Flux de bază: Căutarea unui formular	<ol style="list-style-type: none"> 1. Utilizatorul de bază (gestionarul formularului) selectează opțiunea de a căuta un formular existent (butonul de căutare).

	<p>2. Utilizatorul de bază (gestionarul formularelor) este redirecționat către o pagină care conține toate formularele create. Utilizatorul le poate sorta și filtra în funcție de criterii specifice de pe ecran sau poate efectua o căutare.</p> <p>3. Utilizatorul de bază poate căuta printre formularele existente adăugând cuvinte cheie într-un șir de căutare sau filtrând pe baza altor caracteristici stocate ale formularului, precum data creării, procedura acoperită, numele de utilizator al creatorului formularului etc.</p> <p>4. Rezultatele căutării sunt afișate utilizatorului.</p> <p>5. Prin selectarea rezultatului căutării, formularul este afișat utilizatorului.</p>
Post-condiții	<p>1. Utilizatorul poate vizualiza formulare.</p> <p>2. Utilizatorul poate traduce formulare.</p> <p>3. Utilizatorul poate edita formularele care nu sunt în stare activă.</p>

Sesiunea demonstrativă de la sediul ONRC va avea loc după depunerea ofertelor, data fiind stabilită ulterior, de autoritatea contractantă.

Funcționalitățile aferente componentelor hardware vor fi validate în etapa de evaluare tehnică a ofertelor doar pe baza documentelor justificative prezentate ca parte a ofertei tehnice (documentații tehnice, datasheet-uri, screenshot-uri ale interfețelor, etc.), urmând ca Ofertantul câștigător să le prezinte practic Autorității Contractante în perioada de implementare a proiectului, în urma instalării acestora pe mediile Autorității Contractante (test sau producție). Prezentarea capacităților soluțiilor propuse în cadrul sesiunii demonstrative se va baza pe prezentarea practică a produselor software oferite (de exemplu: a interfețelor expuse de acestea, a fișierelor de configurare ale acestora, etc.) în cadrul unor medii demonstrative și nu doar pe descrieri ale producătorilor (de exemplu: datasheet-uri, manuale de administrare, alte documentații tehnice).

În cazul în care un Ofertant nu poate demonstra în cadrul sesiunii demonstrative îndeplinirea unei cerințe minimale din cele solicitate, Autoritatea Contractantă va respinge oferta acestuia ca neconformă.

De asemenea, refuzul de susținere a sesiunii demonstrative va conduce la declararea ofertei acestuia ca fiind neconformă.

Personalul nominalizat de către Ofertanți pentru participare la sesiunea demonstrativa va fi desemnat din echipa propusa în propunerea tehnică pentru implementarea proiectului.

Sesiunea demonstrativa va fi susținută de către fiecare Ofertant la sediul Autorității Contractante în urma invitației de participare din partea acesteia.

Cu minimum 2 zile lucrătoare înainte de data planificata pentru sesiunea demonstrativa, Ofertantul are obligația să transmită Autorității Contractante lista participanților la sesiunea demonstrativa în care se menționează rolul în timpul sesiunii și relația pe care aceștia o au cu Ofertantul – participanții vor fi dintre cei experții propuși în oferta tehnică. Autoritatea Contractantă nu va accepta în sesiunea demonstrativa decât

persoanele nominalizate de ofertant în lista participanților și care figurează în lista de experți cheie menționați în oferta depusa.

Ofertantul va pune la dispoziția experților săi resursele necesare (de exemplu: laptop-uri, modem-uri de date, servere accesate de la distanță pentru susținerea demonstrației, etc.) pentru derularea în bune condiții a sesiunii demonstrative.

Pe durata sesiunii demonstrative, Autoritatea Contractantă va solicita realizarea de screenshot-uri cu interfețele aplicațiilor utilizate în demonstrarea fiecărei funcționalități ce intra în scopul sesiunii demonstrative. Aceste screenshot-uri vor fi incluse în anexa procesului verbal aferent sesiunii demonstrative ce va fi încheiat de către Autoritatea Contractantă și Ofertant la finalul sesiunii demonstrative.

Rezultatele obținute de ofertant în cadrul sesiunii demonstrative vor fi consemnate, în scris, în cadrul unui proces-verbal, redactat de către autoritatea contractantă și semnat de reprezentantul/reprezentanții autorității contractante și ai ofertantului. Oricare dintre părți are dreptul de a menționa observații pe procesul-verbal, caz în care procesul-verbal se va semna cu observații. Refuzul ofertantului de a semna procesul-verbal aferent sesiunii demonstrative conduce la respingerea ofertei.

De asemenea, Ofertantul va depune prin intermediul SEAP până la data și ora limită de depunere a ofertelor în anunțul de participare, semnată cu semnătură electronică extinsă, o înregistrare audio-video a unei sesiuni demonstrative prin care va prezenta modalitatea prin care soluțiile oferite incluse în soluția tehnică răspund la funcționalitățile minime solicitate în caietul de sarcini la cap. 3.5.4 Cerințe tehnice, cu excepția funcționalităților aferente componentelor din categoria hardware.

Notă: rezoluția înregistrării video trebuie să fie minimum full hd și să permită vizualizarea conținutului în condiții optime (să permită o buna vizualizare a conținutului prezentării).

Menționăm că solicitările referitoare la sesiunile demonstrative nu presupun implementarea de părți din contract. De asemenea, Ofertanții pot utiliza versiuni de tip demo/trial/temporar ale produselor oferite.

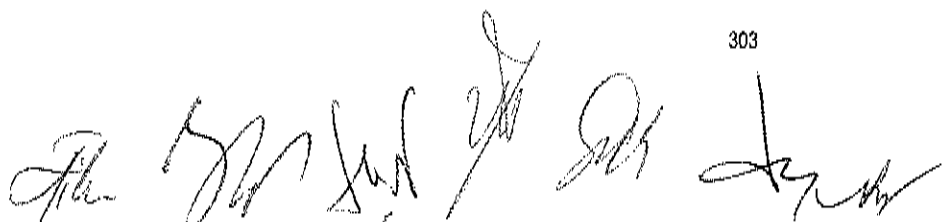
8 Drepturi de proprietate intelectuală

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 și/sau materialelor realizate și nu le va utiliza în scopuri care nu au legătură cu prezentul contract fără acordul scris prealabil al achizitorului.

Cu excepția informațiilor publice, Prestatorul nu va publica articole referitoare la obiectul prezentului contract, nu va face referire la aceste lucrări în cursul executării altor lucrări pentru terți și nu va divulga nicio informație 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 așa cum va considera de cuviință, fără limitare geografică ori

303

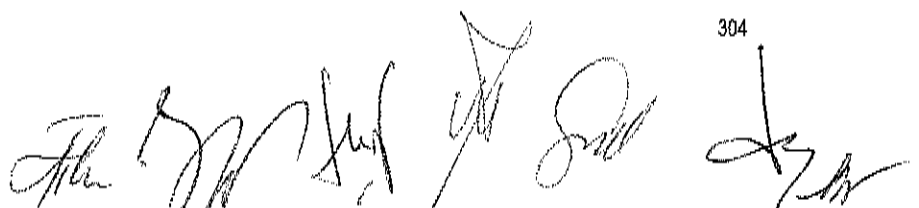


de altă natură, cu excepția situațiilor în care există deja asemenea drepturi de proprietate intelectuală ori industrială.

9 Modalitate de plată

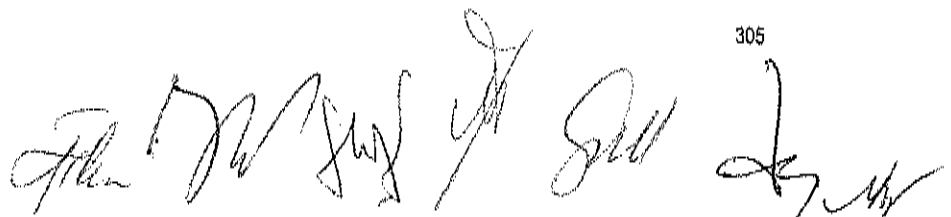
Plata sumei de _____, fără TVA, se va efectua în mai multe tranșe, astfel:

1. O tranșă reprezentând plata intermediară într-un procent de 90% din valoarea aferentă amenajărilor și dotărilor spațiilor tehnice, care se va efectua după aprobarea raportului de progres intermediar RPI1 ce va avea ca anexă procesul-verbal de recepție cantitativă și calitativă a spațiilor tehnice.
2. O tranșă reprezentând o plată intermediară de 80 % din valoarea aferentă serviciilor de analiză care se va efectua după aprobarea raportului de progres intermediar RPI2 ce va avea ca anexe procesele-verbale de recepție cantitativă și calitativă a serviciilor de analiză.
3. O tranșă reprezentând o plată intermediară de 60 % din valoarea aferentă infrastructurii hardware pentru mediul de testare și dezvoltare, care se va efectua după aprobarea raportului de progres intermediar RPI3 ce va avea ca anexe procesele-verbale de recepție cantitativă a produselor livrate.
4. O tranșă reprezentând o plată intermediară de 60 % din valoarea aferentă infrastructurii software pentru mediul de testare și dezvoltare, care se va efectua după aprobarea raportului de progres intermediar RPI4 ce va avea ca anexe procesele-verbale de recepție cantitativă a produselor livrate.
5. O tranșă reprezentând o plată intermediară de 20 % din valoarea aferentă infrastructurii hardware pentru mediul de testare și dezvoltare, care se va efectua după aprobarea raportului de progres intermediar RPI5 ce va avea ca anexe procesele-verbale de recepție calitativă a produselor livrate.
6. O tranșă reprezentând o plată intermediară de 20 % din valoarea aferentă infrastructurii software pentru mediul de testare și dezvoltare, care se va efectua după aprobarea raportului de progres intermediar RPI6 ce va avea ca anexe procesele-verbale de recepție calitativă a produselor livrate.
7. O tranșă reprezentând o plată intermediară de 80 % din valoarea aferentă serviciilor de proiectare care se va efectua după aprobarea raportului de progres intermediar RPI7 ce va avea ca anexe procesele-verbale de recepție cantitativă și calitativă a serviciilor de proiectare software.
8. O tranșă reprezentând o plată intermediară de 60 % din valoarea aferentă infrastructurii hardware pentru mediul de producție, care se va efectua după aprobarea raportului de progres intermediar RPI8 ce va avea ca anexe procesele-verbale de recepție cantitativă a produselor livrate.



9. O tranșă reprezentând o plată intermediară de 60 % din valoarea aferentă infrastructurii software pentru mediul de producție, care se va efectua după aprobarea raportului de progres intermediar RPI9 ce va avea ca anexe procesele-verbale de recepție cantitativă a produselor livrate.
10. O tranșă reprezentând o plată intermediară de 20 % din valoarea aferentă infrastructurii hardware pentru mediul de producție, care se va efectua după aprobarea raportului de progres intermediar RPI10 ce va avea ca anexe procesele-verbale de recepție calitativă a produselor livrate.
11. O tranșă reprezentând o plată intermediară de 20 % din valoarea aferentă infrastructurii software pentru mediul de producție, care se va efectua după aprobarea raportului de progres intermediar RPI11 ce va avea ca anexe procesele-verbale de recepție calitativă a produselor livrate.
12. O tranșă reprezentând o plată intermediară de 40 % din valoarea aferentă serviciilor de dezvoltare software care se va efectua după aprobarea raportului de progres intermediar RPI12 ce va avea ca anexe procesele-verbale de recepție cantitativă a serviciilor de dezvoltare software.
13. O tranșă reprezentând o plată intermediară de 40 % din valoarea aferentă serviciilor de dezvoltare software care se va efectua după aprobarea raportului de progres intermediar RPI13 ce va avea ca anexe procesele-verbale de recepție calitativă pe baza documentelor puse la dispoziție de prestatorul care asigură testarea externă .
14. Plata finală se va efectua după aprobarea raportului final ce va avea ca anexă procesul-verbal de acceptanță finală a tuturor activităților proiectului și punerea în funcțiune a întregului sistem informatic, inclusiv migrarea datelor și instruirea utilizatorilor/administratorilor. Această plată va cuprinde:
 - 10% din valoarea aferentă realizării amenajării și dotării spațiilor tehnice;
 - 20 % din valoarea aferentă serviciilor de analiză;
 - 20% din valoarea aferentă livrării, instalării și configurării infrastructurii hardware aferente mediului de testare și dezvoltare;
 - 20% din valoarea aferentă livrării, instalării și configurării infrastructurii software aferente mediului de testare și dezvoltare;
 - 20 % din valoarea aferentă serviciilor de proiectare;
 - 20 % din valoarea aferentă livrării, instalării și configurării infrastructurii hardware aferente mediului de producție;
 - 20 % din valoarea aferentă livrării, instalării și configurării infrastructurii software aferente mediului de producție;
 - 20 % din valoarea aferentă serviciilor de dezvoltare software;
 - 100% aferentă valorii serviciilor de instruire a utilizatorilor/administratorilor/dezvoltatori;
 - 100% aferentă valorii serviciilor de migrare date;
 - 100% aferentă valorii serviciilor de asistență la acceptanță și trecere în producție.

305



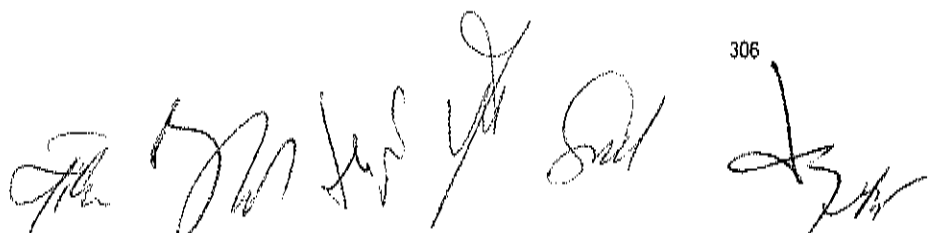
Plata este condiționată de semnarea proceselor-verbale de recepție calitativă/cantitativă a serviciilor/produselor și de aprobarea rapoartelor de progres intermediare/finale aferente.

(1) Plata facturilor se va efectua în termen de 30 de zile calendaristice de la semnarea proceselor-verbale de recepție calitativă/cantitativă a serviciilor/produselor și de aprobarea rapoartelor de progres intermediare/finale aferente, conform art. 6 alin.(1) lit. c) din Legea nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și autorități contractante, cu modificările și completările ulterioare.

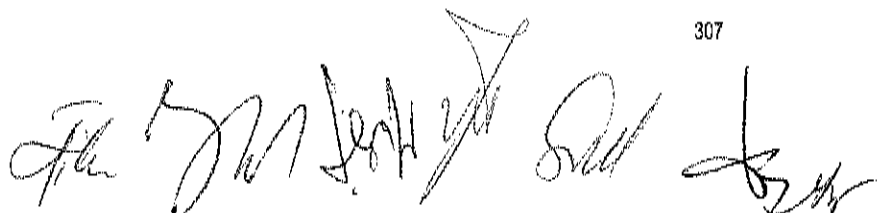
(2) În mod excepțional, plățile pot fi efectuate în termen de maximum 60 de zile calendaristice, în acord cu art. 7 alin.(1) din Legea nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și autorități contractante, cu modificările și completările ulterioare.

Rapoartele 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 (RPI1)** ce va cuprinde descrierea etapelor de recepție cantitativă și calitativă a spațiilor tehnice, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 2 luni și 26 zile de la data semnării contractului.
2. **Raport de progres intermediar nr. 2 (RPI2)** ce va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de analiză, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 5 luni și 25 zile de la data semnării contractului.
3. **Raport de progres intermediar nr. 3 (RPI3)** ce va cuprinde descrierea etapei de recepție cantitativă a produselor hardware livrate aferente mediului de testare și dezvoltare, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 3 luni și 9 zile de la data semnării contractului.
4. **Raport de progres intermediar nr. 4 (RPI4)** ce va cuprinde descrierea etapei de recepție cantitativă a produselor software livrate aferente mediului de testare și dezvoltare, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 6 luni și 2 zile de la data semnării contractului.
5. **Raport de progres intermediar nr. 5 (RPI5)** ce va cuprinde descrierea etapei de recepție calitativă a produselor hardware livrate aferente mediului de testare și dezvoltare, împreună cu instalarea și configurarea acestora, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 3 luni și 23 zile de la data semnării contractului.
6. **Raport de progres intermediar nr. 6 (RPI6)** ce va cuprinde descrierea etapei de recepție calitativă a produselor software livrate aferente mediului de testare și dezvoltare, împreună cu instalarea și configurarea acestora, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 6 luni și 16 zile de la data semnării contractului.



7. **Raport de progres intermediar nr. 7 (RPI7)** ce va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de proiectare, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 7 luni și 27 zile de la data semnării contractului.
8. **Raport de progres intermediar nr. 8 (RPI8)** ce va cuprinde descrierea etapei de recepție cantitativă a produselor hardware livrate aferente mediului de producție, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 4 luni și 14 zile de la data semnării contractului.
9. **Raport de progres intermediar nr. 9 (RPI9)** ce va cuprinde descrierea etapei de recepție cantitativă a produselor software livrate aferente mediului de producție, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 7 luni și 6 zile de la data semnării contractului.
10. **Raport de progres intermediar nr. 10 (RPI10)** ce va cuprinde descrierea etapei de recepție calitativă a produselor hardware livrate aferente mediului de producție, împreună cu instalarea și configurarea acestora, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 5 luni și 18 zile de la data semnării contractului.
11. **Raport de progres intermediar nr. 11 (RPI11)** ce va cuprinde descrierea etapei de recepție calitativă a produselor software livrate aferente mediului de producție, împreună cu instalarea și configurarea acestora, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 8 luni și 10 zile de la data semnării contractului.
12. **Raport de progres intermediar nr. 12 (RPI12)** ce va cuprinde descrierea etapelor de recepție cantitativă a serviciilor de dezvoltare software, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum 11 luni și 14 zile de la data semnării contractului.
13. **Raport de progres intermediar nr. 13 (RPI13)** va include raport financiar și va cuprinde finalizarea etapelor de recepție calitativă a serviciilor de dezvoltare software pe baza documentelor puse la dispoziție de prestatorul care asigură testarea externă. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum un an 4 luni și 3 zile de la data semnării contractului.
14. **Raport de progres intermediar nr. 14 (RPI14)** ce va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de migrare date, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum un an și 25 zile de la data semnării contractului.
15. **Raport de progres intermediar nr. 15 (RPI15)** care va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de instruire utilizatorilor/administratorilor/dezvoltatorilor, care include și raport financiar. Acesta va fi transmis în termen de 10 zile de la sfârșitul perioadei de raportare, aceasta fiind de maximum un an 5 luni și 7 zile de la data semnării contractului



16. **Raport final (RF)** – document elaborat de Prestator la finalul contractului ce 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 ce face obiectul contractului de finanțare.

Aprobarea documentelor sau notificarea cu privire la neconformitățile identificate de beneficiar se va efectua în maximum 10/15 zile lucrătoare (funcție de complexitate) de la primirea acestora. Prestatorul va revizui și retransmite documentele în maximum 5 zile lucrătoare de la notificare.

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.

10 Recepții aferente proiectului

Recepția reprezintă ansamblul operațiunilor de identificare și verificare cantitativă și calitativă, desfășurată în prezența furnizorului/prestatorului/executantului, prin care se verifică modul în care acesta și-a îndeplinit obligațiile asumate prin contract.

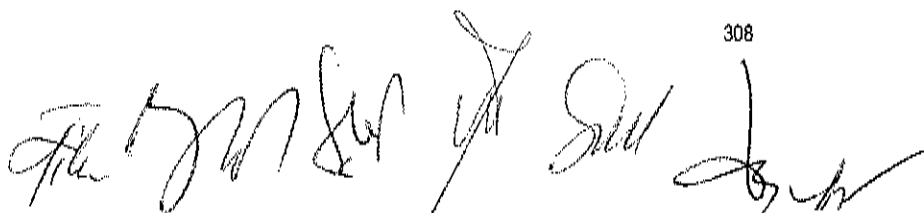
Desfășurarea activității de recepție se realizează cu respectarea principiilor: legalitate, profesionalism, corectitudine și transparență. De asemenea, se respectă principiul separării atribuțiilor, potrivit căruia persoanele care au responsabilități în elaborarea contractelor, comenzilor sau a documentelor de înregistrare în contabilitate și de plată nu pot fi numite membri ai comisiei de recepție a bunurilor/serviciilor/lucrărilor.

Comisia de recepție va avea în vedere, cel puțin :

- a) **verificarea contractului**, în vederea completării corecte a cerințelor de calitate/verificarea documentelor de însoțire a produselor/bunurilor, serviciilor, lucrărilor/ factura fiscală/aviz de însoțire a mărfii, după caz/certificat de calitate sau declarație de conformitate, după caz/alte documente prevăzute în contract ;
- b) **verificarea concordanței** între performanțele prevăzute în certificate și nivelul parametrilor înscrși în contract;
- c) **identificarea și verificarea vizuală** a bunurilor/materialelor;
- d) **verificarea calitativă**, ulterior parcurgerii cel puțin a etapelor detaliate mai sus, dar la care se mai pot adăuga și alte activități ce rezultă din obiectului recepției.

Comisia va consemna rezultatele recepției în Procesele verbale de recepție cantitativă și calitativă, Procesul verbal de punere în funcțiune, Procesul verbal de recepție la terminarea lucrărilor și Procesul verbal de recepție la finalizarea lucrărilor.

308



Recepțiile produselor se vor realiza la destinația finală, conform graficului de implementare și vor include:

- a) recepția cantitativă, (RCT) care va consta în inspectarea și verificarea vizuală, respectiv numărarea produselor livrate, (obligatoriu, se vor consemna toate seriile produselor livrate);
- b) recepția calitativă, (RCL) care va presupune efectuarea de teste funcționale, după caz în vederea verificării respectării specificațiilor tehnice din caietul de sarcini și propunerea tehnică.

În situația în care, cu ocazia efectuării recepțiilor cantitative și calitative se constată că nu au fost livrate toate produsele sau toate accesoriile aferente acestora, sau unele dintre produsele nu corespund specificațiilor tehnice din caietul de sarcini/propunerea tehnică sau sunt defecte, achizitorul va avea dreptul de a respinge produsele respective, iar furnizorul va avea obligația de a remedia deficiențele constatate, fără costuri suplimentare pentru achizitor, prin furnizarea produselor/accesoriilor lipsă și/sau înlocuirea produselor/accesoriilor constatate defecte sau neconforme, fără a depăși termenele finale stabilite pentru fiecare dintre etape.

Recepțiile cantitative și calitative se vor finaliza prin semnarea de către membrii comisiei de recepție a achizitorului și reprezentanții autorizați ai furnizorului a proceselor verbale de recepție cantitativă/calitativă.

Livrabilele sunt documente cu caracter general, deschis, și care pot fi modificate, completate sau actualizate pe parcursul derulării tuturor etapelor rămase până la finalizarea proiectului, ori de câte ori este necesar pentru atingerea obiectivelor proiectului.

1. **Activitățile de recepție aferente etapei nr.1 (RE1)**, la împlinirea termenului specificat, părțile vor proceda la recepția lucrărilor executate și testarea tuturor sistemelor și produselor livrate, instalate și puse în funcțiune a spațiilor tehnice amenajate în cadrul etapei nr.1, conform cerințelor caietului de sarcini și a propunerii tehnice.

Livrabile pentru aceasta etapa:

- Proces verbal de recepție calitativa a spatiului tehnic amenajat, care va cuprinde cel puțin următoarele documente:
 - Proces/e verbal/e recepție cantitativa spatiu tehnic amenajat
 - Raport/e privind amenajarea spațiului tehnic
 - Scenarii de testare a spațiului tehnic
 - Rapoarte de testare a spațiilor tehnice

Finalizarea etapei nr. 1 de implementare a contractului se va concretiza prin:

- a) Semnarea de către membrii comisiei de recepție a achizitorului și reprezentanții autorizați ai furnizorului a unui proces-verbal de recepție cantitativă și calitativă. Acesta va fi întocmit

pe baza rezultatelor recepțiilor aferente și a proceselor-verbale de recepție cantitativă/calitativă parțiale aferente lucrărilor executate, sistemelor și produselor aferente, instalate, configurate, puse în funcțiune, integrate și operaționalizate

- b) Raportul de progres intermediar nr.1 (RPI1) ce va cuprinde descrierea etapelor de recepție cantitativă și calitativă a spațiilor tehnice, care include și raport financiar.

2. Activitățile de recepție aferente etapei nr.2 (RE2), se vor realiza prin parcurgerea operațiunilor de recepție cantitativă și calitativă a serviciilor de analiză, conform cerințelor caietului de sarcini

Livrabile pentru recepția cantitativă

- Proces verbal de recepție cantitativă a serviciilor de analiză care să cuprindă cel puțin următoarele documente:
 - Documentului de analiza de business,
 - Scenarii de testare, incluzând cazuri și scenarii de testare funcționale și respectiv de integrare, pentru componentele dezvoltate/adaptate conform cerințelor din prezentul proiect

Livrabile pentru recepția calitativă:

- Proces verbal de recepție calitativă a serviciilor de analiză care să cuprindă cel puțin următoarele documente
 - Documentului de analiza de business (actualizat conform observațiilor/modificărilor autorității contractante)
 - Scenarii de testare, incluzând cazuri și scenarii de testare funcționale și respectiv de integrare, pentru componentele dezvoltate/adaptate conform cerințelor din prezentul proiect (actualizat conform observațiilor/modificărilor autorității contractante)

Finalizarea etapei nr.2 de implementare a contractului se va concretiza prin:

- a) Semnarea de către membrii comisiei de recepție a RCL
- a) Raportului de progres intermediar nr. 2 (RPI2) ce va cuprinde descrierea etapelor de recepție cantitativă și calitativă a serviciilor de analiză, care include și raport financiar.

3. Activitățile de recepție aferente etapei nr.3 (RE3), la împlinirea termenului specificat, părțile vor proceda la recepția cantitativă a produselor hardware livrate aferente mediului de testare și dezvoltare, (obligatoriu, se vor consemna toate seriile produselor livrate, inclusiv poze ale acestora).

Livrabile pentru aceasta etapa:

- Proces/e verbale de recepție cantitativa a produselor hardware

Finalizarea etapei nr.3 de implementare a contractului se va concretiza prin:

- a) semnarea de către membrii comisiei de recepție a proceselor verbale de recepție cantitativa a produselor hardware livrate aferente mediului de testare și dezvoltare,
 - b) Raportul de progres intermediar nr. 3 (RPI3) ce va cuprinde și raport financiar
4. **Activitățile de recepție aferente etapei nr.4 (RE4)**, la împlinirea termenului specificat, părțile vor proceda la recepția cantitativa a produselor software de bază (aplicații necesare funcționării sistemului informatic, exemplu software pentru componentele prezentate in capitolul 3.5.4.3) livrate aferente mediului de testare și dezvoltare.

Livrabile pentru aceasta etapa:

- Proces/e verbal/e de recepție cantitativa software de baza care va/vor cuprinde: denumire produs, cantitate, unitate de măsură, serial no./Part no.și licență

Finalizarea etapei nr.4 de implementare a contractului se va concretiza prin:

- a) semnarea de către membrii comisiei de recepție a proceselor verbale de recepție cantitativa a produselor software livrate aferente mediului de testare și dezvoltare,
 - b) Raportul de progres intermediar nr. 4 (RPI4) ce va cuprinde și raport financiar.
5. **Activitățile de recepție aferente etapei nr.5 (RE5)** la împlinirea termenului specificat, părțile vor proceda la recepția calitativă a produselor hardware livrate aferente mediului de testare și dezvoltare se va consemna pt. fiecare tip de echipament hardware îndeplinirea cerințelor tehnice conform caietul de sarcini și a propunerii tehnice.

Livrabile pentru aceasta etapa:

- Procesul verbal de recepție calitativa pentru produsele hardware care va conține cel puțin următoarele livrabile:
 - Raport infrastructura hardware
 - Raport de instalare și configurare infrastructură hardware
 - Proces verbal de punere in functiune echipamente hardware
 - Scenarii de testare infrastructura hardware
 - Raport de testare echipamente hardware

Finalizarea etapei nr. 5 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de recepție a procesului verbal de recepție calitativa pentru produsele hardware
 - b) Raportului de progres intermediar nr.5 (RPI5) ce va cuprinde și raport financiar.
6. **Activitățile de recepție aferente etapei nr.6 (RE6)** la împlinirea termenului specificat, părțile vor proceda la recepția calitativa a produselor software de bază(aplicații necesare funcționării sistemului



informatic, exemplu software pentru componentele prezentate in capitolul 3.5.4.3) livrate aferente mediului de testare și dezvoltare, îndeplinirea cerințelor tehnice și funcționale conform caietul de sarcini și propunerii tehnice

Livrabile pentru aceasta etapa:

- Procesul verbal de recepție calitativă pentru produsele software și a serviciilor de instalare și configurare a acestora, care va conține cel puțin următoarele livrabile:
 - Produse software de baza
 - Raport de instalare și configurare software
 - Scenarii de testare software
 - Licențele și serviciile de mentenanță și suport de la producători pentru toate aplicațiile software aferente mediului de testare și dezvoltare

Finalizarea etapei nr. 6 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a procesului verbal de recepție calitativă pentru produsele software și a serviciilor de instalare și configurare a acestora,
- b) Raportului de progres intermediar nr.6 (RPI6) ce va cuprinde și raport financiar

7. Activitățile de recepție aferente etapei nr.7 (RE7), se vor realiza prin parcurgerea operațiunilor de recepție cantitativă și calitativă a serviciilor de proiectare, conform cerințelor caietului de sarcini

Livrabile pentru recepția cantitativă:

- Proces/e verbal/e de recepție cantitativa - servicii de proiectare, care va conține cel puțin următoarele livrabile:
 - Document proiectare detaliata - proiect tehnic
 - Scenarii de testare non-funcțională

Livrabile pentru recepția calitativă:

- Proces/e verbal/e de recepție calitativa - servicii de proiectare, care va conține cel puțin următoarele livrabile:
 - Document proiectare detaliata - proiect tehnic (actualizat conform observațiilor/modificărilor ale autorității contractante)
 - Scenarii de testare non-funcțională (actualizat conform observațiilor/modificărilor ale autorității contractante)
 - Standarde de dezvoltare
 - Arhitectura module/aplicatii
 - Strategia de integrare



Finalizarea etapei nr. 7 de implementare a contractului se va concretiza prin:

- a) semnarea de către membrii comisiei de recepție a proceselor verbale de recepție cantitativa și calitativa
- b) Raportului de progres intermediar nr.7 (RPI7) ce va cuprinde și raport financiar

8. **Activitățile de recepție aferente etapei nr.8 (RE8)**, la împlinirea termenului specificat, părțile vor proceda la recepția cantitativa a produselor hardware livrate aferente mediului de producție, care va consta în inspectarea și verificarea vizuală, respectiv numărarea bucată cu bucată a produselor livrate (obligatoriu, se vor consemna toate seriile produselor livrate inclusiv poze ale acestora).

Livrabile pentru aceasta etapa:

- Procese verbale de recepție cantitativa a produselor hardware

Finalizarea etapei nr.8 de implementare a contractului se va concretiza prin:

- a) semnarea de către membrii comisiei de recepție a proceselor verbale de recepție cantitativă a produselor hardware livrate aferente mediului de producție
- b) Raportului de progres intermediar nr. 8 (RPI8) ce va cuprinde și raport financiar.

9. **Activitățile de recepție aferente etapei nr.9 (RE9)**, la împlinirea termenului specificat, părțile vor proceda la recepția cantitativă a produselor software (aplicații necesare funcționării sistemului informatic, exemplu software pentru componentele prezentate în capitolul 3.5.4.3) livrate aferente mediului de producție.

Livrabile pentru aceasta etapa:

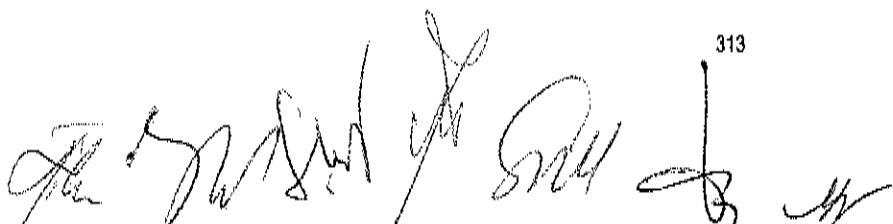
- Procese verbale de recepție cantitativă software de bază care va cuprinde: denumire produs/serviciu, cantitate, unitate de măsură, denumire componenta și licența

Finalizarea etapei nr.9 de implementare a contractului se va concretiza prin:

- a) semnarea de către membrii comisiei de recepție a proceselor verbale de recepție cantitativa a produselor software livrate aferente mediului de producție,
- b) Raportului de progres intermediar nr. 9 (RPI9) ce va cuprinde și raport financiar.

10. **Activitățile de recepție aferente etapei nr.10 (RE10)** la împlinirea termenului specificat, părțile vor proceda la recepția calitativă a produselor hardware livrate aferente mediului de producție se va consemna pt. fiecare tip de echipament hardware îndeplinirea cerințelor tehnice conform caietului de sarcini și a propunerii tehnice.

Livrabile pentru aceasta etapa:



- Procese verbale de recepție calitativă pentru produsele hardware care va conține cel puțin următoarele livrabile:
 - Rapoarte de instalare și configurare infrastructura hardware
 - Procese verbale de punere în funcțiune echipamente hardware
 - Scenarii de testare infrastructură hardware
 - Rapoarte de testare echipamente hardware

Finalizarea etapei nr. 10 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a proceselor verbale de receptie calitativa pentru produsele hardware
- b) Raportului de progres intermediar nr.10 (RPI10) ce va cuprinde și raport financiar.

11. Activitățile de recepție aferente etapei nr.11 (RE11) la împlinirea termenului specificat, părțile vor proceda la recepția calitativă a produselor software (aplicații necesare funcționării sistemului informatic, exemplu software pentru componentele prezentate in capitolul 3.5.4.3) livrate aferente mediului de producție, îndeplinirea cerințelor tehnice și funcționale conform caietul de sarcini.

Livrabile pentru aceasta etapa:

- Proces/e verbal/e de recepție calitativă pentru produsele software și a serviciilor de instalare și configurare a acestora, care va conține cel puțin următoarele livrabile:
 - Rapoart/e de instalare și configurare software
 - Scenarii de testare software
 - Licențe și servicii de mentenanță și suport de la producători pentru toate aplicațiile software aferente mediului de testare și dezvoltare

Finalizarea etapei nr. 11 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a proceselor verbale de recepție calitativă pentru produsele software și a serviciilor de instalare și configurare a acestora,
- b) Raportului de progres intermediar nr.11 (RPI11) ce va cuprinde și raport financiar.

12. Activitățile de recepție aferente etapei nr.12 (RE12), se vor realiza prin parcurgerea operațiunilor de recepție cantitativă a serviciilor de dezvoltare software, conform cerințelor caietului de sarcini

Livrabile pentru recepția cantitativă:

- Procese verbale de recepție cantitativa a modulelor/aplicațiilor care va/vor conține cel puțin:
 - Codul sursa documentat al modulelor/aplicațiilor pana la nivel de clasa (Java), funcții și proceduri stocate;

- Codul sursa al modulelor/aplicațiilor dezvoltate, biblioteci, inclusiv fișierele de configurare din cadrul tuturor componentelor sistemului, atât pentru software-ul dezvoltat cât și pentru configurarea celorlalte componente hardware/software care sunt diferite de configurația standard de instalare;
- Codul fișierelor de configurare;
- Raport cuprinzand rezultatele testelor Prestatorului;
- Procedura de compilare a codului sursa;
- Procedura detaliata de instalare și configurare pentru fiecare modul/aplicație;
- Manuale utilizatori
- Manuale administrare pentru baze de date, dezvoltatori, administrare utilizatori
- Codului sursa pentru tot sistemul informatic instalat va fi pe repository GITLab. Acesta sa fie compilabil pe utilitarul de dezvoltare folosit de prestator și instalat pe mediul de dezvoltare și testare al beneficiarului.

Finalizarea etapei nr. 12 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a proceselor verbale de recepție cantitativa
- b) Raportului de progres intermediar nr.12 (RPI12) ce va cuprinde și raport financiar

13. Activitățile de recepție aferente etapei nr.13 (RE13), se vor realiza prin parcurgerea operațiunilor de recepție calitativă a serviciilor de dezvoltare software,

- a. conform cerințelor caietului de sarcini

Livrabile pentru recepția calitativă:

- Procese verbale de recepție calitativa a modulelor/aplicațiilor care va/vor conține cel puțin:
 - Acceptarea codului sursă pentru sistemul informatic se va face cu demonstrarea funcționării acestuia. Se va efectua cel puțin o modificare, se va compila, se va instala și se va demonstra ca funcționează corect pe mediu de test al beneficiarului.
 - Raport de testare a prestatorului extern pentru testare functionala, testare de integrare, de performanta, etc. - conform testelor planificate cu prestatorul extern de testare

- b. pe baza documentelor furnizate de prestatorul care asigura testarea externa

Livrabil pentru recepția calitativă

- Documente/Rapoarte puse la dispozitie de prestatorul care asigura testarea externa, privind rezultatele testarii sistemului informatic

Finalizarea etapei nr. 13 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a proceselor verbale de recepție calitativa a serviciilor de dezvoltare,

b) Raportului de progres intermediar nr.13 (RPI13) ce va cuprinde și raport financiar

14. Activitățile de recepție aferente etapei nr.14 (RE14), se vor realiza prin parcurgerea operațiunilor de recepție cantitativă și calitativă a serviciilor de migrare, conform cerințelor caietului de sarcini.

Livrabile pentru recepția cantitativă:

- Proces verbal de recepție cantitativa care va cuprinde minim următoarele documente:
 - Planul de migrare a datelor
 - Strategia de migrare a datelor

Livrabile pentru recepția calitativă:

- Proces verbal de recepție calitativa care va cuprinde cel puțin:
 - Raport privind migrarea datelor

Finalizarea etapei nr. 14 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a procesele verbale de recepție calitativa pentru planul/strategia de migrare,
- b) Raportului de progres intermediar nr.14 (RPI14).

15. Activitățile de recepție aferente etapei nr.15 (RE15), se vor realiza prin parcurgerea operațiunilor de recepție cantitativă și calitativă a de instruire utilizatorilor /administratorilor/ dezvoltatorilor, conform cerințelor caietului de sarcini

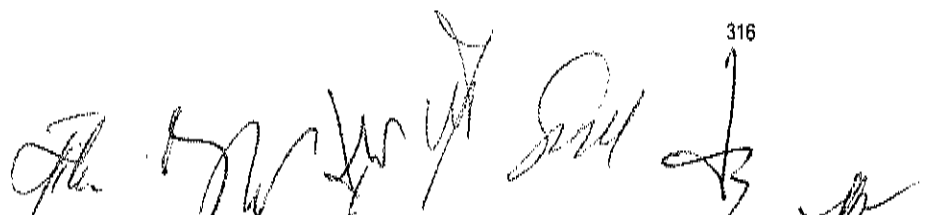
Livrabile pentru aceasta activitate:

- procese verbale cu distribuirea suportului de curs
- rapoarte de activitate
- liste participanți/sesiune
- pontaje
- teste de evaluare a participanților
- formularele de evaluare
- liste de distribuire diplome
- manuale utilizare și administrare (actualizate)

Finalizarea etapei nr. 15 de implementare a contractului se va concretiza prin:

- a) semnarea de catre membrii comisiei de receptie a procesului verbal de recepție cantitativa și calitativa pentru desfășurarea sesiunilor de instruire utilizatorilor/administratorilor/dezvoltatorilor,

316



b) Raportului de progres intermediar nr.15 (RPI15).

16. **Activitățile de recepție aferente etapei finale**, se vor realiza prin efectuarea recepției întregului sistem informatic.

Livrabile pentru aceasta activitate:

- Proces verbal de recepție finală, care va cuprinde cel puțin:
 - Raport de punere în funcțiune a sistemului informatic
 - Raport cuprinzând codul sursă documentat al modulelor/aplicațiilor dezvoltate (actualizat/e). Acceptarea codului sursă pentru sistemul informatic se va face cu demonstrarea funcționării acestuia. Se va efectua cel puțin o modificare, se va compila, se va instala și se va demonstra că funcționează corect pe mediu de test/producție al beneficiarului
 - Fisier/e de configurare module/aplicații (actualizat/e)
 - Procedura de compilare a codului sursă (actualizate)
 - Raport privind existența pe repository GitLab a codului sursă actualizat aferent sistemului informatic
 - Rapoarte de monitorizare și control al proiectului
 - Certificat de garanție pentru sistemul informatic
 - Manuale utilizatori (actualizate)
 - Manuale administrare pentru baze de date, dezvoltatori, administrare utilizatori (actualizate)
 - Raport final al prestatorului care realizează testarea externă
 - Raport de acceptanță și trecere în producție


Finalizarea implementării contractului se va concretiza prin :

- a) semnarea de către membrii comisiei de recepție a achizitorului și reprezentanții autorizați ai furnizorului a procesului verbal de recepție finală
- b) Raportul final (RF) – document elaborat de Prestator prin care se vor recepționa toate activitățile proiectului și punerea în funcțiune a întregului sistem informatic ce face obiectul contractului de finanțare care va cuprinde și raport financiar final.

Toate procesele-verbale aferente activităților de recepție vor conține în mod obligatoriu seriile/versiunile/licențele tuturor produselor hardware și software instalate, configurate și puse în funcțiune precum și toate documentele solicitate în caietul de sarcini și prezentate în propunerea tehnică.

Dacă procedurile realizate de prestatorul care asigură testarea externă vor necesita, după caz, eventuale corecții/update-uri/upgrade-uri, prestatorul va corecta toate problemele constatate, în vederea atingerii scopului declarat al achiziției și anume realizarea unui sistem informatic perfect funcțional și operațional, în termenele stabilite prin graficul de implementare.

317



Procedurile urmate cu ocazia efectuării recepțiilor în cadrul contractului vor fi convenite de comun acord de achizitor și prestator. În caz de divergență între achizitor și prestator, punctul de vedere al achizitorului, emis pe baza prevederilor caietului de sarcini, va prevala.

Se va considera că obligațiile ce revin prestatorului au fost îndeplinite integral în momentul în care sistemul informatic integrat va fi funcțional și operațional 100% la nivel național, conform cerințelor prezentului caiet de sarcini și propunerii tehnice, fapt ce se va materializa prin semnarea de către membrii comisiei de recepție a achizitorului și reprezentanții autorizați ai prestatorului a procesului verbal de recepție finală.

Produsele vor fi livrate în mod obligatoriu împreună cu următoarele documente:

- a) aviz de însoțire a mărfii;
- b) certificate de calitate și garanție;
- c) declarații de conformitate;
- d) documentații tehnice, conform caietului de sarcini și propunerii tehnice.

Documentele/rapoartele/livrabilele solicitate prestatorului sunt prezentate la fiecare activitate și nu exista o limitare a acestora.

Cerințele privind conținutul acestora sunt minimale și se vor adapta conform metodologiei de implementare a proiectului și a ofertei tehnice.

Prestatorul va lua în calcul prezentarea în cadrul propunerii tehnice a cel puțin o revizuire în etapa calitativa în funcție de dimensiunea și importanța lor, cu încadrarea în termenele limita prevăzute în caietul de sarcini pentru fiecare etapa.

11 Informații finale

Ofertantul are obligația de a prezenta organizarea și metodologia privind prestarea serviciilor conform Formularului de propunere tehnică - Anexa 2 la Caietul de Sarcini.

În situația în care comisia de evaluare constată că elemente de preț ale unei oferte sunt aparent neobișnuit de scăzute, prin raportare la prețurile pieței, comisia de evaluare va solicita ofertantului care a depus oferta în cauză explicații cu privire la posibilitatea îndeplinirii contractului în condițiile de calitate impuse prin documentația de atribuire. Explicațiile aduse de ofertant vor fi însoțite de dovezi concludente privind elementele prevăzute la art. 210 alin. (2) din Legea nr. 98/ 2016, precum și, după caz, documente privind prețurile ce pot fi obținute de la furnizori, modul de organizare și metodele utilizate în cadrul procesului de lucru, nivelul de salarizare al personalului ofertantului, performanțele și costurile implicate de anumite utilaje sau echipamente de lucru.

În cazul în care ofertantul nu prezintă comisiei de evaluare informațiile și/sau documentele solicitate sau acestea nu justifică în mod corespunzător nivelul scăzut al prețului sau al costurilor propuse, oferta va fi considerată inacceptabilă.

Ofertanții trebuie să întocmească 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

îndeplinește aceste cerințe, planul de lucru, personalul utilizat și organizarea acestuia, astfel încât comisia de evaluare să aibă posibilitatea evaluării acestuia în mod obiectiv.

Simpla copiere a conținutului caietului de sarcini în Propunerea Tehnică nu reprezintă îndeplinirea cerințelor de conformitate anterior enunțate.

La elaborarea propunerii tehnice, ofertanții vor răspunde punct cu punct la toate cerințele prezentei documentații detaliind soluția oferită într-un mod în care să se poată face cu ușurință verificarea conformității.

Pentru fiecare componentă, fie hardware, fie software, se vor preciza în mod distinct denumirea, producătorul, cantități, capacități, referințe la materiale din care să reiasă în mod clar soluția oferită.

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).

Ofertantul va detalia modul în care echipamentele, componentele și produsele software oferite răspund la fiecare dintre cerințele enumerate în parte, descriind funcționalitățile și opțiunile acestora. Separat, vor fi prezentate de asemenea și funcționalitățile suplimentare.

Oferta va cuprinde obligatoriu fisele tehnice, manualele sau/și ghidurile de prezentare sau orice alte documente relevante pentru toate echipamentele, componentele și produsele software prezentate, astfel încât să rezulte faptul că acestea respecta cerințele din prezentul caiet de sarcini.

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 caietul de sarcini. Oferta tehnică trebuie să fie prezentată și într-un format editabil care să permită selectarea textului, copierea acestuia, precum și cu toate referințele (link-urile) către site-uri în format hyperlink, „gata de click” (în acest sens solicităm prezentarea ofertei tehnice și în format Microsoft Word sau într-un format care să permită copierea textului către Microsoft Word cu păstrarea formatării acestuia).

Ofertanții au obligativitatea prezentării pentru fiecare dintre membrii personalului care va face parte din echipa de proiect, conform poziției de expert cheie pe care este alocat, toate documentele necesare evaluării, în mod ordonat, pentru a facilita procesul de evaluare.

Omission sau neîndeplinirea corespunzătoare a oricărei dintre cerințele prezentului caiet de sarcini poate conduce la declararea ofertei ca fiind 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 ofertanților și intră în răspunderea acestora prezentarea dovezilor concrete în sprijinul oricăror afirmații care se pot încadra în categoria exemplului anterior menționat.

Toate livrabilele furnizate în cadrul proiectului de către Prestator vor fi în limba română.

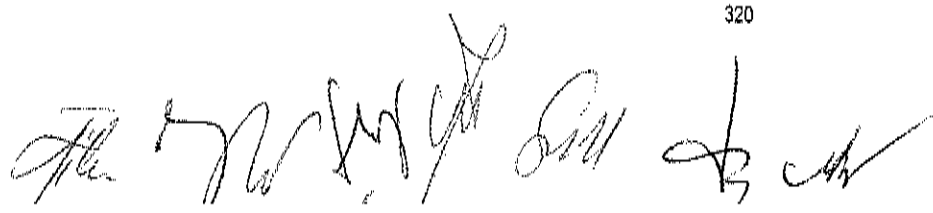
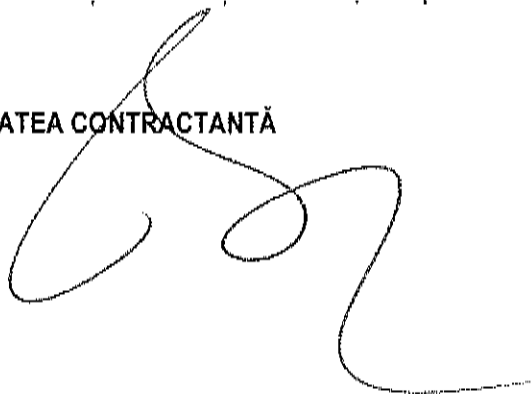
Specificațiile tehnice definite în cadrul prezentului caiet de sarcini corespund necesităților și exigentelor autorității contractante. Având în vedere specificitatea acestui proiect, autoritatea a descris sistemul informatic ce va fi achiziționat la nivelul de detaliu necesar operatorilor economici interesați, permițând identificarea obiectului acestui contract de achiziție publică.

Orice referire din cuprinsul prezentei documentații de atribuire (inclusiv a caietului de sarcini), prin care se indică o anumită atestare/autorizare/certificare, origine, sursă, producție, un procedeu special, o marcă de



fabrică sau de comerț, un brevet de invenție și/sau o licență de fabricație se va citi și interpreta ca fiind însoțită de mențiunea „sau echivalent”.

AUTORITATEA CONTRACTANTĂ



12 Anexa 1 – Indicatori de performanță pentru realizarea activităților 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
Document de analiză adecvat pentru scopul utilizării	Capitolul Analiza - Document analiză de business	Documentația de analiză este livrată conform cerințelor stabilite în Caietul de Sarcini	Nivelul de acuratețe al documentației livrate după o "evaluare reciproca" (ponderare informații inexacte / sub nivelul de calitate agreat în informațiile furnizate)	<p>Foarte bine(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. Documentația a fost folosită pentru etapa următoare așa cum a fost prezentată de către Prestator.</p> <p>Bine (4 puncte) – Documentația livrată include unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreat. Documentația a fost folosită pentru etapa următoare așa cum a fost prezentată, fiind necesare doar ajustări nemateriale.</p> <p>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.</p>	Evaluarea aplicabilității și relevanței documentației de analiză

321



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
				<p>Documentația a putut fi folosită pentru etapa următoare după ce a fost corectată de câteva ori.</p> <p>Nu au existat întâzieri semnificative ca urmare a corecturilor.</p> <p>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 (de exemplu au cauzat întâzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate, fără costuri suplimentare pentru Autoritatea Contractantă.</p> <p>Foarte Slab (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.</p>	



 322

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
Document proiectare adecvat pentru scopul utilizării	Capitolul Proiectarea software Document proiectare detaliata	Documentația de proiectare este livrată conform cerințelor stabilite în Caietul de Sarcini	Nivelul de acuratețe al documentației livrate după "evaluare reciprocă" (ponderare informațiilor inexacte / sub nivelul de calitate agreeat în informațiile furnizate)	<p>Autonitatea 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.</p> <p>Foarte bine(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. Documentația a fost folosită pentru etapa următoare așa cum a fost prezentată de către Prestator.</p> <p>Bine (4 puncte) – Documentația livrată include unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreeat. Documentația a fost folosită pentru etapa următoare așa cum a fost prezentată, fiind necesare doar ajustări nemateriale.</p>	Evaluarea aplicabilității și relevanței documentației de proiectare

323

[Handwritten signature]

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
				<p>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.</p> <p>Documentația a putut fi folosită pentru etapa următoare după ce a fost corectată de câteva ori.</p> <p>Nu au existat întârzieri semnificative ca urmare a corecturilor.</p> <p>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 (de exemplu au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate, fără costuri suplimentare pentru Autoritatea Contractantă.</p>	

324



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
Livrabil final în termenul agreat	Capitolul Servicii de management de proiect	Sistemul informatic a fost pus în funcțiune conform termenului agreat în contract	Livrarea la timp a rezultatelor	<p>Foarte Slab (1 punct) – Documentația livrată a inclus neconformități / inexactități majore față de nivelul agreat sau a fost folosit tehnologii/metode complet învechite care erau, în principal, abandonate de industrie, iar aceste aspecte nu au putut fi corectate. 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.</p> <p>Foarte bine(5 puncte) – rezultatele au fost livrate de către Prestator în termenele convenite în contract.</p> <p>Bine (4 puncte) – livrate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului.</p> <p>Acceptabil (3 puncte) – livrate după încheierea termenelor convenite în Contract conducând la</p>	
				Evaluarea finalizării la timp punerii în funcțiune a sistemului informatic	

325

[Handwritten signature]

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
				<p>întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate.</p> <p>Nesatisfăcător (2 puncte) – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului (de exemplu mai mult de 60 de zile).</p> <p>Foarte Slab (1 puncte) – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului (de exemplu mai mult de 120 de zile).</p>	


 325