Caiet de Sarcini

“Achiziţie a infrastructurii hardware şi software de bază, a serviciilor de dezvoltare şi implementare a Sistemului Informatic pentru Managementul Integrat al Serviciilor pentru Cetateni (SIMISC) propus prin proiect (analiză, proiectare, implementare, testare sistem informatic, inclusiv portal web), precum si a serviciilor de instruire a personalului care va utiliza şi administra sistemul informatic dezvoltat, respectiv a serviciilor de consultanţă în domeniul managementului de proiect”

Axa Prioritară III "Tehnologia Informaţiei şi Comunicaţiilor pentru sectoarele privat şi public"

Domeniul Major de Intervenţie 2 „Dezvoltarea şi creşterea eficienţei serviciilor publice electronice”

Operaţiunea 1 „Susţinerea implementării de soluţii de e-guvernare şi asigurarea conexiunii la broadband, acolo unde este necesar”

1.

1. AUTORITATEA CONTRACTANTA

Numele instituţiei conform actului de înfiinţare: Ministerul Afacerilor Externe

Cod de înregistrare fiscală: 4266863

Adresa poştală: Aleea Alexandru, Nr. 31, Sector 1, Bucureşti, cod 011822

Telefon / Fax: (40 21) 319.21.08 sau 319.21.25/ (40 21) 319.68.62

Ministerul Afacerilor Externe (MAE) este organizat şi funcţionează în conformitate cu Hotărârea Guvernului nr. 8 din 9 ianuarie 2013 privind organizarea şi funcţionarea Ministerului Afacerilor Externe.

Activitatea ministerului este condusă de ministrul afacerilor externe, care totodată îl reprezintă în raporturile cu celelalte autorităţi publice, cu persoanele juridice şi fizice din ţară şi din străinătate, precum şi în justiţie. De asemenea, ministrul afacerilor externe răspunde de întreaga activitate a ministerului în faţa Guvernului, precum şi, în calitate de membru al Guvernului, în faţa Parlamentului.

Misiunea Ministerului Afacerilor Externe este de a asigura realizarea politicii externe a statului român în concordanţă cu interesele naţionale şi cu statutul României de stat membru în structurile europene şi euroatlantice.

Conform actelor normative în vigoare, Ministerul Afacerilor Externe, denumit în continuare MAE, asigură realizarea politicii externe a statului român, inclusiv participarea la procesul de integrare europeană şi euroatlantică a României, şi colaborează la elaborarea, fundamentarea şi realizarea politicii economice a României, în conformitate cu reglementările legale în vigoare şi cu Programul de guvernare.

Prin atribuţiile sale principale, MAE:

- Apără şi promovează pe plan extern interesele naţionale ale României;
- Iniţiază activităţi internaţionale menite să ducă la dezvoltarea de relaţii paşnice şi de cooperare cu toate statele, întemeiate pe principiile şi pe normele general admise ale dreptului internaţional;
- Asigură promovarea intereselor României în organizaţii internaţionale cu caracter universal, european, euroatlantic, regional şi subregional;
- Asigură conectarea ţării la instituţiile europene şi euroatlantice cu caracter politic, strategic şi economic;
- Participă la coordonarea sistemului naţional de gestionare a afacerilor europene;
- Asigură, prin acţiuni de politică externă, consolidarea statului de drept şi a structurilor democratice din societatea românească, precum şi proiectarea unei imagini reale a României în lume;

- Urmăreşte evoluţia vieţii internaţionale şi semnalează tendinţele care apar în contextul internaţional;
- Contribuie la asigurarea prezenţei active şi demne a României şi a cetăţenilor săi pe plan internaţional;
- Promovează pe plan internaţional valorile democraţiei, respectarea drepturilor omului, colaborarea paşnică şi solidaritatea umană;
- Apără în străinătate drepturile şi interesele statului român, ale cetăţenilor şi ale persoanelor juridice române, pe baza legislaţiei române şi în conformitate cu practica internaţională şi cu acordurile bilaterale şi multilaterale la care România este parte;
- Elaborează şi aplică politica statului român în domeniul relaţiilor cu comunităţile româneşti din afara graniţelor şi acţionează pentru întărirea legăturilor cu românii din afara frontierelor României şi pentru păstrarea, dezvoltarea şi exprimarea identităţii lor etnice, culturale, lingvistice şi religioase, cu respectarea legislaţiei statului ai cărui rezidenţi sunt;
- Iniţiază sau participă la negocierea tratatelor şi a altor înţelegeri internaţionale pentru România;
- Prezintă Guvernului, singur sau, după caz, împreună cu celelalte ministere, propuneri privind semnarea, ratificarea, aprobarea sau acceptarea înţelegerilor internaţionale, aderarea la acestea ori denunţarea lor, efectuează schimbul instrumentelor de ratificare, depune instrumentele de ratificare sau de aderare, notifică aprobarea ori acceptarea înţelegerilor internaţionale şi denunţarea lor, eliberează documente certificând deplinele puteri;
- Urmăreşte, direct sau în conlucrare cu ministerele şi cu celelalte autorităţi publice centrale de specialitate, aplicarea prevederilor tratatelor şi ale altor înţelegeri internaţionale la care România este parte şi prezintă propuneri pentru îndeplinirea întocmai şi cu bună-credinţă a obligaţiilor asumate;
- Exercită, în numele Guvernului României, prerogativele de Agent guvernamental în procedurile în faţa Curţii Europene a Drepturilor Omului şi a Comitetului Miniştrilor ale Consiliului Europei, îl informează constant pe primul-ministru cu privire la activitatea Agentului guvernamental şi formulează propuneri de acţiune;
- Elaborează sau cooperează cu ministerele şi cu celelalte autorităţi publice centrale de specialitate la elaborarea proiectelor de acte normative care au legătură cu relaţiile externe şi cu politica de comerţ exterior ale României;
- Asigură asistenţă permanentă şi coordonare în domeniul relaţiilor internaţionale tuturor ministerelor;
- Formulează norme şi asigură sprijin instituţiilor centrale de stat în materie de protocol şi curtoazie internaţională;
- Contribuie la monitorizarea respectării angajamentelor asumate prin Tratatul de aderare la UE;

- Colaborează la elaborarea politicii României în domeniul relaţiilor economice internaţionale;
- Promovează interesele economice ale României în relaţiile cu alte state, precum şi cu organizaţiile economice cu vocaţie universală, cu caracter regional şi cu alte grupări economice;
- Participă sau colaborează, după caz, la negocierea şi la încheierea de tratate, acorduri şi alte înţelegeri internaţionale cu caracter economic sau pentru stabilirea cadrului juridic necesar, în vederea desfăşurării relaţiilor comerciale externe ale României, potrivit legii;
- Păstrează originalele tuturor înţelegerilor internaţionale bilaterale şi copiile certificate de pe înţelegerile internaţionale, originalele înţelegerilor internaţionale al căror depozitar este România şi îndeplineşte obligaţiile ce decurg din această calitate;
- Păstrează sigiliul de stat al României;
- Supune spre aprobare scrisorile de acreditare, cererile de agrement şi de exequatur; ţine legătura cu misiunile diplomatice şi cu oficiile consulare din România în conformitate cu regulile şi cu practica internaţională;
- Organizează, îndrumă şi controlează activitatea misiunilor diplomatice şi a oficiilor consulare ale României; organizează curierul diplomatic;
- Asigură aplicarea politicii naţionale în domeniul relaţiilor culturale, ştiinţifice şi de învăţământ cu alte state;
- Contribuie la cunoaşterea şi difuzarea valorilor culturii, ştiinţei şi învăţământului românesc şi sprijină participarea României la manifestări internaţionale de profil.

Pentru realizarea obiectivelor din domeniul său de activitate, MAE exercită următoarele funcţii:

- Funcţia de strategie, prin care se asigură elaborarea strategiei de punere în aplicare a Programului de guvernare în domeniul său de activitate;
- Funcţia de reglementare, prin care se asigură elaborarea cadrului normativ şi instituţional pentru realizarea obiectivelor strategice din domeniul său de activitate;
- Funcţia de reprezentare, prin care se asigură, în numele statului sau al Guvernului României, reprezentarea pe plan intern şi extern în domeniul său de activitate;
- Funcţia de autoritate de stat, prin care se asigură urmărirea şi controlul aplicării şi respectării reglementărilor legale din domeniul său de activitate şi a celor privind organizarea şi funcţionarea instituţiilor care îşi desfăşoară activitatea în subordinea sau sub autoritatea sa;
- Funcţia de administrare, prin care se asigură administrarea patrimoniului său, potrivit dispoziţiilor legale.

2. BENEFICIARII PROIECTULUI

BENEFICIARII DIRECȚI:

Cetăţenii români vor avea acces la informaţii consulare de calitate într-un mod eficient şi transparent. Aceștia vor beneficia de un confort crescut datorită posibilității de a interacționa Online (direct) cu personalul Ministerul Afacerilor Externe, de a trimite solicitări prin mijloace electronice fără a mai fi nevoiţi să se deplaseze in mod repetat la ghişeu, eliminându-se astfel barierele birocratice și pe cele geografice.

Proiectul vizează pentru aceștia simplificarea depunerii şi ridicării de acte administrative referitoare la serviciile consulare prestate de Ministerul Afacerilor Externe, prin rețeaua consulară externă, obținându-se astfel o diminuare a birocrației.

Pe termen lung, îmbunătățirea datorată implementării proiectului va duce la creşterea încrederii cetăţeanului/mediului de afaceri în serviciile consulare furnizate de Ministerul Afacerilor Externe.

Cetățenii si mediul de afaceri vor avea acces direct la informații consulare, indiferent de timp și spațiu, procedurile de rutină vor avea o durată mai mică, iar problemele și cererile persoanelor fizice și juridice vor putea fi rezolvate rapid și interactiv, modulele propuse prin proiect având un grad ridicat de actualizare a informațiilor de ordin consular.

Ministerul Afacerilor Externe, prin reprezentanțele sale consulare va beneficia ca urmare a implementării proiectului prin faptul ca își va îmbunătăţi și diversifica calitatea serviciilor oferite cetăţenilor și mediului de afaceri.

Principala modalitate prin care se vor materializa beneficiile pe care le va aduce proiectul Ministerului Afacerilor Externe va fi reprezentată de standardizarea procedurilor de lucru şi consolidarea structurilor de date, reducerea birocraţiei şi descongestionarea activităţii desfăşurate de reprezentanțele sale, dar la și reducerea reală a costurilor interne ale insituției.

În calitate de beneficiar direct, Ministerul Afacerilor Externe va avea oportunitatea deținerii unui nou flux organizaţional rezultat odată cu finalizarea implementării proiectului prin prisma faptului că fiecare din modulele noului sistem informatic implementat va impune crearea unor noi tipuri de activități, responsabilități, atribuții și matrice funcționale.

Angajații Ministerul Afacerilor Externe implicaţi în derularea proceselor de urmărire a stadiului de derulare/finalizare a solicitărilor cetăţenilor români în contextul automatizării fluxurilor interne de lucru vor beneficia de o creştere a productivităţii. Tot aceștia își vor îmbunătăţi competenţele profesionale prin organizarea de cursuri de instruire care să le permită să acţioneze mai eficient prin folosirea sistemului informatic integrat propus. In urma utilizării sistemului propus, numărului de erori datorate fluxului de lucru complicat din cadrul Ministerului Afacerilor Externe va scădea.

BENEFICIARI INDIRECȚI:

Guvernul României, având în vedere realaționarea directă cu Ministerul Afacerilor Externe, va beneficia de fiecare din schimbarile produse în instituția solicitantului și de rezultatele implementării proiectului.

Direcţia Cazier Judiciar, Statistică si Evidenţe Operative este unul dintre beneficiarii indirecți ai proiectului prin prisma interacțiunii reprezentate cel puțin de schimbul de date cu privire la cazierele eliberate de catre Ministerul Afacerilor Externe, sistemul informatic integrat reprezentând instrumentul ce va asigura transferul în timp real al informațiilor în mod bidirecțional, asigurând inclusiv realizarea statisticilor imediate.

Uniunea Nationala a Notarilor Publici din Romania deține calitatea de beneficiar indirect avand în vedere nevoile și soluționarea acestor nevoi prin implementarea proiectului, nevoie ce privește trasferul în timp real de documente cu incidență juridica între cele două instituții.

Directia pentru Evidenta Persoanelor și Administrarea Bazelor de Date va avea ca beneficiu principal, odată cu finalizarea implementării proiectului, accesul la informațiile cu privire la cetățenii români ce solicita servicii prin intermediul Ministerului Afacerilor Externe și implicit cu privire la statutul acestora.

Putem enumera fară a ne limita printre beneficiarii indirecți și Autoritatea Națională pentru Cetățenie, Centrul de Cooperare Polițienească Internațională, Inspectoratul General al Poliției Române, Ministerul Justiției etc.

Statul Român prin prisma calității imaginii pe care o va propaga față de cetățenii români odată cu oferirea unor servicii moderne și eficiente.

3. OBIECTIVELE PROIECTULUI

Obiectiv general: îl reprezintă implementarea unui sistem informatic de eficientizare și modernizare a serviciilor în domeniul consular oferite cetățenilor români ce va garanta creşterea eficacităţii şi calităţii serviciilor asigurate de Ministerul Afacerilor Externe (MAE), alături de accesul facil la serviciile administrației publice, inclusiv prin eficientizarea activităţilor interne ale instituţiei utilizând mijloace specifice tehnologiei informaţiei şi comunicaţiei.

Obiective specifice care trebuie indeplinite:

1. Creşterea capacităţii de comunicare, înregistrare, interfaţare, sinteză şi raportare asupra cererilor de servicii formulate de cetățenii români și adresate MAE și reprezentanților Ministerul Afacerilor Externe, dar şi a activităţii de control a instituţiei în vederea diminuării timpului de răspuns şi creşterii calităţii prestaţiei către diferiţi actori cu care instituţia interacţionează, în conformitate cu legislaţia în vigoare, în respect cu principiile e-guvernarii, respectiv al promovarii valorilor democratice privind deschiderea, transparența și răspunderea în interacțiunea cu ceilalți actori;

2. Creşterea calităţii serviciilor destinate cetățenilor români oferite de Ministerul Afacerilor Externe prin realizarea unui portal de aplicare online având ca scop obținerea serviciilor specifice instituției, în respect cu principiul e-guvernării privind accesibilitatea printr-un instrument centrat pe nevoile cetăţeanului şi nu pe fluxurile interne ale administraţiei publice, instrument ce va asigura oferirea de mecanisme de navigare clare, respectiv conținut relevant și de calitate;

3. Asigurarea unui instrument informatic inteligent care, prin nivelul ridicat de deschidere către cetățean, va reprezenta un mijloc de comunicare și interacțiune sigur și, în același timp transparent, între cei doi actori principali ce vor beneficia de acest instrument – cetățeanul român și Ministerul Afacerilor Externe;

4. Eficientizarea activităţilor de control şi raportare a angajaților Ministerului Afacerilor Externe prin reducerea birocrației și sporirea capacităţii tehnologice de a accesa informație relevantă din sistemele informatice ale instituției, în timp real, în concordanță cu principiul e-guvernarii privind eficientizarea și cresterea productivității muncii angajaților, o organizare mai bună a acestora și producerea de economii financiare având la bază o arhitectura TIC mai vastă și îmbunătățită;

5. Modernizarea și creșterea productivității muncii angajaților prin eficientizarea activităţii interne a instituţiei, care stă la baza furnizării de servicii publice electronice eficace, prin informatizarea sistemelor, în respect cu principiul e-guvernarii privind îmbunatatirea eficacității organizației prin reducerea birocratiei si cresterea satisfactiei utilizatorului;

6. Creşterea accesului și a numarului utilizatorilor la serviciile electronice moderne prin crearea posibilitaţii de a interacţiona online cu administraţia publică, de a solicita şi primi raspunsuri la solicitări, dar şi de a fi informaţi cu privire la ultimele noutăţi de interes public, in lumina principiului e-guvernarii privind accesibilitatea prin furnizarea serviciului prin canale alternative, oferirea unei interfete simple, usor de invățat și de utilizat;

7. Reducerea timpului alocat completării, depunerii de formulare, dar şi obţinerea informaţiilor de interes public în timp real, prin mijloace electronice complet tranzacționale (sofisticare nivel 5) (cetăţean – administraţie publică, administraţie publică - cetăţean), în conformitate cu principiul e-guvernării privind siguranța, respectiv protejarea confidențialității datelor furnizate de utilizatori;

8. Creşterea abilităţilor de utilizare a tehnologiei informaţiei de către angajaţii Ministerului Afacerilor Externe utilizand cunoştinte specifice dobândite în urma activităţilor de training.

4. CERINȚE PRIVIND SOLUȚIA TEHNICĂ

4.1.Activităţile implementării sistemului

Realizarea activităților implementării sistemului trebuie realizate in maxim 11 luni de la data semnării contractului de furnizare.

Activitățile sunt prezentate în continuare:

Activitatea 3. Dezvoltarea şi implementarea Sistemului Informatic pentru Managementul Integrat al Serviciilor pentru Cetateni	
Subactivitate	**Descriere**
Subactivitatea 3.1. Analiza sistemului informatic integrat	Activitatea constă în analiza cadrului legislativ și a activității derulate de instituția solicitantă în vederea stabilirii în mod concret a elementelor ce definesc procesele de lucru corespunzatoare solicitării și asigurării serviciilor consulare de Ministerul Afacerilor Externe și destinate cetățenilor români. În cadrul acestei activităţi vor fi determinate cerinţele funcţionale ale SIMISC, atât din punctul de vedere al cetățeanului român în calitate de solicitant al serviciilor, cât și din punctul de vedere al Ministerului Afacerilor Externe și reprezentanților sale – în calitate de furnizor al serviciilor, dar şi din punctul de vedere al infrastructurii tehnice şi de securitate, cu accent pe scalabilitate, securitate si interoperabilitate. Tot în cadrul acestei etape se va urmări în mod expres ca noul sistem să dețină capacitatea de a suporta în mod corect și sigur un volum mare de încărcare și de a permite mărirea sau extinderea sa în viitor, prin asigurarea opțiunii de adăugare de resurse adiționale (hardware și software) – scalabilitate verticală și orizontală.
Subactivitatea 3.2. Livrarea, instalarea și configurarea infrastructurii hardware și software necesare pentru realizarea proiectului	Această activitate va presupune livrarea, instalarea și configurarea infrastructurii hardware și software necesare pentru realizarea proiectului la sediul solicitantului
Subactivitatea 3.3. Proiectarea și dezvoltarea SIMISC	În cadrul activității se va realiza: 3.3.1. Definirea arhitecturii funcţionale ce va presupune identificarea și detalierea proceselor ce vor fi informatizate în cadrul proiectului de implementare al SIMISC. Totodată, pentru fiecare proces se vor detalia machetele de ecran precum și constrângerile şi regulile asociate. Indicatorii de calitate urmariti

Activitatea 3. Dezvoltarea şi implementarea Sistemului Informatic pentru Managementul Integrat al Serviciilor pentru Cetateni	
Subactivitate	**Descriere**
	vor fi: fiabilitatea, scalabilitatea, performanța și securitatea; 3.3.2. Definirea arhitecturii tehnice, ce presupune detalierea SIMISC din punct de vedere tehnic, ținând cont de infrastructura de servere, stocare şi comunicaţii. 3.3.3. Dezvoltarea modelului informaţional ce va presupune realizarea efectiva a arhitecturii de date a SIMISC, la nivel logic şi fizic. 3.3.4. Proiectarea modulelor SIMISC ce va include cel puțin: 1. Portal – componentă externă cu secțiune privată și secțiune publică; 2. Portal – componentă internă de gestiune cereri servicii; 3. Modul de raportare; 4. Modul de gestiune financiară; 5. Modul registratură; 6. Modul gestiune programări; 7. Modul transformare şi preluare date de la Direcția pentru Evidența Persoanelor și Administrarea Bazelor de Date (DEPABD); 8. Modul interfaţare cu SIIEASC (Sistemul informatic integrat de emitere a actelor de stare civila); 9. Modul interfațare cu sistemele electronice puse la dispoziție de Uniunea Notarilor Publici din România; 10. Modul interfațare cu DGP și CCPI, pentru cetățenii români arestați, deținuți sau decedați; 11. Modul interfațare cu sistemul electronic al Cazierului judiciar; 12. Modul interfațare cu Autoritatea Națională pentru Cetățenie; 13. Modul interfațare cu Ministerul Justiției; 14. Modul interfațare cu Autoritatea Electorală Permanentă; 15. Modul derulare plăți electronice online;

Activitatea 3. Dezvoltarea şi implementarea Sistemului Informatic pentru Managementul Integrat al Serviciilor pentru Cetateni	
Subactivitate	**Descriere**
	16. Modul interfațare cu Direcția Protecția Copilului; 17. Alte interfațări ce vor rezulta în urma analizei detaliate din cadrul implementării proiectului, într-un număr de până la 25 de interfațări; 18. Gestionarea în format electronic a normelor și procedurilor interne de lucru în domeniul consular;
Subactivitatea 3.4. Testarea SIMISC	SIMISC va fi testat din punct de vedere funcţional, rezultatele testării urmând a fi consemnate pe baza unui proces verbal de acceptanţă. Această activitate se va focaliza pe procesul de identificare a posibilelor erori de program, erori care ar putea avea un impact negativ asupra desfăşurării activităţilor viitoare. Totodată se va realiza în perioada implementării un pilot de testare cu un numar redus de locații.
Subactivitatea 3.5. Implementarea SIMISC	Această activitate va presupune punerea în funcțiune a componentelor SIMISC și utilizarea acestora în mediu de producție, în mod asistat.
Subactivitatea 3.6. Instruirea personalului care va utiliza produsele software implementate şi a celui care va asigura mentenanţa SIMISC	Instruirea se va realiza de catre contractorul serviciilor de dezvoltare sistem SIMISC și va avea loc în limba română, furnizorul de instruire urmând a emite certificate de participare pentru toţi cursanţii. Activitățile de instruire vor viza 3 tipuri de utilizatori ai sistemului: 1.Administratori – vor beneficia de nivelul tehnic cel mai ridicat din punct de vedere al cunoștințelor diseminate pe durata instruirii (5 persoane, 1 sesiune, 3 zile/sesiune de instruire) 2. Utilizatori cheie – vor beneficia de un nivel tehnic mediu din punct de vedere al cunostințelor disemniate pe durata instruirii. Metoda de instruire utilizată pentru acest tip de utilizatori va respecta principiile metodologiei “Train of trainers” (formare de formatori), având în vedere că ulterior finalizării perioadei de implementare a proiectului, utilizatorii cheie vor avea responsabilitatea de instruire a noilor utilizatori ai sistemului (20 persoane, 2 sesiuni de instruire, 3 zile/sesiune de instruire) 3.Utilizatori finali – vor beneficia de un nivel tehnic corespunzător necesarului de cunostințe în vederea operării curente a soluției

Activitatea 3. Dezvoltarea şi implementarea Sistemului Informatic pentru Managementul Integrat al Serviciilor pentru Cetateni	
Subactivitate	**Descriere**
	implementate (140 persoane, 20 sesiuni de instruire, 1 zi/sesiune de instruire). De asemenea, furnizorul serviciilor de instruire va pune la dispoziţia utilizatorilor o documentaţie de instruire în limba română, atât în format fizic, cât și în format electronic, care va include materiale în limba română, pe categorii de utilizatori: manuale/ghiduri de administrare pentru persoanele care vor administra sistemul; manuale/ghiduri de configurare și manuale/ghiduri pentru instruire pentru persoanele care vor asigura instruirea noilor utilizatori ai aplicației; manuale/ghiduri de utilizare pentru utilizatorii ce vor asigura operarea curentă a soluției implementate.

4.2.Cerinţe generale

În definirea arhitecturii sistemului integrat SIMISC, s-au avut în vedere următoarele caracteristici fundamentale, necesare sistemului ce se aliniază principiilor e-guvernare și necesităților cetățeanului:

Valoare reală pentru cetățean:

Sistemul integrat trebuie sa ofere cel puțin 8 categorii generale mari de servicii electronice care trebuie să se constituie într-un ajutor real pentru cetățean prin îmbunătățirea experienței acestuia în relația cu MAE, prin scurtatea timpului și diminuarea efortului necesar pentru accesarea serviciilor. Valoarea acestora trebuie demonstrată prin asigurarea în cadrul proiectului a implementării unor servicii cu nivel de sofisticare 4 și 5 (efectuarea de plăţi prin mijloace electronice şi pro-activitate a sistemului).

Servicii complete pentru cetățean:

Trebuie sa se realizeze implementarea unui set complet de servicii electronice pentru cetățean, nu a câtorva servicii izolate, pentru crearea unei experiențe comune în utilizare și mai ales pentru a maximiza șansele ca cetățeanul să poată beneficia în mod integral de toate serviciile dorite în mod electronic. Sistemul integrat trebuie sa implementeze minim 8 categorii generale mari de servicii electronice cu funcționalități front-office, adică în mod direct accesibile cetățeanului (solicitare serviciu online, solicitare serviciu cetățenie, solicitare documente identitate și de călătorie, solicitare serviciu acte stare civilă, solicitare serviciu acte notariale, solicitare serviciu obținerea de acte din România, solicitare serviciu alte servicii, registre etc).

În același timp, în mod indirect, cetățeanul trebuie sa beneficieze și de serviciile electronice de tip back-office: managementul serviciilor oferite, configurare program lucru la reprezentanță, raportări, gestiune tipizate, gestiune parametri aplicație, gestiune reprezentanțe, gestiune angajați, gestiune nomenclatoare suport.

Accesibilitate:

Serviciile electronice oferite trebuie furnizate utilizatorilor folosind o interfaţă grafică simplă, ce va permite accesul nerestricţionat unui număr cât mai mare de utilizatori. Design-ul interfeţei grafice trebuie sa fie realizat în funcţie de nevoile utilizatorilor pentru a le permite acestora accesul rapid la toate serviciile electronice, formularele şi informaţiile de interes public. Formularele şi structura serviciilor din cadrul portalului trebuie sa aibă prezentare standard, facilitând astfel claritatea, navigabilitatea şi uşurinţă de folosire. Portalul trebuie sa ofere posibilitatea de acces personalizat (prin pagini personalizate ale utilizatorilor), facilitate care va uşura mult navigarea şi înregistrarea diferitelor solicitări.

Accesul utilizatorilor la serviciile electronice nu trebuie sa fie îngrădit în niciun fel, în sensul că nu trebuie sa existe o limitare a numărului maxim de utilizatori logaţi.

Deasemenea serviciile electronice trebuie să poată fi accesate într-un mod facil și folosind echipamentele mobile.

Eficiența:

Procedurile trebuie sa fie clare şi directe, formularele mai uşor de completat, datele trebuie sa fie mai uşor de prelucrat, gradul de responsabilizare şi siguranţa va creşte, iar instituția îşi va eficientiza activitatea (costurile vor fi scăzute, vor fi promovate serviciile cu impact ridicat, va creşte productivitatea muncii angajaţilor, etc.)

Implementarea proiectului trebuie sa aibă un impact pozitiv direct asupra întregii activităţii a instituţiei. Asfel va creşte eficienţa muncii angajaţilor instituţiei prin reducerea aglomeraţiei de la ghişeu, se va reduce timpul de procesare a informaţiilor, se vor reduce costurile de furnizare a informaţiilor prin economia de hârtie ce se va realiza.

Eficacitate:

Oferirea alternativei electronice la serviciile clasice, precum şi automatizarea activităţilor funcționarilor vor asigura o reducere a timpului de prestare a serviciilor şi vor spori confortul utilizatorilor interni şi al cetăţenilor, aceştia din urmă putând beneficia de o interacţiune online directă cu MAE, eliminându-se barierele birocratice.

Inovativitate şi neutralitate tehnologică, adaptare la modificări:

Aplicaţia trebuie sa fie proiectată astfel încât soluţiile ce vor fi folosite la implementare să fie scalabile tehnologic pentru a permite dezvoltări continue. Astfel aplicaţia informatică trebuie sa fie inovativa şi să poată fi dezvoltată continuu în funcţie de necesităţi, de evoluțiile la nivel legislativ, fără restricţii. Totodată, aplicaţia trebuie să permită conectarea la orice sistem naţional cu dezvoltări ulterioare minime ***prin conectori in tehnologie web si XML***.

Siguranța - protejarea confidenţialităţii datelor furnizate de utilizatori:

Proiectul propus trebuie sa respecte prevederile legislaţiei în vigoare care asigura confidenţialitatea datelor cu caracter personal şi cea privind dreptul de informare al cetăţeanului:

- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice
- Legea nr. 677/2001 privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
- Legea nr. 52/2003 privind transparentă decizională în administraţia publică;
- Ordinul Avocatului Poporului nr. 52/2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.

Scalabilitatea:

Aplicaţia informatică trebuie să facă faţă unui nivel de încărcare continuu crescător, fără a-i fi diminuată performanţă. Componentele majore ale arhitecturi de sistem ce trebuie sa se supuna scalabilităţii sunt: topologiile şi sistemele de reţea, serverele de aplicaţii, serviciile de infrastructură, componentele de management al infrastructurii şi subsistemele responsabile de stocarea datelor. Sistemul nu trebuie să permită pierderea datelor, în acest sens fiind necesare capabilităţi de restaurare în caz de accident şi modalităţi de prevenire a acestora. Totodată, arhitectura de sistem trebuie să conțină o componentă de securizare a infrastructurii care să nu permită accesul neautorizat la date.

Aplicația trebuie să poată integra, prin metode consacrate de interconectare (conectori in tehnologie web si XML), module ce vor fi dezvoltate ulterior, în cadrul altor proiecte.

Aplicaţia electronică ce trebuie să fie implementată va fi interconectată cu Sistemul Electronic Naţional cu ajutorul serviciilor web deschise, conform Legii nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificări şi completări ulterioare, respectând condiţiile tehnice în care se poate asigura interconectarea.

4.3.Prevederi de securitate

Luând în considerare natura confidenţială a datelor ce vor fi colectate, sistemul integrat SIMISC trebuie să conţină un sistem de securitate performant, ce suportă funcţionalităţi de integrare şi autentificare, care să respecte obligatoriu cel puţin cerinţele minime de securitate prezentate în ORDINUL nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal, emis de Avocatul Poporului.

Accesul utilizatorilor la interfaţa de colectare a datelor la nivelul sistemului central trebuie să se efectueze securizat, prin autentificare cu utilizator şi parola. Trebuie sa se implementeze politici

de securitate a parolelor, cum ar fi modul de schimbare a acestora, tipul de caractere necesare în crearea unei parole, etc.

Trebuie inclusă o componentă de management a parolelor pentru accesul administrativ la echipamentele și aplicațiile informatice din cadrul proiectului astfel încât să se reducă la minim riscurile la atacurile informatice de tip brute force și social engineering.

Soluția trebuie să ofere cel puțin următoarele funcționalități:

- Cheie master de instalare AES minim 256 biți;
- Cheie pentru baza de date stocată de către soluția ofertata;
- Să securizeze procesul de autentificare;
- Să securizeze transmisiile de date între server și soluția ofertată;
- Să securizeze datele stocate în soluția ofertată prin criptare AES minim 256 biți;
- Să securizeze procesul de acces la date prin alocarea de drepturi de acces utilizatorilor în funcție de permisiunile acordate în procesul de configurare.

Soluția trebuie să fie compatibilă cu standardul FIPS 140 level 2.

Soluția trebuie să faciliteze:

- Implementarea sigură a politicilor privind managementul parolelor;
- Monitorizarea și jurnalizarea tentativelor de autentificare eșuate;
- Închiderea sesiunilor utilizatorilor inactivi;
- Definirea unor perioade de timp configurabile pentru expirarea parolelor;
- Trimiterea de notificări automate;
- Criptarea dual a parolelor stocate;
- Accesul off-line cu ajutorul unei aplicații mobile;
- Logarea automată configurabilă în sistemele controlate;
- Integrarea cu aplicațiile de tip director.

Soluția trebuie să fie licențiată pentru minim 5 utilizatori de tip administrator, să nu fie limitată la numărul de utilizatori obișnuiți, iar licența trebuie să fie de tip perpetuu.

Canalele de comunicaţii utilizate pentru transfer trebuie sa fie securizate.

5. DESCRIEREA TEHNICĂ A PROIECTULUI

5.1.Cerinţele funcţionale ale sistemului

SIMISC constă intr-un pachet de funcţionalităţi integrate pentru gestiunea serviciilor prestate de Ministerul Afacerilor Externe din România prin reprezentanțele sale. Acestea pot fi la

rândul lor structurate în funcţie de disponibilitatea în zonele cu acces public în funcţionalităţi front-office şi funcţionalităţi back-office. Funcţionalităţile front-office trebuie sa asigure comportamentul sistemului în afară instituţiei, respectiv în relaţia cu petenţii, cetăţenii români care solicita servicii. Funcţionalităţile back-office trebuie sa asigure fluxurile, procesele şi conţinutul intern necesare efectuării serviciilor solicitate, acestea fiind accesibile doar personalului autorizat.

De asemenea, gruparea funcţionalităţilor în acest mod confirmă nivelul ridicat de interacţiune al cetăţenilor cu sistemul SIMISC. În continuare sunt prezentate funcţionalităţile generice ale sistemului, din perspectiva disponibilităţii pentru public, respectiv zona front-office şi zona back-office.

5.1.1. Funcţionalităţi front-office

Funcţionalităţile front-office trebuie sa includă serviciul de informare prin care cetăţenii trebuie să aibă acces la informaţii referitoare la legislaţie, serviciile disponibile la reprezentanţele MAE, precum şi serviciul de înregistrare dosare de solicitare pentru unul sau mai multe servicii. Funcţionalităţile necesare trebuie să includă cel puțin următoarele:

5.1.1.1. *Solicitare serviciu online*

Orice cetăţean care accesează portalul extern trebuie sa se poata informa asupra condiţiilor în care poate beneficia de serviciile reprezentaţelor MAE. Trebuie sa fie afişate sub forma descriptiv-informativă în zona de prezentare a portalului extern. După informarea prealabilă, cetăţeanul poate decide să apeleze la acele servicii de interes în varianta online. Un cetăţean trebuie să poată apela la mai multe servicii prin depunerea unui singur dosar de documente online. Fluxul de lucru pentru ca un cetăţean să beneficieze de serviciile online trebuie sa includa menţionarea serviciilor, specificarea reprezentanţei MAE căreia acesta se adresează, introducerea unor date de identificare ale persoanei, împreună cu identificarea unică a dosarului de documente al acesteia şi completarea formularelor specifice serviciilor utilizate. Înainte de transmiterea datelor completate în dosarul online, cetăţeanul trebuie sa aibă posibilitatea să îşi facă o programare online în una din zilele disponibile în funcţie de selecţia serviciilor făcută. În funcţie de încărcarea funcţionarilor, trebuie sa se efectueze verificarea dosarului. În momentul în care dosarul este corect şi complet, datele trebuie sa fie preluate în portalul intern unde se va soluţiona dosarul completat online.

Soluţionarea trebuie sa se realizeze în portalul intern al sistemului de către funcţionarii responsabili de serviciul respectiv. Înainte de soluţionarea propriu zisa a serviciului, petentul trebuie să plătească taxele aferente serviciului (stabilite de funcţionar în conformitate cu legile în vigoare), fie la ghişeu, fie prin plată electronică online. Serviciul, odată plătit, trebuie sa se înregistreze în registrele specifice şi pentru acesta se vor tipări toate formularele care necesită semnătura petentului.

5.1.1.2. *Solicitare serviciu Cetăţenie*

Serviciile de cetăţenie disponibile în portalul extern trebuie sa includă următoarele:

- Solicitarea redobândirii cetăţeniei române conform art. 10 din legea cetăţeniei nr. 21/1991 cu modificările ulterioare;

- Solicitarea redobândirii cetăţeniei române conform art. 11 din legea cetățeniei nr. 21/1991 cu modificările ulterioare;
- Solicitarea renunţării la cetăţenia română;
- Solicitarea clarificării statutului juridic (verificarea statutului cetăţeniei unei persoane, nu neapărat a celei care solicită serviciul).
- Solicitarea depunerii jurământului de credință față de România
- Solicitarea, în portalul extern, a serviciului de eliberare a dovezii de cetățenie română;
- Interfațarea cu MJ-ANC pentru transmiterea de date de la MD/OC către ANC și invers;
- Transmiterea de date, în portalul intern, de la ANC la MD/OC – ordine, rectificări, repunere în termen, completare dosar, verificarea stadiului dosarului.

Suplimentar, trebuie sa existe si o serie de informaţii cu privire la acordarea cetăţeniei române.

Activităţile efectuate de către funcţionar pentru soluționare trebuie sa se desfăşoare atât prin intermediul sistemului informatic, cât şi în afara acestuia. Toţi ceilalţi actori din cadrul fluxului aferent soluţionării serviciilor de cetăţenie (Petent, ANC) trebuie să poată realiza activităţile în afara sistemului informatic al MAE.

Pentru a preîntâmpina cazurile în care un cetățean solicită același serviciu de cetățenie la mai multe reprezentanțe MAE, vor fi gestionate persoanele ale căror dosare sunt respinse la ghișeu din motive obiective (lipsă documente, documente expirate, dosare depuse anterior sau suspiciune de fals). Astfel, la preluarea unei solicitări pentru un serviciu de cetățenie, se va verifica faptul că petentul nu a mai solicitat același serviciu, anterior, la o altă reprezentanță MAE.

De asemenea, se vor gestiona persoanele pentru care s-a procedat la încetarea efectelor Ordinelor ANC de redobândire a cetățeniei române (temei legal - depășire termen legal/necunoașterea lb. române) cu acces direct de la orice reprezentanță MAE. Sistemul va oferi și alerte referitoare la adăugarea de noi persoane, în cazul în care acestea solicită depunerea jurământului de credință în alt stat (după incetarea efectelor Ordinelor ANC).

5.1.1.3. *Solicitare Documente de identitate și de călătorie*

Serviciile disponibile trebuie sa includa:

- Identificarea unui cetăţean (verificarea identităţii);
- Eliberarea unui document de călătorie.

Documentele de călătorie care trebuie să poată fi eliberate includ:

- Paşaport simplu;
- Paşaport simplu cu domiciliu în străinătate;
- Paşaport temporar;
- Paşaport de serviciu;
- Paşaport diplomatic;
- Titlu de călătorie.

Pentru paşapoartele temporare emise sistemul trebuie să permită generarea de e-mail-uri de notificare asupra valabilității actului care trebuie să poată a fi trimise automat la apropierea datei de expirare.

Pentru a solicita un serviciu din această categorie, petentul trebuie să poată completa în portalul extern cererea de serviciu doar dacă nu s-a completat deja o altfel de cerere în cadrul dosarului (pentru cazul în care sunt solicitate mai multe servicii în cadrul aceluiaşi dosar).

Serviciul de eliberare a documentelor de călătorie trebuie sa se soluţioneze prin intermediul sistemului ePass. Sistemul E-Pass permite vizualizarea stării serviciului, aceasta trebuie să poată fi preluată și publicată atât in portalul intern cât și în portalul extern. Suplimentar, pentru serviciul de identificare, funcţionarii trebuie să poată avea acces la o bază de date pusă la dispoziţie de DEPABD, pentru a face interogările necesare.

5.1.1.4. *Solicitare serviciu - Acte stare civilă*

Actele care fac obiectul acestui serviciu includ:

- Înregistrare acte de naștere/căsătorie/deces;
- Înscriere în registrele de stare civilă romîne a certificatelor de naștere/căsătorie/deces eliberate de către autoritățile străine;
- Înscriere de mențiuni privind modificările intervenite în străinătate în statutul civil (divorț, schimbare de nume etc);
- Procurare din România de certificate/extrase de naștere/căsătorie/deces în locul celor pierdute/anulate/deteriorate;
- Declarație de celibat (declarație pe propria răspundere);
- Procurare din România a unei adeverințe privind statutul civil al cetățeanului român;
- Certificat de cutumă;
- Atribuire Cod Numeric Personal (CNP).

Documentele administrative emise de autorităţile străine prezentate pentru înregistrare în registrele de stare civilă române, precum şi traducerile acestora, care sunt făcute la un notar public din străinătate, trebuie să îndeplinească următoarele condiţii:

- Documentele eliberate de instituţii ale statelor semnatare ale Convenţiei de la Haga din 5 octombrie 1961 se apostilează;
- Documentele eliberate de statele cu care România a încheiat tratate/convenţii/acorduri de asistenţă judiciară sunt scutite de supralegalizare, apostilare sau orice altă formalitate;
- Documentele care nu se regăsesc în una dintre situaţiile prevăzute mai sus trebuie sa se supralegalizeze.
- Extrasele multilingve eliberate în baza Convenţiei 16 de la Viena sunt scutite de legalizare şi traducere în limba română

5.1.1.5. *Solicitare serviciu Acte notariale*

Prin intermediul acestui serviciu vor fi gestionate actele notariale. Acestea pot fi dupa cum urmează:

- Servicii standard, la care vor fi puse la dispoziție anumite modele și/sau tipizate de acte notariale, ce includ, fără a se limita:
  - Autentificarea procurilor;
  - Legalizarea copiilor de pe înscrisuri;
  - Legalizarea traducerilor;
  - Legalizarea semnăturilor și sigiliilor care urmează să producă efecte juridice în România;
  - Eliberarea unei copii sau a unui extras de pe actele aflate în arhivele misiunilor diplomatice sau oficiilor consulare;
  - Efectuarea unei traduceri din sau în limba română;
  - Testamente (serviciu diponibil numai prin prezentarea solicitantului la ghișeul misiunilor diplomatice sau oficiilor consulare);
  - Alte servicii notariale: certificarea unor fapte constatate personal de funcționarul consular, certificarea modificărilor survenite în rolul de echipaj al navelor, inclusiv schimbarea comandantului de navă, prelungirea valabilității actelor de convenție a navelor, înregistrarea și vizarea protestului pe mare, jurnalului de bord și a jurnalului de mașini, eliberarea permisului provizoriu de naționalitate, pentru navele construite în străinătate, achiziționate sau cărora li se schimbă clasa etc
- Servicii nestandard – unde vor putea fi procesate si documente/acte notariale care nu au un anumit model/tipizat. Acestea vor putea fi încărcate in sistem in format editabil, după ce în prealabil au fost completate de solicitant / eventual verificate de către funcționarul consular / cu informațiile dorite de solicitant.

Unele tipuri de acte notariale trebuie transmise, fără intarziere, în format electronic criptat și semnat, catre UNNPR pentru a fi înregistrate în registrele naționale notariale administrate

de UNNPR prin intermediul CNARNN- Infonot. Această procedura va presupune interconectarea sistemului cu portalul CNARNN.

5.1.1.6. *Solicitare serviciu Obținerea de acte din România*

Prin acest serviciu petentul trebuie să poată solicita:

- Eliberarea unui cazier judiciar – pentru pestarea acestui serviciu va fi necesară interfațarea cu sistemul informatic specific gestionat de Inspectoratul General al Poliției Romîne – direcția Cazier Judiciar, Statistică și Evidență Operativă;
- Atribuirea de Cod Numeric Personal
- Înscriere menţiuni privind modificarea statutului civil (divorţ, schimbare de nume, rectificări)
- Eliberarea unui duplicat al unui act de stare civilă emis în România sau pentru un act de stare civilă înscris / transcris în registrele româneşti.
- Eliberare dovezi privind statutul civil

5.1.1.7. *Solicitare serviciu - Alte servicii*

În cadrul acestui serviciu petentul trebuie să poată alege unul dintre următoarele servicii:

- Paşaport mortuar;
- Verificarea autenticităţii permisului de conducere;
- Atestat de domiciliu;
- Intermedierea apostilării / supralegalizării;
- Identificarea de persoane pe teritoriul României;
- Inregistrarea cetățenilor români aflați în străinătate;
- Alte servicii conform specificului statului de reședință (diverse adeverințe etc).

5.1.1.8. *Registre*

La nivelul reprezentanțelor MAE trebuie să existe două registre.

Registru de Corespondenţă - Acesta trebuie sa fie informatizat şi trebuie sa cuprinda toate intrările şi ieşirile de corespondenţă din instituţie referitoare la serviciile oferite. Personalul de secretariat din cadrul serviciului, precum şi funcţionarii trebuie sa aibă acces direct la acest registru online. Numerele din Registrul de Corespondenţă trebuie sa se aloce automat de sistem, acestea trebuie sa fie unice la nivel de reprezentanță, iar la începutul fiecărui an numerotarea trebuie să se reseteze şi să înceapă de la 1.

Registrul Unic Consular (registru ce va conține serviciile consulare prestate) - Acesta trebuie sa fie informatizat şi trebuie sa cuprinda toate inregistrările referitoare la serviciile prestate. Va conține fără a se limita minim următoarele funcții:

- Inregistrare, evidență și actualizare informații referitoare la cererea de servicii;
- Evidența datelor financiare (taxe defalcate și totale, sume încasate și chitanțe) pentru fiecare serviciu prestat;
- Salvarea și arhivarea electronică a informațiilor cuprinse in Registrul Unic Consular

Personalul consular trebuie sa aibă acces direct la acest registru prin intermediul aplicației interne. Numerele din Registrul Unic Consular trebuie să se aloce automat de sistem, acestea trebuie să fie unice la nivel de reprezentanță, iar la începutul fiecărui an numerotarea trebuie să se reseteze şi să înceapa de la 1.

5.1.2. Funcţionalităţi back-office

Funcţionalităţile back-office trebuie să fie accesate prin intermediul secţiunii private a portalului extern (zona accesată de funcţionari) şi prin intermediul portalului intern şi sunt caracteristice modulelor şi platformelor incluse în cadrul nivelului de logică de business.

În această categorie de funcţionalităţi intră:

5.1.2.1. *Managementul serviciilor oferite*

Managementul serviciilor trebuie să permită implicarea utilizatorilor Administrator central şi Administrator local în procesul de definire şi modificare a serviciilor prestate la nivel de reprezentanță MAE. În funcţie de rolul fiecărui utilizator, aceasta trebuie să poată defini serviciile prestate în cadrul unei reprezentanțe, trebuie să poată modifica sau seta durata medie de lucru a dosarului pentru fiecare serviciu în parte.

Pentru ca serviciile oferite cetățenilor români să fie complete, in cadrul zonei de back-office sistemul va gestiona următoarele funcții suport pentru serviciile consulare, după cum urmează:

- **Gestiunea cetățenilor români domiciliați sau rezidenți în străinătate**, in conformitate cu prevederile art. 5, lit.d din Legea nr. 248/2005

- **Gestiunea cetățenilor români arestați în afara României**. Astfel, vor fi stocate cel puțin următoarele informații despre cetățenii români arestați: nume si prenume, data şi locul naşterii, prenumele părinţilor, Cod Numeric Personal, motivul arestării/reţinerii/încarcerării, ţara unde este arestat/reţinut/încarcerat cetăţeanul român, cuantumul pedepsei cu datele de începere și de încheiere a execuției, dacă cetăteanul român a solicitat/nu a solicitat transferul în România și care este stadiul acestei solicitări, observaţii. În cazul în care cetațeanul român reținut/încarcerat/arestat este transferat în altă țară, fie ea România sau alt stat, marcarea acestei acțiuni se va efectua și la nivelul aplicației, astfel încât situația globală a arestaților să fie una actualizată. Parte a informațiilor despre cetățenii români privați de libertate este transmisă către alte autoritățile interesate din România – Ministerul Justiției și Centrul de Cooperare Polițienească Internațională. Modalitatea prin care aceste informații se vor transmite va fi detaliată în cadrul etapei de analiză a proiectului.

- **Gestiunea cetățenilor români decedați în afara României**. Astfel, vor fi stocate cel puțin următoarele informații despre cetățenii români decedați: nume și prenume, data şi locul naşterii, data şi locul decesului, prenumele părinţilor, Cod Numeric Personal, cauza decesului, ţara în care s-a produs decesul, ultimul domiciliu al defunctului, posibilitatea înhumării/incinerării pe plan local. Parte a informațiilor despre cetățenii români decedați în afara României este transmisă către alte autoritățile interesate din țară – Direcția Generală Pașapoarte. Modalitatea prin care aceste informații se transmit va fi detaliată în cadrul etapei de analiză a proiectului.

- **Gestiunea evidenței minorilor neînsoțiți de cetățeni români, supuși unor măsuri speciale de protecție (minori repatriați, minori tutelați de autorități locale etc);**

- **Gestiunea manualului de proceduri consulare** în cadrul unei secţiuni de e-Learning

- **Gestiunea răspunsurilor misiunilor diplomatice și oficiilor consulare ale MAE** pentru solicitările venite din Centrala MAE

- **Gestiunea documentelor transmise prin curier diplomatic** între reprezentanţele MAE şi Centrala MAE. Astfel, vor fi furnizate informaţii referitoare la documentele ce urmează a fi transmise prin primul curier disponibil. Încărcarea în portalul intern, la fiecare MD/OC, și cu posibilitatea de accesare din Centrala MAE a adreselor de transmitere (inclusiv a tabelelor aferente) a curierului diplomatic privind: filele consulare, registre de stare civilă, certificate constatatoare, acte de identitate, permise de conducere, documentelor transmise în Centrală pentru a fi apostilate, precum și corespondența interna MAE. Acest modul este necesar pentru a avea o imagine de ansamblu a volumului de curier transmis în Centrala MAE și a permite o identificare simplă și eficientă a unui anumit document/persoană/act după cuvinte cheie.

- **Gestiunea survolurilor, tranzit terestru şi naval.** Vor fi gestionate toate solicitările ce se primesc pe o anumită adresă de e-mail. Pentru fiecare solicitare nouă se va genera şi câte o alertă în cadrul sistemului. Totodată, vor fi gestionate legislaţia specifică (Conventia de la Montreux 1936, Conventia de la Chicago 1944, HG 912/210), formularele de survol si/sau tranzit specifice fiecărui stat în conformitate cu legislaţia internă, termenele de inaintare a cererile de tranzit si/sau survol pentru fiecare stat precum şi condiţiile de survol pentru delegaţii oficiale la nivel de șef de stat şi guvern, condiţii specifice fiecărui stat. Se va crea interfațarea cu autoritățile cu care MAE colaborează în acest domeniu.

5.1.2.2. *Configurare program de lucru la reprezentanță*

Administratorul local trebuie să poată stabili la nivelul portalului parametrii în funcţie de care cetăţeanul se poate programa. Aceşti parametri trebuie să includa: numărul de funcţionari, ziua în care lucrează, serviciul pe care lucrează, intervalul orar în care lucrează şi durata medie a serviciului setată per reprezentanță.

În cadrul programărilor, zilele cu program diferă pe reprezentanțe şi trebuie sa permită configurarea de excepţii în cadrul acestora (de exemplu, zilele de sărbătoare, zilele de repaos), conform legislaţiei locale.

Sistemul trebuie să permită introducerea anulărilor, caz în care se vor trimite e-mail-uri de notificare automat către petenți.

Centrala MAE trebuie să aibă acces la programările misiunilor, inclusiv drept de anulare/reprogramare a cererilor și, în acest sens, de notificare prin email a petenților.

5.1.2.3. *Raportări*

Administratorul local sau administratorul general trebuie sa aibă posibilitatea să genereze din aplicație diferite rapoarte prestabilite, în funcție de serviciu, reprezentanță și perioada dorită.

5.1.2.4. *Gestiune tipizate*

Administratorul local trebuie să țină în sistem evidența tipizatelor alocate reprezentanței. Tipizatele folosite pentru soluționarea serviciilor trebuie să poată fi anulate în anumite situații, de deteriorare fizică sau de erori materiale.

5.1.2.5. *Gestiune parametri aplicație*

Valorile parametrilor configurați la nivel de sistem trebuie să poată fi modificate de către Administratorul central, dar numai auditabil.

5.1.2.6. *Gestiune reprezentanțe*

Oricând se deschide sau se închide o reprezentanță, aceasta trebuie să poată fi adaugată în sistem de către administratorul central, dar numai auditabil.

5.1.2.7. *Gestiune angajați*

Procesul de gestiune al angajaților trebuie sa includa alocarea de roluri aferente funcțiilor pe care aceștia le îndeplinesc în cadrul reprezentanței. Trebuie să se păstreze un istoric cu fiecare angajat și rolurile pe care acesta le-a avut.

5.1.2.8. *Gestiune nomenclatoare suport*

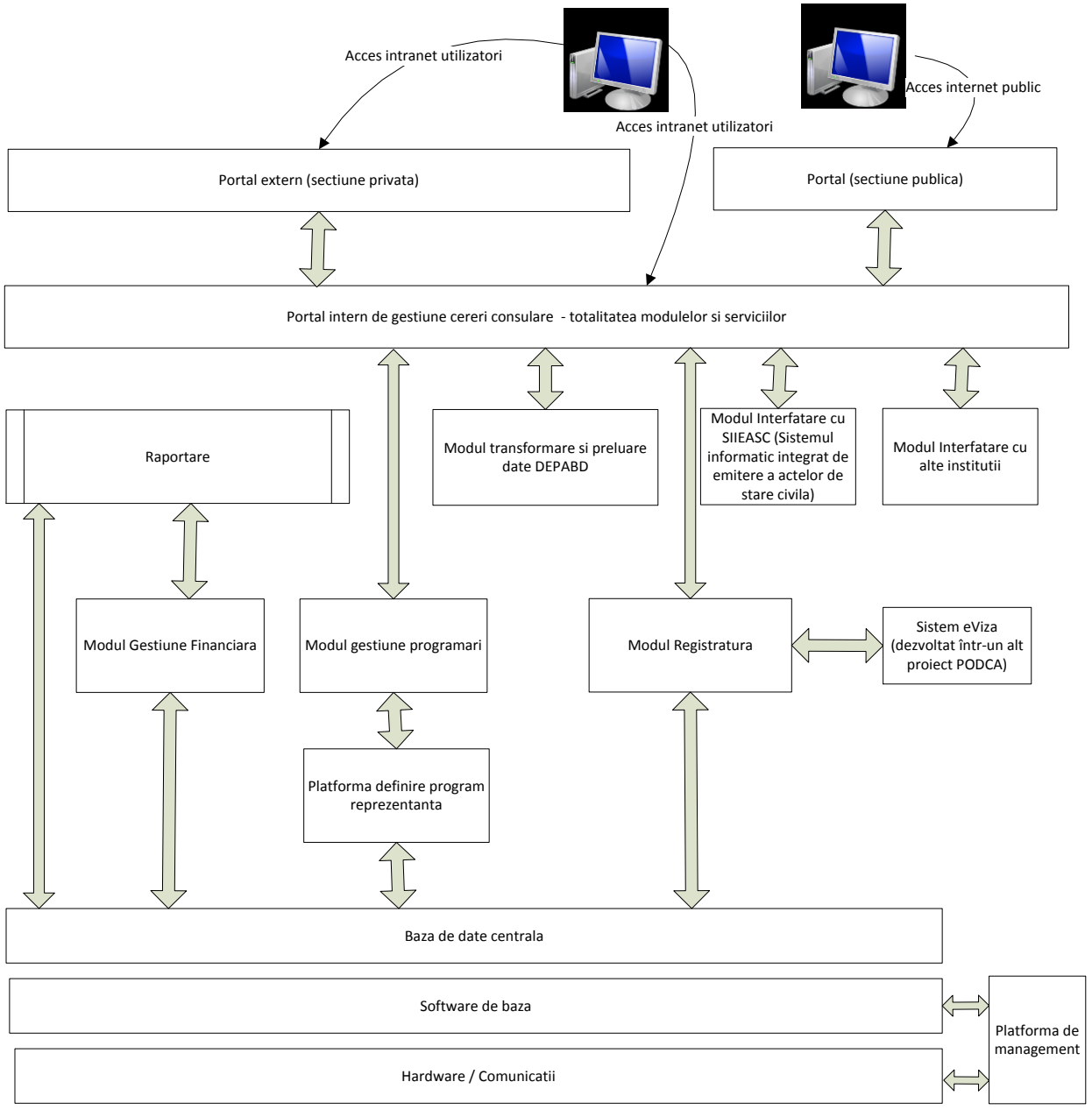
Procesul de gestiune al nomenclatoarelor suport trebuie să permită modificarea de către administratorul aplicației a informațiilor prezente în nomenclatoare prin inserare, ștergere sau modificare de date. Nomenclatoarele nu trebuie să poată fi șterse atâta timp cât există legături către ele în aplicație.

5.2.Arhitectura funcţională a sistemului

Arhitectura propusă trebuie sa fie multi-nivel, web-based, astfel incat toate funcţionalităţile sistemului să poată fi accesate prin intermediul unui portal specializat, cu o secţiune privată, respectiv o secţiune publică.

Accesul la sistem trebuie sa fie posibil utilizând un browser web standard, atât de către utilizatorii autorizaţi ai Ministerului Afacerilor Externe (prin intranet/internet), cât şi de către publicul larg (prin internet).

Arhitectura functionala a sistemului solicitat este prezentata in imaginea de mai jos.



Arhitectura funcțională generală

5.2.1. Portal extern cu secţiune privată şi secţiune publică

Secţiunea publică trebuie sa fie deschisă publicului larg şi trebuie sa faciliteze accesul catre următoarele servicii:

- Serviciul de informare, prin care cetăţenii trebuie sa aibă acces la informaţii referitoare la legislaţie, serviciile disponibile la reprezentanțele MAE, informaţii de interes general;

- Serviciul de înregistrare dosare de solicitare a unuia sau mai multor servicii, cu prezentarea stării pe flux a acestora. Acţiuni care trebuie sa fie disponibile:

    - Inregistrare dosar, cu alegerea serviciilor dorite şi încărcare de documente ataşate la serviciile solicitate;

    - Continuarea unei sesiuni de înregistrare dosar, dacă aceasta a fost întreruptă;

    - Trimiterea dosarului spre validare reprezentanței MAE;

    - Vizualizarea răspunsului din partea reprezentanței MAE în ceea ce priveşte validarea dosarului şi completarea dosarului dacă este cazul;

    - Alegerea datei şi orei dorite pentru programare, dintre cele disponibile;

    - Transmiterea dosarului către portalul intern;

    - Vizualizarea stării în care se găseşte fiecare dintre serviciile din dosar;

    - Înregistrarea in baza de date privind cetatenia română.

Secţiunea privată trebuie sa fie disponibilă exclusiv utilizatorilor autorizaţi din partea MAE şi sa ofere acces la funcţionalităţile dedicate solicitate şi anume:

- Vizualizarea şi consultarea dosarelor adresate reprezentanței MAE pe care o reprezintă utilizatorul autorizat;

- Validarea/invalidarea dosarelor adresate reprezentanței MAE pe care o reprezintă utilizatorul autorizat.

Portalul extern trebuie sa prezinte un certificat digital calificat (trebuie să poată fi evidențiat în certificat organizația beneficiară) care sa ateste autenticitatea portalului fata de utilizatorii externi ai portalului si față de alți consumatori de servicii.

5.2.2. Portal intern de gestiune cereri servicii

Aceasta componentă trebuie sa asigure funcţionalităţile de back-end pentru cererile de servicii recepţionate prin intermediul secţiunii publice a portalului extern. Suplimentar, aceasta componentă trebuie sa asigure şi introducerea datelor specifice cererilor de servicii, de către personalul instituției, pentru cazul în care cetăţenii se prezintă la reprezentanța MAE fără a fi completat anterior un dosar în portalul extern.

Soluţionarea unui serviciu trebuie sa se realizeze în portalul intern al sistemului de către personalul instituției responsabil de serviciul respectiv. În momentul prezentării la ghişeu a

petentului, responsabilul fie va căuta dosarul completat online în portalul extern şi preluat ulterior în portalul intern, fie va introduce pe loc datele serviciului solicitat în portalul intern.

Înainte de soluţionarea propriu zisa a serviciului, petentul trebuie să plătească taxele aferente serviciului (stabilite de personalul instituției în conformitate cu legile în vigoare), pentru care trebuie sa primeasca o dovadă tipărită (chitanţa).

Serviciul, odată plătit, trebuie sa fie înregistrat în registrele specifice şi pentru acesta trebuie să se tiparească toate formularele ce necesită semnătura petentului. Data formularelor trebuie sa fie data tipăririi acestora.

După ce au fost urmaţi paşii de mai sus, serviciul trebuie sa fie dat în lucru, iar petentul să aşteapte soluţionarea acestuia.

La completarea unei rezoluţii pentru un serviciu în cadrul portalului intern, petentul ce l-a solicitat trebuie sa fie notificat cu privire la faptul că a fost pusă o rezoluţie. Aceasta rezoluţie trebuie să poată fi consultată de către petent în portalul extern, în contextul dosarului de aplicare pentru serviciu.

La nivelul portalului intern trebuie sa fie disponibile următoarele funcţionalităţi, fără nicio limitare:

- Sistem de securitate bine definit şi structurat, care garantează accesul la datele confidenţiale doar utilizatorilor care au setate drepturile respective;
- Înregistrarea, evidența şi actualizarea informaţiilor referitoare la cererea de servicii introdusă de către funcționar (înregistrare, soluţionare, plată servicii);
- Posibilitatea de tipărire a documentelor/formulare rezultate în urma anumitor intervenţii ale personalului, de exemplu: eliberare chitanţă;
- Notificare pe email către petent referitoare la stadiul cererii depuse în vederea vizualizării dosarului sau în portalul extern.

5.2.3. Modul de raportare

Prin implementarea acestui modul, administratorul local sau administratorul general trebuie sa aibă posibilitatea să genereze din aplicaţie diferite rapoarte prestabilite, în funcţie de serviciu, reprezentanță şi perioada dorită.

Modulul trebuie să poată fi folosit pentru o vizualizare rapidă şi facilă a informaţiilor statistice şi sintetice, structurate şi grupate după criterii şi caracteristici predefinite într-o bibliotecă de rapoarte sau configurabile de către utilizator.

Capabilităţi generale necesare ale componentei de raportare:

- Conectarea la surse de date de diferite tipuri;
- Lucrul cu baza de date în timp real;

- Agregarea şi diseminarea datelor;
- Mod de lucru simplu şi uşor de înţeles;
- Modelarea informaţiilor în structuri multidimensionale;
- Căutare rapidă a informaţiilor;

Capabilităţi tehnice şi funcţionale necesare ale componentei de Raportare:

- Uşurinţă în utilizare, de la definirea structurilor On-Line Analytical Processing (OLAP) la modalităţile de utilizare şi prezentare a datelor şi informaţiilor colectate în sistem;
- Sistem de securitate bine definit şi structurat, care garantează accesul la datele confidenţiale doar utilizatorilor care au setate drepturile respective (prin intermediul LDAP);
- Administrarea facilă a sistemului de raportare;
- Diseminarea informaţiilor trebuie efectuată după mai multe criterii:
    - Grupare după criterii stabilite de către aplicaţie sau utilizator;
    - Distribuirea informaţiilor către utilizatori după reguli de vizualizare definite în administrare;
- Structurile OLAP folosite trebuie să poată fi:
    - Editate de către utilizatorii autorizaţi;
    - Accesate prin servicii web;
    - Expuse pe web prin pagini HTML, unde utilizatorul poate manipula dimensiunile după necesităţile analizei;
- Existenţa istoricului pe rapoarte;
- Executarea rapoartelor la orice oră, în funcţie de necesităţile utilizatorilor;
- Export în HTML, XML, XLS, PDF;
- Accesarea rapoartelor prin interfeţe web;
- Trebuie sa asigure posibilitatea de a combina informaţiile structurate cu cele nestructurate;
- Trebuie ca toate aceste date să poată fi mapate pe o harta interactivă a lumii, astfel incât la selectarea unei misiuni să poată fi afișate volumul și starea serviciilor din acea locație.

5.2.4. Modul de gestiune financiară

Acest modul trebuie să permită centralizarea activităţii şi datelor financiare aferente serviciilor consulare prestate pentru cetăţenii români, la nivelul fiecărei reprezentanțe: taxele

încasate – defalcate și totale, emiterea de chitanţe, diverse statistici financiare, gestiunea financiară a tipizatelor etc. De asemenea, pentru fiecare serviciu prestat în parte trebuie să se reţină date cu privire la plată, în numerar sau prin alte forme.

În cazul chitanţierului, acesta se va emite în mod automat, pentru fiecare reprezentanţă MAE, pentru operaţiunile de încasări în numerar. Modelul chitanțierului va fi furnizat de către MAE, în cadrul etapei de analiză.

Trebuie sa fie permise următoarele funcţionalităţi:

- Modificarea şi completarea descrierii serviciilor, precum şi valoarea taxelor per serviciu (defalcat și total), în euro, conform legii, de către utilizatorii autorizaţi;
- La toate misiunile care operează cu alte valute decât euro, trebuie să fie inserat în aplicație, lunar (ultima zi a fiecărei luni calendaristice) și ori de câte ori apare o variație de +/- 10% față de cursul anterior calculat, cursul mediu de schimb dintre valuta națională a țării în care funcționează reprezentanța MAE și euro;
- Calcularea automată a taxelor aferente serviciilor predefinite, defalcat și total, listarea tuturor serviciilor și a texelor acestora în portalul intern și extern;
- Corelarea în aplicație, a listei de servicii și a valorii taxelor aferente cu celelalte module ale aplicatiei;
- Arhivarea listei tuturor serviciilor și a costurilor acestora, procesate în sistem.

5.2.5. Modul de registratură

Prin implementarea acestui modul se doreşte înlocuirea registrelor fizice existente la reprezentanțe cu unele electronice.

Se vor crea două registre:

- Registrul unic consular
- Registrul de corespondență consulară

Acest modul trebuie să permită centralizarea rezultatelor activităţii de înregistrare serviciu la nivel de reprezentanță MAE, prin înregistrarea, evidentă şi actualizarea informaţiilor fiecărui tip de serviciu solicitat de către petent, într-un Registru unic al serviciilor consulare. De asemenea, trebuie efectuata si centralizarea electronică a Registrului Secretariatului în care sunt păstrate toate intrările şi ieşirile din cadrul MD/OC, pe problematică consulară, inclusiv cele care nu ţin de serviciile oferite, de exemplu scrisorile către alte instituţii, etc.

Trebuie sa fie disponibile următoarele funcţionalităţi, fără limitare:

- Înregistrarea, evidentă şi actualizarea informaţiilor referitoare la cererea de servicii;
- Evidența datelor financiare (taxe defalcate și totale, sume, chitanţe) pentru fiecare serviciu prestat;

- Posibilitatea de accesare a acestor registre electronice prin servicii web;
- Distribuirea informaţiilor către utilizator după reguli de vizualizare definite în administrare sau selectate anterior de către acesta;
- Salvarea și arhivarea electronică a informaţiilor cuprinse în Registrele serviciilor consulare, în diferite formate accesibile utilizatorilor din cadrul reprezentanțelor MAE.

5.2.6. Modul de gestiune programări

Personalul reprezentanțelor care derulează activităţi trebuie sa aibă posibilitatea, în funcţie de reprezentanța la care îşi desfăşoară activitatea, să îşi stabilească programul de lucru apriori, iar petentul să se poată programa, în portalul extern, în intervalul orar definit la nivel de reprezentanță. În vederea definirii programului apriori la nivelul reprezentanței, modulul trebuie sa conţina o platformă de definire program.

Programul de lucru al reprezentanțelor, precum şi fluiditatea traficului petenţilor la ghişeu, diferă de la caz la caz. Astfel există reprezentanțe care preiau cereri pentru toate serviciile în orice zi a săptămânii, altele care preiau într-o zi cereri pentru anumite servicii, iar în altă zi cereri pentru alte tipuri de servicii. De asemenea, programul de lucru poate varia, existând zile în care nu se preiau deloc cereri de servicii sau se preiau într-un interval orar redus.

În cadrul acestui modul utilizatorii trebuie sa aibă acces la următoarele informaţii/funcţionalităţi, fără limitare:

- Setarea la nivelul sistemului a parametrilor în funcţie de care petentul se poate programa, de exemplu: numărul de funcţionari, ziua în care lucrează, serviciul pe care lucrează, intervalul orar în care lucrează;
- Definirea zilelor cu program diferit la nivel de reprezentanță şi setarea excepţiilor în cadrul acestora (de exemplu zilele de sărbătoare etc);
- Posibilitatea de vizualizare a programărilor făcute la nivel de serviciu, precum şi la nivel de utilizator pe o anumită perioadă;
- Posibilitatea petentului de a primi o notificare pe email, în cazul în care programul setat inițial la nivel de MD/OC se modifică;
- Posibilitatea aplicației de a propune petentului cele mai apropiate sloturi de programare libere, în jurul datei alese de acesta, în cazul în care în acel interval de timp, inițial ales, nu era disponibil niciun slot.

5.2.7. Modul transformare şi preluare date DEPABD (Direcţia pentru Evidenţa Persoanelor şi Administrarea Bazelor de Date)

Prin acest modul se doreşte ca în momentul prezentării petentului la ghişeu, utilizatorul să poată verifica în timp real identitatea fiecărui cetăţean român solicitant de servicii. Dat fiind faptul că în acest moment verificarea cărţilor de identitare se poate realiza în România doar la Direcţia Consulară, se doreşte extinderea acestui tip de verificare/validare şi la reprezentanțele MAE.

Interogarea bazelor de date de la DEPABD trebuie sa se efectueze cu ajutorul unui serviciu web pus la dispoziţie de noul sistem DEPADB şi interogat de sistemul eGuvernare. Pentru a putea fi implementate aceste verificări de identitate direct de la reprezentanțe, trebuie sa se creeze mai întâi cadrul legal în baza căruia se va defini protocolul între MAE şi DEPABD, acest cadru legal nu intră în responsabilitatea ofertanților. Ofertantul declarat câștigător va primi toate informațiile necesare în etapa de analiză necesară impelementării sistemului informatic solicitat.

5.2.8. Modul interfaţare cu SIIEASC (Sistemul informatic integrat de emitere a actelor de stare civilă)

Prin acest modul, în vederea facilitării corespondenței dintre Sistemul informatic integrat de emitere a actelor de stare civilă şi SIMISC, trebuie efectuată implementarea următoarelor fluxuri de schimb de date:

- SIMISC -> SIIEASC: Transmiterea online din primul şi al doilea exemplar din registrul de stare civilă, în paralel cu transmiterea în format hârtie a acestora, conform art.41 alin (2) din Legea 119/1996 cu privire la actele de stare civilă;
- SIMISC -> SIIEASC: Transmiterea de cereri pentru procurarea de acte de stare civilă din România;
- SIMISC -> SIIEASC: Transmiterea de cereri de coduri numerice personale precalculate, în vederea înscrierii lor în actele de naştere întocmite şi în certificatele eliberate în baza acestora;
- SIIEASC -> SIMISC: Transmiterea listei de coduri numerice precalculate, la nivel de reprezentanță MAE.

Pentru a putea fi implementate aceste operațiuni direct de la reprezentanțe, trebuie să se creeze mai întâi cadrul legal în baza căruia se va defini protocolul între MAE şi SIIEASC, acest cadru legal neintrând în responsabilitatea ofertanților. Ofertantul declarat caştigator va primi toate informațiile necesare în etapa de analiză, necesare impelementarii sistemului informatic solicitat.

5.2.9. Modul de interfaţare cu alte instituţii/entităţi cu care MAE desfăşoară activităţi

Prin aceste module se va realiza interfațarea sistemului SIMISC cu Uniunea Națională a Notarilor Publici din România, Ministerul Justiției, Inspectoratul General al Poliției Române, Centrul de Cooperare Polițienească Internațională etc. Prin aceste interfațări, sistemele vor comunica în mod automat si transparent pentru utilizatori, realizând schimbul de date, conform fluxurilor de lucru.

5.2.10. Modulul de derulare plăţi electronice online

Sistemul trebuie să includă o componentă Front-End de derulare a plăților în mediu electronic, care trebuie să permită achitarea facilă prin mijloce de plată online a diferitelor taxe necesare.

Componenta Front-end trebuie sa fie integrată cu autoritatea de certificare şi va prezenta utilizatorilor un certificat digital calificat pentru autentificarea către utilizator. Certificatul digital va fi

folosit şi la realizarea conexiunilor SSL/HTTPS între platformă şi utilizatori pentru a minimiza riscul atacurilor de tip "man în the middle". Componenta Front-End trebuie sa nu permita accesul utilizatorilor prin protocolul nesecurizat HTTP în procesul de autentificare al acestora şi nici după autentificarea utilizatorilor până în momentul deautentificarii cu scopul părăsirii platformei de către utilizatorul autentificat, sau al expirării sesiunii.

5.2.11. Integrarea componentelor

Modularitatea sistemului integrat SIMISC trebuie să ofere autonomia funcţională a sistemelor componente, însă comunicarea între acestea asigura realizarea completă şi eficientă a proceselor modelate la nivelul portalului, precum gestionarea cererilor de servicii, gestionarea programărilor sau gestionarea financiară. Comunicarea sistemelor trebuie sa fie posibilă prin integrarea componentelor care susţin activităţile acestora. La nivelul SIMISC, integrarea componentelor în sistem se va face respectând standardele în domeniu, după cum urmează:

- XML pentru transferul de date inter-aplicaţii;
- SOAP/WSDL pentru apelul de proceduri inter-aplicaţii;

Sistemul trebuie sa fie unul de tip modular, el trebuie sa funcţioneze ca un tot unitar.

În ceea ce priveşte interfaţarea sistemului SIMISC, au fost identificate următoarele sisteme/instituţii cu care acesta se va interfaţa, fără a ne limita la acestea, după cum urmează:

- DEPABD (Directia pentru Evidenta Persoanelor si Administrarea Bazelor de Date)
- UNNPR (Uniunea Naionala a Notarilor Publici din Romania)
- SIIEASC (Sistemul Informatic Integrat de Emitere a Actelor de Stare Civilă)
- ANC (Autoritatea Naţională pentru Cetăţenie)
- IGPR (Poliţia Română - Direcţia Cazier Judiciar, Statistică şi Evidenţe Operative)
- DRPCIV (Directia Regim Permise de Conducere și Înamtriculare a Vehiculelor)
- MJ (Ministerul Justiţiei - Direcţia Drept Internaţional şi Cooperare Judiciară)
- CCPI (Centrul de Cooperare Poliţienească Internaţională)
- REN-FEC (Registrul Electronic Naţional pentru Fişele de Evidenţă Centrală a Persoanelor)

Autentificarea în sistem trebuie sa se efectueze printr-un mecanism de tip „Single Sign-On”, permiţând accesul utilizatorului în toate modulele pentru care dispune de drepturile necesare după introducerea numelui de utilizator şi a parolei o singură dată în cadrul unei sesiuni de lucru.

5.3. Arhitectura tehnică

5.3.1. Parametrii tehnici

Pentru asigurarea unui cadru optim de implementare a sistemului integrat SIMISC arhitectura şi parametrii tehnici trebuie să respecte următoarele cerinţe generale:

- Trebuie asigurată dotarea cu servere şi echipamente pentru Data Centere care să satisfacă complet necesităţile de prelucrare a datelor, conform specificaţiilor din secţiunea „Descrierea infrastructurii necesare";
- Tehnologia web implementată trebuie să implice resurse minime din partea staţiilor de lucru, astfel încât să permită personalului și petenților să lucreze şi pe calculatoare mai puţin performante;
- Trebuie asigurată unicitatea informaţiilor (fără informaţii redundante, dublate, incomplete);
- Sistemul trebuie sa dispună de manuale de operare a tuturor aplicaţiilor software şi a dispozitivelor hardware.
- Sistemul trebuie sa fie conform sau sa implementeze standarde din domeniu astfel:
  - XML pentru transferul de date inter-aplicaţii;
  - XSL pentru transformarea datelor dintr-o structură în alta;
  - SOAP/WSDL pentru apelul de proceduri inter-aplicaţii;
  - SQL pentru interogarea bazelor de date;
  - LDAP pentru acces la soluţia directory.
- **Disponibilitate** - Disponibilitatea datelor trebuie să fie asigurată prin salvari zilnice; lucrul în cadrul sistemului trebuie să fie tranzacţional/ multiuser/ concurent. Sistemul trebuie să fie modular şi să nu condiţioneze funcţionarea unui subsistem de funcţionarea celorlalte subsisteme.
- **Scalabilitate şi redundanţă** – sistemul trebuie să dispună de facilitaţi de redundanţa si recuperare în urma unui dezastru pentru a proteja beneficiarul de eventuale defecţiuni care pot surveni în timpul funcţionării.
- **Standardizare** - subsistemele şi platforma hardware trebuie să fie astfel proiectate pentru a respecta standardele de aplicaţie în domeniu - 3 niveluri: baze de date, server de aplicaţii şi interfaţa utilizator. Dispunerea componentelor aplicaţiilor pe echipamente trebuie efectuată în conformitate cu specificul fiecărei componente: cele de bază de date pe serverul de bază de date, cele de aplicaţii pe serverele de aplicaţii, iar cele de interfaţa grafică pe calculatoarele operatorilor. Serverele pot fi fizice sau virtuale in funcție de Soluția aleasă de ofertanți.

- **Interfaţa utilizator** - Aplicaţiile sistemului informatic trebuie să folosească limba română pentru toate meniurile, ecranele, rapoartele de aplicaţie accesibile utilizatorului final. De asemenea, documentaţia şi materialele de instruire pentru utilizatorii finali trebuie sa fie livrate în limba română. Aplicaţiile trebuie sa asigure calitatea datelor introduse prin proceduri de validare (prin definirea câmpurilor obligatorii, a formatului acceptat pentru anumite câmpuri, a unor valori sau plaje de valori posibile pentru anumite câmpuri etc.) precum şi prin verificarea şi atenţionarea utilizatorilor asupra incompatibilităţilor sau contradicţiilor dintre înregistrări. Sistemul trebuie să nu permită existenţa datelor dublate, să sesizeze datele inconsistente, datele lipsă sau deteriorate. Se va permite navigarea facilă în şir între toate modulele şi accesarea tuturor funcţiilor şi comenzilor la care utilizatorul are acordate drepturi în cadrul aceleiaşi sesiuni de lucru;

- **Scalabilitate şi flexibilitate:** Scalabilitate şi flexibilitate în distribuirea sistemului, care să permită extinderea sau modificarea structurii organizatorice a utilizatorilor. Sistemul trebuie să prezinte un grad mare de parametrizare care să permită modificări rapide şi facile în cadrul aplicaţiei. Sistemul trebuie să fie complet configurabil şi capabil să facă faţa necesităţilor unui număr crescând de utilizatori.

- **Extensibilitate şi integrare:** Sistemul oferit trebuie să permită integrarea cu funcţionalităţi de semnare electronică şi de verificare a semnăturilor documentelor gestionate de aplicaţii; Sistemul trebuie să permită extinderea cu alte funcţionalităţi dorite de către instituţie, pentru aceasta fiind disponibile interfeţe de programare (API) publice şi bazate pe standarde deschise (SOA, WEB-Services, XML); Toate interfeţele între module sau cu module externe trebuie să fie realizate folosind protocoale în conformitate cu standardele descrise mai sus sau cu alte standarde neproprietare. Totodată, sistemul trebuie să poată acomoda eventuale modificări legislative cu impact în procedurile consulare pe toata perioada pana la acceptanță finală a proiectului.

5.3.2. Descrierea infrastructurii necesare

Pentru implementarea sistemului informatic trebuie sa se folosească o arhitectură centralizată, cu înaltă disponibilitate și redundanță în două locații ale beneficiarului, cu serviciile prezentate pe web.

Sistemul Informatic centralizat, cu înaltă disponibilitate și redundanță în două locații ale beneficiarului se caracterizează prin faptul că întregul proces de prelucrare și stocare a datelor precum și dezvoltarea sistemului se realizează la nivelul celor doua locatii ale MAE, unde se află poziționate infrastructurile hardware pe care ruleaza bazele de date ale sistemului precum și ansamblul aplicațiilor.

Conexiunea cu utilizatorii și reprezentanțele MAE trebuie sa se efectueze prin intermediul legăturilor de comunicații securizate.

Avantajele centralizării trebuie sa fie reprezentate de:

- Control asupra dezvoltării și utilizării software-ului;

- Control asupra integrității și securității datelor;
- Partajarea resurselor hard și soft între utilizatori;
- Facilitarea aplicării schimbărilor la nivelul ansamblului;
- Eliminarea riscului incompatibilităților hardware și software între utilizatori;
- Promovarea cu uşurinţă a standardelor (tehnice, de proiectare, procedurale, etc.) la nivelul întregului sistem;
- Asigurarea unui numar însemnat de solicitări ale beneficiarilor datorită puterii de calcul sporite la nivelul întregului sistem;
- Inregistrarea on-line a tranzacțiilor în baza de date centrală din toate locațiile distribuite geografic, cu reflectare la nivel central.

Din punct de vedere logic, SIMISC trebuie sa aibă o arhitectură client – server dispusă pe trei niveluri:

- Nivelul interfața client (web);
- Nivelul de implementare a logicii de business;
- Nivelul de accesare și stocare a datelor;

Pentru a beneficia la maxim de avantajele arhitecturii centralizate, sistemul informatic trebuie implementat cu ajutorul unei infrastructuri hardware dezvoltate pe baza aceloraşi principii de flexibilitate şi eficienţa maximă. Aceste principii aplicate pentru platformă hardware înseamnă o nouă viziune asupra resurselor necesare care nu mai sunt dedicate unui anumit proces în parte, ci sunt mai degrabă sunt puse la dispoziţie în mod global. Îndeplinirea acestui deziderat se face prin împărţirea resurselor pe categorii, respectiv resurse de procesare, resurse de stocare şi resurse de interconectare. Pentru implementarea fiecărei categorii trebuie să se folosească tehnologii de ultimă generaţie care să aibă următoarele caracteristici comune: platformă tehnologică deschisă, suport pentru virtualizare şi management unitar.

Resursele de procesare trebuie să fie implementate în tehnologie x86 cu ajutorul unor echipamente de tip blade. Implementarea trebuie efectuată pe o platformă bazată pe standarde deschise. Astfel procesoarele folosite trebuie să fie în arhitectura x86/x64, iar sistemele de operare trebuie sa fie de tip Microsoft Windows, Linux sau echivalent.

Toate resursele de stocare trebuie sa fie concentrate într-un sistem de stocare centralizată accesibil într-o reţea de tip SAN, redundant, instalat în cele două locații ale MAE. Următoarele caracteristici vor asigura flexibilitatea şi eficientă necesară:

- Toate serverele trebuie sa fie conectate la un sistem de stocare centralizată;
- Sistemul de stocare trebuie să permită acces simultan la nivel de fişier în reţele Ethernet precum şi la nivel de bloc în reţele Ethernet (iSCSI) şi Fibre Channel; In

configuratia ofertata, sistemul de stocare trebuie să includă licențe pentru cel puțin funcționalitatea de acces la nivel de bloc în retele Ethernet (iSCSI) și Fibre Channel;

- Sistemul de stocare trebuie să suporte minim următoarele protocoale SAN: Fibre Channel Protocol (fabric-attached and direct-attached) şi iSCSI;
- Sistemul de stocare trebuie să suporte minim următoarele protocoale de reţea: NFS, CIFS.

Interconectarea acestor resurse precum şi a utilizatorilor trebuie sa se efectueze prin tehnologii LAN/SAN bazate pe mecanisme de virtualizare, ca principal motor a flexibilităţii în utilizare.

Prezenţa virtualizării în toate categoriile de resurse asigura mecanismele necesare pentru alocarea simplă și eficientă a resurselor către diferitele procese. Aceste mecanisme trebuie sa fie completate de sistemul de management unitar.

Pentru a asigura un nivel maxim de disponibilitate a serviciilor IT arhitectura hardware trebuie să fie de tip „no single point of failure”. În acest sens:

- Sistemele trebuie să includă soluții de High Availability si Disaster Recovery;
- Sistemul de stocare trebuie să suporte cel puţin un tip de matrice RAID care să permită continuarea operaţiunilor de scriere şi citire în eventualitarea defectării simultane a oricăror două hard-discuri;
- Sistemul de stocare trebuie să permită replicări sincrone şi asincrone a volumelor de date pentru implementare de Disaster Recovery;

Prin respectarea arhitecturii și parametrilor tehnici propuși, soluţia tehnică trebuie să răspundă în totalitate scopului și obiectivelor proiectului, asigurând în același timp scalabilitatea necesară, atât software cât și hardware, cât și flexibilitate în utilizare, condiții de bază ale unei infrastructuri IT cu adevărat eficiente.

5.3.3. Componente de infrastructură

Componentele de infrastructură principale și care nu trebuie să lipsească din sistemul informatic sunt descrise în subcapitolele următoare:

5.3.3.1. *Portal*

Portalul trebuie sa prezinte următoarele caracteristici:

- Interfaţă web standardizată, simplă şi intuitivă;
- Interfaţă cu utilizatorii bogată în funcţionalităţi, care să ofere un nivel ridicat de accesibilitate

- Grad ridicat de securitate a sistemului, care să garanteze confidenţialitatea şi securitatea datelor utilizatorilor pentru accesul neautorizat atât dinafara cât şi din interiorul sistemului;
- Servicii şi extensii ale portalului, de tip modular, care să permită dezvoltarea ulterioară de noi funcţionalităţi;
- Arhitectură orientată pe servicii, astfel încât toate serviciile implementate pentru gestionarea conţinutului în portal (publicare, căutare, versionare, etc.), să poată fi reutilizate şi incluse în alte aplicaţii;
- Administrarea şi dezvoltarea portalului trebuie sa se poata realiza facil, utilizând doar un browser web;
- Trebuie să ofere acces către toate resursele prezente în cadrul portalului printr-o singură autentificare, la deschiderea sesiunii.

Portalul trebuie sa fie construit pornind de la nevoile utilizatorului final, interfaţa sa oferind funcţionalităţi intuitive, dinamice şi rapide care conduc la o performanţă remarcabilă. De asemenea arhitectura trebuie sa fie bazată pe tehnologii deschise şi facilităţile de integrare deja prezente, care permit o extensibilitate facilă a sistemului, indiferent de modalitatea aleasă pentru acest lucru. Astfel, vor putea fi folosite toate serverele de aplicaţii majore, baze de date, sisteme de operare, limbaje de programare diverse.

Soluția de portal folosită trebuie sa ofere următoarele funcţionalităţi:

- Managementul conţinutului web – platforma trebuie să ofere toate uneltele şi funcţionalităţile necesare pentru managementul conţinutului web şi să permită crearea de pagini web personalizate: editor de text WYSIWYG, separarea conţinutului de layout, conţinut reutilizabil, CSS, şabloane pentru crearea paginilor web, generare dinamică de taxonomii web, site map, Search Engine Optimization (SEO), motor de căutare, etc;
- Facilităţi de colaborare - componenta de colaborare trebuie să ofere uneltele necesare pentru a sprijini interacţiunea utilizatorilor: forum de discuţii, calendar, anunţuri şi alerte, RSS, etc.

Soluţia trebuie să fie astfel construită încât să ofere suport pentru instalarea de servere multiple pe o singură maşină fizică. În fapt trebuie să suporte clusterizare multi-nivel pentru orice combinaţie de niveluri posibilă (prezentare, serviciu, logică de business şi bază de date) prin implementarea celor mai noi tehnologii în domeniu:

- Advanced Caching;
- Page Caching;
- Load Balancing;
- Session Replication;

- Distributed Cache;
- Static Content Export.

Soluţia trebuie să fie dezvoltată folosind o strategie de tip SOA şi să ofere suport pentru standardul WSRP 1.0 şi 2.0 care permite o integrare uşoară a portleţilor remote, aplicaţiilor şi conţinutului.

Soluţia trebuie să ofere posibilitatea de import al conţinutului de la diferite alte surse de date (alte aplicaţii similare, sisteme de fişiere, baze de date, pagini web, servicii web, etc.)

Soluţia trebuie să ofere funcţionalităţi de conţinut personalizat şi facilităţi de personalizare avansate funcţie de context.

Soluţia trebuie să fie complet web-based astfel încât absolut toate operaţiunile, inclusiv administrarea şi definirea layout-ului şi a resurselor Portal să se facă din browser-ul web.

Soluţia trebuie să fie construită în întregime pe o infrastructură de securitate care să ofere mecanisme de control al accesului granularizat la nivel de utilizator, grup şi rol şi care să garanteze confidenţialitatea, autenticitatea şi integritatea informaţiilor din portal.

Soluţia trebuie să permită un singur punct de acces la toate modulele.

Arhitectura soluţiei trebuie să permită o scalabilitate sporită, performanţă sporită, înaltă disponibilitate şi simplitate pentru deservirea unui număr mare de utilizatori.

Soluţia trebuie să ofere suport pentru instalarea pe diverse servere de aplicaţii, trebuie să ofere suport toate serverele de aplicaţii majore din piaţă, cu capabilităţi de clustering, balansare şi failover.

Soluţia trebuie să permite funcţionalitatea dynamic virtual hosting care permite ca după setarea unui site web, intranet sau portal, pe aceeaşi maşină fizică să se poată seta şi alte site-uri sau portal-uri, fiecare cu propria adresă URL unică, şi cu alte funcţionalităţi şi interfaţe cu utilizatorul.

Soluţia trebuie să ofere un mecanism de tip asistent (wizard) pentru crearea automată a site-urilor pe bază de şabloane.

Soluţia trebuie să suporte funcţionalitatea de drag and drop dinamic, permiţând utilizatorilor să adauge module şi funcţionalităţi în paginile portalului fără a fi necesară scrierea de cod sau reproiectarea modulelor existente.

Soluția ofertată trebuie să permită accesul unui număr nelimitat de utilizatori externi, iar licența sa fie dimensionată pentru toată puterea de procesare a mașinii fizice gazdă.

Având în vedere natura regională a proiectelor, soluția de tip portal trebuie să ofere și o componentă de transpunere a datelor în mod grafic din orice format în orice format și din orice sursă în orice destinație. Aceasta componentă va avea două module, unul ce se va putea instala pe stațiile administratorilor sistemului și unul de tip server pentru execuția și stocarea șabloanelor de integrare.

Soluția trebuie să suporte minim următoarele tipuri de date/protocoale/limbaje de programare/standarde:

- XML;
- Baze de date precum SQL Server, DB2, Oracle, Sybase, MySQL, PostgreSQL, Access;
- Fișiere simple (CSV, tab-separated, fixed width, etc.);
- EDI;
- Excel (OOXML);
- XBRL;
- Web Service;
- Java, C#, C++;
- integrare cu Visual Studio si Eclipse IDE.

Subcomponenta tip „desktop”

Cerințe specifice privind modelarea integrării datelor:

- Modelarea trebuie să se facă în mod grafic;
- Trebuie să suporte exportul modelelor direct din interfața grafică către modulul de tip server;
- Asocierile dintre sursele și destinațiile datelor trebuie să se realizeze usor și intuitiv oferind functionalități de tip "drag and drop";
- Soluția trebuie să dispună de o librărie de sabloane cu filtre și funcții ce pot fi aplicate pentru procesarea datelor;
- Soluția trebuie să dispună de un constructor vizual de funcții pentru a putea combina mai multe operațiuni;
- Soluția trebuie să suporte integrări de date din fișiere multiple simultan cu posibilitatea de a selecta sursele sau destinațiile în mod dinamic la rulare;
- Soluția trebuie să permită reutilizarea modelelor de integrare pentru orice fel de continut;
- Soluția trebuie să genereze codul de integrare in timpul sesiunii de lucru și să îl poată afișa la cerere;
- Soluția trebuie să permită manipularea datelor preluate prin aplicarea de filtre, inserare de funcții, constante sau alti operatori astfel încât datele să fie utilizabile de sistemul destinație;

- Soluția trebuie să permită transformări complexe de date în care datele de ieșire dintr-o integrare sau transpunere să devină date de intrare pentru alt proces;
- Soluția trebuie să poată sorta datele de intrare sau de ieșire după caz;
- Soluția trebuie să permită maparea grafica a datelor în format XML;
- Soluția trebuie să permită transformarea de date XML;
- Soluția trebuie să permită crearea de mapări complexe XML în care datele de ieșire ale unei mapări devin date de intrare pentru alte mapări;
- Soluția trebuie să permită crearea de mapări pe baza unor surse de date provenite din baze de date;
- Soluția trebuie să permită crearea de mapări din baza de date către date XML;
- Soluția trebuie să permită construirea de servicii web pornind de la surse de date;
- Soluția trebuie să permită conectarea la servicii web bazate pe WSDL 1.1 sau 2.0 și integrarea funcționalităților direct in mapările XML destinație;
- Soluția trebuie să permită generarea automată de cod într-un limbaj de tip enterprise pentru crearea de mapări ;
- Soluția trebuie să permită folosirea de semnaturi digitale XML.

Subcomponenta de tip server

Modulul de tip server va fi componenta principala de orchestrare și automatizare a proceselor de integrare. Acest modul este motorul de execuție al modelelor generate de modulul de tip desktop și trebuie să poată rula independent de serverul de aplicații sau portal.

Modulul server trebuie să ofere minim următoarele funcționalități:

- Trebuie să ofere o interfață grafică Web pentru administrare și monitorizare a tranzacțiilor;
- Trebuie să suporte configurare programabilă folosind “triggeri” pentru rularea job-urilor;
- Trebuie să suporte configurarea mai multor triggeri pentru același job;
- Trebuie să permită rularea mai multor triggeri simultan;
- Trebuie să permită funcții de tip “precaching” al datelor pentru tranzacțiile consumatoare de resurse sau timp;
- Trebuie să ofere posibiliatea generării de log-uri pentru toate job-urile executate;
- Trebuie să permită configurarea unor containere pentru stocarea maparilor, profilelor și datelor stocate pentru fiecare utilizator;

- Trebuie sa suporte configurații de tip “multi-tenant” într-o singură instanță pentru a permite folosirea de mai multe departamente sau utilizatori a soluției;
- Trebuie să permită configurarea de alerte e-mail pentru toți pașii de execuție;
- Trebuie să permită rularea fluxurilor din interfața grafică sau direct din consola (CLI);
- Trebuie sa ofere capabilități de preprocesare ale mapărilor de date pentru optimizarea vitezei de execuție dar și a utilizării memoriei serverului;
- Trebuie să permită importul de fișiere generate de administratori în modulul desktop;
- Sisteme de operare suportate: Windows, Linux, MacOS X.

5.3.3.2. *Baza de date*

Pentru bazele de date este necesară o soluţie robustă şi scalabilă, capabilă să asigure disponibilitatea sistemului. Sistemul de baze de date trebuie să îndeplinească următoarele obiective:

- Schimb uşor de date, fiabilitate şi robusteţe;
- Acces la date prin protocoale standardizate (ODBC, XML, SOAP);
- Facilități de tip ”ETL – Extract-Transform-Load”;
- Facilităţi de depozit date (partiționabil), analiză a datelor, data mining (OLAP);
- Facilități de tip “business intelligence” în cadrul aceleiasi aplicații;
- Administrare şi dezvoltare simplificată.

Funcţionalităţile generale pe care trebuie să le îndeplinească sistemul de baze de date, sunt:

- Suport pentru transferul datelor din baza de date din şi în alte baze de date prin protocoale standard (ODBC, XML, TXT) pentru a putea permite integrarea la nivel de date a altor sisteme externe.
- Funcţionalităţi de administrare grafică a sistemului de gestiune a bazelor de date
- Suport pentru mecanisme de control şi blocare la nivel de tabelă, fără escaladare, pentru a permite accesul concurent şi manipularea datelor;
- Suport pentru suspendarea operaţiilor consumatoare de resurse;
- Facilităţi pentru gestionarea automată a memoriei (self-tuning);
- Suport pentru rularea mai multor instante de server de baze de date pe acelaşi echipament;
- Suport pentru servere cu mai multe procesoare;

- Suport pentru interogare în format XML;
- Suport pentru stocare date în format XML şi comunicare cu aplicaţii în format XML;
- Funcţionalităţi de tip Data Mining;
- Funcţionalităţi de tip OLAP;
- Suport de servicii de transformare a datelor pentru a putea permite importuri din surse de date neomogene;
- Suport pentru limbaje de tip SQL;
- Mecanism de securitate bazat pe utilizatori şi roluri, integrat în sistemul LDAP;
- Facilităţi pentru diagnosticarea problemelor: urmărirea execuţiei, expertiză, analiza, prognoza;
- Facilităţi pentru monitorizarea tranzacţiilor;
- Facilităţi pentru monitorizarea, configurarea şi optimizarea performanţelor;
- Suport pentru replicarea datelor;
- Facilităţi de partiţionare a tabelelor pentru a asigura suport pentru baze de date foarte mari;
- Facilităţi de indexare în paralel a datelor şi suport pentru indecşi multipli pentru obiectele stocate;
- Facilităţi pentru view-uri indexabile pentru a mări viteza de acces a interogărilor on-line;
- Suport pentru „database mirroring”;
- Suport pentru funcţionare în regim clustering;
- Suport pentru indexare on-line;
- Facilităţi de administrare a aplicaţiei din programe cu interfaţa grafică prietenoasă fără a fi nevoie de a utiliza scripturi de acces;
- Facilităţi de optimizare a bazei de date şi de tuning a arhitecturii;
- Suport nativ pentru acces la interogări prin servicii web;
- Suport pentru interogarea bazei de date în standardul xQuery 1.0;
- Facilităţi de rulare proceduri automate de back-up, arhivare, recuperare a unor versiuni mai vechi a bazei de date;

- Facilităţi pentru proceduri de administrare şi configurare, prin intermediul interfeţelor grafice;
- Facilităţi de operare a modificărilor în setul de date prin intermediul unor instante intermediare (transaction log);
- Facilităţi pentru anularea tranzacţiilor în ordine inversă (rollback);
- Facilităţi pentru asigurarea integrităţii datelor în timpul utilizării prin soluţii echivalente;
- Raportare “ad hoc”: utilizatorii să poată edita propriile rapoarte pe baza unui model (template), fară să deţină cunoştinţe de baze de date sau despre structura acestora. Serviciile de raportare să fie incluse în produs, fără add-on-uri suplimentare ;
- Interogare și analiza ad-hoc și self-service a datelor: facilități de interogare a datelor disparate în momentul solicitării rapoartelor ;
- Instrumente de dezvoltare a obiectelor din baza de date: Soluția trebuie să ofere unelte de dezvoltare pentru modulele ETL (Extract, Transform, Load), pentru design-ul bazelor de date atât relaționale cat și multidimensionale, pentru design-ul rapoartelor;
- Criptarea transparenta a datelor, a fişierelor de date şi a fişierelor jurnal fără să fie necesară modificarea aplicaţiei. Funcționalitățile de criptare sunt necesare pentru îndeplinirea cerinţelor şi respectarea reglementărilor generale cu privire la confidenţialitatea datelor. Criptarea trebuie să ofere inclusiv instrumente de căutare în datele criptate utilizând sisteme de regăsire într-un interval sau căutarea parţială, fără modificarea aplicaţiilor existente.

Soluția ofertată trebuie licențiată pentru întreaga capacitate de procesare a minim două (2) servere fizice în configurație activ/pasiv și să nu fie limitată la numărul de utilizatori. Soluția ofertată trebuie de asemenea să asigure suport nativ pentru sistemul de operare oferit în cadrul prezentului proiect.

5.3.3.3. *Sisteme de operare*

Această componentă trebuie sa asigura o baza solidă pentru toate celelalte module ale sistemului. Principalele funcționalități solicitate sunt:

- Asigurarea unui suport software robust și fiabil;
- Asigurarea unui suport de stocare a informațiilor robust și scalabil pentru a permite stocarea unui numar foarte mare de informații acumulate;
- Asigurarea unei arhitecturi deschise la integrarea cu alte instituții.

Sistemul de operare va trebui sa asigure cel puțin următoarele:

- Sa ofere suport pentru minim 2 socketuri procesor;

- Sa ofere suport pentru urmatoarele tipuri de procesoare:
  - x86;
  - x86-64;
- Sa ofere suport pentru tehnologia 64-bit;
- Sa ofere suport pentru urmatoarele tipuri de conectivitate cu echipamentele de stocare :
  - NAS;
  - SATA;
  - SAS;
  - SCS;
  - FC;
  - FcoE;
  - iSCSI.
- Să permită instalarea în configurații cluster tip “high-availability”;
- Să ofere suport pentru tehnologia de “virtualizare” ofertată;
- Să ofere o interfață unică pentru configurarea și monitorizarea serverului;
- Să ofere o componenta shell cu linie de comandă și limbaj de script;
- Să ofere instrumente de diagnosticare asupra mediului serverului, fizic și virtual;
- Să permită administrarea serverului de la locații de la distanță;
- Să permită instalari în configurație minimală;
- Să includă mecanisme de “backup” a datelor;
- Să includă funcționalități privind Sistemele de fișiere;
- Să includă funcționalități de Management al accesului;
- Să includă funcționalități de Tipărire;
- Să includă funcționalități de Stocare;
- Să includă funcționalități de Directory – Server de LDAP;
- Să includă funcționalități privind Rețele si comunicații;
- Să includă funcționalități privind Securitatea;
- Să includă funcționalități privind Administrare remote.

Se vor include licențe de sisteme de operare în număr suficient pentru licențierea corectă a arhitecturii propuse.

5.3.3.4. *Soluția de virtualizare*

Platforma de virtualizare trebuie să îndeplinească următoarele caracteristici:

- Hypervizorul trebuie să fie independent de producătorul echipamentelor pe care se instalează sau de metoda de stocare internă/externă disponibilă în platforma de procesare și/sau stocare pe care rulează;
- Trebuie să permită virtualizare de tip 1 (bare metal) – permite rularea direct pe gazda hardware pentru controlarea echipametului și pentru gestiunea sistemelor de operare gazdă;
- Platforma de virtualizare trebuie să ofere suport pentru utilizarea tuturor procesoarelor și nucleelor de procesare ale serverelor care se virtualizeaza conform arhitecturii;
- Platforma de virtualizare trebuie să permită adăugarea on-line de spațiu de stocare pentru mașinile virtuale;
- Platforma de virtualizare trebuie să ofere mecanisme on-line pentru adăugarea de resurse de procesare și memorie;
- Platforma de virtualizare trebuie să permită mutarea mașinilor virtuale de pe un server pe altul fără întreruperea funcţionării maşinii virtuale, de pe un server fizic pe altul;
- Platforma trebuie să includă o componentă de administrare și monitorizare;
- Componenta de management și monitorizare a infrastructurii trebuie să permită autentificarea utilizatorilor bazată pe roluri și privilegii distincte de utilizare;
- Platforma de management trebuie să asigure și mecanisme de definire și aplicare a profilelor standard de configurație pentru serverele ce fac parte din infrastructura virtuală;
- Platforma trebuie să integreze un portal de tip dashboard pentru afisarea si analizarea tuturor informatiilor legate de disponbilitate, grad de ocupare a resurselor, metrici de performanță, istoric al acțiunilor administrative și corective, precum și recomandări de optimizare a întregii funcționalități puse la dispoziție de platforma de virtualizare. Portalul trebuie să permită executarea directă de acțiuni corective și administrative asupra elementelor de infrastructură vizate (mașini virtuale, resurse de procesare, stocare și comunicație), acțiuni bazate pe recomandările afișate în portal în urma analizelor efectuate asupra respectivelor elemente;
- Datele monitorizate trebuiesc automat analizate și exprimate sub forma de metrici de stare, risc și eficiență, permițând identificarea rapidă a potențialelor probleme în infrastructură;

- Platforma trebuie sa ofere analize de capacitate și să identifice explicit resursele ce sunt supra-utilizate, ajutând în procesul de redistribuire a sarcinilor de încărcare între elementele platformei în scopul eficientizarii rulării aplicațiilor și serviciilor, respectiv să ofere scenarii predefinite de simulare a încărcării pentru a elimina procesele deductive de alocare a resurselor platformei;

- Platforma trebuie să ofere analize automate a proceselor de instalare și configurare a mediului virtualizat, în scopul detectării rapide a eventualelor probleme ce pot apărea datorită configurărilor defectuoase sau a elementelor noi introduse în infrastrcutură;

- Platforma trebuie să integreze funcții automate de alertare în cazul depășirii pragurilor optime de funcționare, atât pentru starea tuturor elementelor platformei de virtualizare, cât și pentru metrici de performanță și capacitate;

- Platforma de virtualizare trebuie să permită crearea de imagini ale stărilor curente ale mașinilor virtuale de tip "snapshots";

- Platforma de virtualizare trebuie să permită asigurarea unei disponibilităţi ridicate pentru toate maşinile virtuale, chiar şi în cazul defectării serverului fizic pe care acestea rulau, prin repornirea lor automată pe un alt server fizic disponibil, sau funcţionarea fără întrerupere a maşinilor virtuale critice chiar şi în cazul defectării serverului fizic pe care acestea rulau, prin rularea în paralel a acelor maşini virtuale pe 2 servere fizice şi comutarea instantanee pe cel de-al doilea server fizic în cazul defectării unuia dintre ele;

- Platforma de virtualizare trebuie sa ofere mecanisme integrate de balansare a încărcării resurselor fizice și virtuale disponibile în infrastructură și redistribuire a sarcinilor generate de utilizatori, servicii și aplicatii, prin integrarea nativă cu platformele hardware, indiferent de producatorul respectivelor elemente de infrastructură. Aceste mecanisme trebuie să fie disponibile atât la comandă prin intervenția unui operator cât și prin operațiuni automate definite în funcție de necesități, gradul de ocupare al resurselor și/sau pe baza unor reguli/politici prestabilite;

- Platforma de virtualizare trebuie sa ofere suport pentru urmatoarele sisteme de operare instalabile în mașină virtuală: Windows Xp/Vista/7/2003/2008/2008/2012 R2, Linux Suse/Red Hat/CentOS, FreeBSD, Solaris, Netware și să permită adaugarea de spațiu de stocare pentru mașinile virtuale prin folosirea următoarelor protocoale : NAS – NFS/CIFS ; SAN – iSCSI/FCP și prin folosirea următoarelor sisteme de fișiere : FAT32, NTFS, EXT2, EXT3, asigurând astfel compatibilitate cu majoritatea tehnologiilor implementate în mod uzual atât în platformele de procesare cât și în platformele de stocare;

- Platforma de virtualizare trebuie să permită configurarea spațiului de stocare virtual prin integrarea directă cu platforma de stocare aleasă prin intermediul unor conectori/componente native sau de la producătorul platformei de stocare, mecansim ce va permite extinderea discurilor virtuale fără a fi necesară oprirea

mașinilor virtuale ce au atașate aceste discuri. Deasemenea prin integrare directă cu platforma de stocare, trebuie să ofere mecanisme automate de monitorizare a încărcării I/O și de alocare/realocare dinamică a resurselor I/O către mașinile virtuale în funcție de cerintele acestora (ad-hoc sau conform unei politici prestabilite), realizând astfel o prioritizare inteligentă a accesului aplicațiilor la resursele de stocare.

- Platforma trebuie să permită identificarea și folosirea optimă a mecanismelor de asigurare a căilor redundante de acces în platformele de stocare și a mecanismelor terțe de protecție a datelor stocate, incluzând volumele adresate direct de platforma de virtualizare, respectiv volumele de date folosite de aplicații, servicii și utilizatori;

- Platforma trebuie să ofere integrare nativă cu platformele de stocare alese, trebuie să permită alocarea dinamică de spațiu către mașinile virtuale, chiar dacă acel spațiu nu este fizic disponibil în aceste platforme, permițând funcționarea corectă a aplicațiilor și serviciilor ce necesită resurse stricte de spatiu de stocare, respectiv creșterea transparentă a volumelor de date prin adăugarea de resurse fizice de stocare (discuri) doar în momentul când acestea devin necesare;

- Platforma trebuie să includă mecanisme proprii de catalogare și grupare a resurselor disponibile în platformele de stocare, indiferent de tipul, producătorul și numărul acestora (tipuri de discuri, latența, tipul volumelor și metoda de export aplicată asupra lor), permițând astfel crearea de profile de stocare și asocierea acestor profile cu distribuirea/redistribuirea mașinilor virtuale în funcție de cereri temporare ale aplicațiilor sau în baza unor politici predefinite.

- crearea și managementul planurilor de Disaster Recovery direct din interfața de management a mediului virtual (HyperV sau echivalent);

- permite arhitecturi diferite, în care protecția poate fi configurată bidirecțional sau în care se utilizează un site de comun pentru protejarea mai multor site-uri;

- suport pentru diferite metode de replicare, la nivel de host sau la nivel de storage, și descoperirea automată a mașinilor virtuale protejate prin cele două metode;

- poate integra diferite soluții de replicare sincronă sau asincronă, la nivel de storage: ISCSI, FibreChannel sau NAS, pe baza unor plugin-uri (storage replication adapters) oferite de producătorii soluțiilor de stocare;

- se integrează cu replicarea asincrona la nivel de host (vSphere Replication sau echivalent) asigurând protecția granulară, la nivel de mașina virtuală și recuperarea mai multor puncte în timp, cu un RPO (recovery point objective) cuprins între 15 minute și 24 ore;

- permite maparea resurselor din site-ul de disaster recovery la mașinile virtuale protejate;

- permite rularea de scripturi (out of guest sau in guest) pentru extinderea planurilor de Disaster Recovery;
- permite definirea de roluri pentru controlul accesului la planurile de Disaster Recovery;
- alertează automat operatorul în cazul în care legătura cu site-ul protejat a căzut, oferind totodată opțiunea de recuperare rapidă, pe baza planurilor prestabilite și testate, în site-ul de Disaster Recovery;
- asigură pornirea automata a mașinilor virtuale în caz de Disaster Recovery, permițând stabilirea ordinii de boot-are a acestora;
- asigură un mecanism simplu de reconfigurare a adreselor IP pentru recuperarea mașinilor virtuale în site-ul de Disaster Recovery;
- asigură managementul și monitorizarea planului de Disaster Recovery direct din interfața de management a mediului virtual, permițând oprirea temporara și intervenția manuală în caz de necesitate pentru rezolvarea eventualelor probleme apărute;
- asigură protejarea automata, în oglindă, a mașinilor virtuale protejate prin inversarea replicării către site-ul original protejat;
- asigură testarea automată a planului de disaster recovery în orice moment de timp și fara intreruperea funcționării sau protecției mașinilor virtuale protejate prin utilizarea de snapshot-uri la nivel de storage și recuperarea mașinilor virtuale într-un mediu de lucru izolat;
- asigură curățarea automata a site-ului de Disaster Recovery după efectuarea testelor (ex. oprirea mașinilor, ștergerea snapshot-urilor)
- rezultatele testelor sunt stocate și pot fi vizualizate sau exportate direct din interfața de management a mediului virtual;
- permite utilizarea planului de Disaster Recovery și pentru migrări planificate, în care mașinile virtuale protejate sunt oprite într-o stare consistentă a aplicațiilor la nivelul site-ul protejat, după care se face sincronizarea datelor cu site-ul de Disaster Recovery și refacerea pe baza planului de Disaster Recovery a mașinilor virtuale protejate;

Soluția de virtualizare trebuie sa fie licențiată pentru toată puterea de procesare solicitată în cadrul prezentului caiet de sarcini, inclusiv Soluția de management centralizat a mașinilor virtuale și distribuția acestora pe echipamentele fizice indiferent de locația unde se află acestea, iar pentru disaster recovery trebuie să fie licențiată pentru întreaga infrastructura solicitată în cadrul prezentului caiet de sarcini, dar nu mai puțin de 20 de mașini virtuale.

5.3.3.5. *Soluția de management*

Soluția de management va permite monitorizarea echipamentelor, aplicaţiilor şi a fluxului informaţional din cadrul acestora pe mai multe niveluri, pornind de la nivelul software până la componentele hardware care susţin sistemul. Soluția trebuie să faciliteze:

- Administrarea evenimentelor sistemelor de operare, printr-un jurnal de evenimente la nivel de întreprindere care colectează şi raportează problemele şi informaţiile generate referitoare la sistemele şi aplicaţiile din reţeaua companiei;
- Monitorizarea switch-urilor, routerelor şi altor dispozitive prin SNMP;
- Raportarea şi analiza tendinţelor necesare pentru urmărirea problemelor în timp şi generarea rapoartelor detaliate despre starea de funcţionare generală a mediului administrat;
- Monitorizarea aplicaţiilor distribuite pe mai multe servere;
- Soluția trebuie să dispună de un editor în mod grafic de componente ale unui serviciu;
- Permita monitorizarea şi raportarea evenimentelor, urmărirea nivelului de sănătate al sistemului;
- Permita identificarea fiecărui echipament din reţea printr-o icoană grafică;
- Aceste rapoarte trebuie să poată fi accesate local sau să poată fi publicate în site-urile Web pentru accesul facil la informaţiile de administrare ale sistemelor.
- Soluția trebuie să permită definirea de hărţi de monitorizare într-un editor grafic, cu posibilităţi de a crea prin operaţii de tip wizard şi drag-n-drop:
    - Harta echipamentelor în rack;
    - Harta aplicaţiilor pe echipamente;
    - Harta echipamentelor/aplicaţiilor în camerele unde sunt instalate;
    - Harta camerelor în cadrul clădirilor;
    - Harta clădirilor în cadrul oraşelor;
    - Harta tuturor elementelor monitorizate la nivel de ţara sau glob.
- Utilizatorul trebuie să poată naviga între hărţi astfel încât să comute de la un nivel de detaliere la altul, vizualizând oricând, în timp real, starea aplicaţiilor şi a echipamentelor monitorizate;
- În cadrul unui proces informaţional utilizatorul trebuie să poată să ajungă repede, din elementele de proces monitorizate până la poziţia în rack a echipamentului care a produs defecţiunea;
- Modulul trebuie să permită crearea de hărţi de proces, geografice, topologice sau de tip panou de bord pe care să se poziţioneze elementele monitorizate;
- Hărţile elementelor monitorizate trebuie să poată fi afişate în baza rolurilor utilizatorilor printr-un browser web;
- Să prezinte portleti specifici pentru cel puţin un portal (ex: Sharepoint, Websphere, WebLogic etc);
- Crearea de rapoarte de disponibilitate a aplicaţiilor pe baza interdependentelor între hărţi.

5.3.3.6. *Soluția de backup*

Soluția de backup dedicată şi redundantă pentru realizarea operațiunilor de backup, trebuie licențiață și configurată corespunzător instalării în cele două locații ale beneficiarului.

Suportul pentru stocarea seturilor de date de backup va fi asigurat in fiecare locatie de o bibliotecă de benzi automatizată echipata cu o unitate de bandă LTO-6 conectată in SAN si echipament destinat replicarii datelor salvate in regim deduplicat intre cele doua locatii geografic diferite. Fiecare bibliotecă de benzi:

- Trebuie să ofere minim o unitate de LTO-6 cu interfaţa FC şi minim 8 slot-uri pentru casete
- Trebuie să asigure o capacitate de transfer de cel puţin 500 / 1400 GB/ oră (nativ/comprimat)
- Trebuie să asigure o viteza de cel puţin 160/400 MB/s (scriere/citire)
- Trebuie livrată impreună cu minim 25 de casete de bandă LTO-6.

Soluția de backup trebuie sa asigure usurință în instalare și configurare prin utilizarea unor asistenți dedicați procesului (wizard).

De asemenea, utilizarea produsului trebuie sa se faca de catre administratorii MAE printr-o interfata grafica intuitiva. Pentru job-uri customizate, administratorul trebuie sa se poata interfata la CLI (command line interface).

Aplicația trebuie să suporte toate modelele de backup/restaurare (full, incremental, differential) precum si o functie de consolidare a backup-urilor incrementale.

Soluția trebuie să aibă o arhitectura modulara care sa asigure dezvoltarea acesteia in timp prin adaugarea unor noi componenete.

De asemenea, estimând o crestere abrupta a datelor pe care trebuie sa le protejam, Soluția trebuie să permită un grad inalt de scalabilitate.

Pentru a se putea alege o varianta adaptata cerintelor noastre Soluția va trebui sa ofere o flexibilitate crescuta in modelul de licentiere :

- licentiere volumetrica a datelor care vor fi protejate.

Cerinte functionale:

- Protectie centralizata intrun mediu heterogen, cu impact minimal asupra unui sistem aflat in productie.
- Soltuie de back-up complet integrata, ce include soft si echipament dedicat pentru back-up unificate sub acelasi producator.
- Interfata centralizata de administrare si raportare a soft-ului si echipamentului dedicat pentru back-up.
- Model simplificat de adoptare a unor capabilitati avansate prin integrarea cu tehnologie de ultima generatie pentru protectia infromatiei precum deduplicarea datelor, API-uri destinate mediului virtual si recuperarea server-ului la nivel fizic

- Protejarea si recuperarea mediilor virtuale precum VMware (VMware API pentru protectia datelor si VMware Change Block Tracking pentru back-up si recuperare) si Hyper-V pentru a oferi clinetilor valorificarea optima a mediului virtual.
- Arie extinsa de capabilitati backup-to-disk, inclusiv back-up SAN si NAS (NDMP) si integrarea nativa cu echipamentul dedicat pentru back-up.
- Backup la nivel de unitate de bloc pentru Servere Windows care utilizeaza Sisteme de Fisiere de densitate mare.
- Suport pentru deduplicarea optimizata la nivel de volume utilizate de Windows Server 2012 R2 pentru back-up-ul acestora in forma deduplicata optimizata.
- Fiecare agent de backup are capacitatea de a trimite datele direct catre destinatia de backup via conexiune IP sau conexiune FC eliminand astfel necesitatea de a trece infromatiile prin server-ul de back-up.
- Posibilitate de back-up fara Server dedicat, partajarea librariei, si partajarea dinamica a drive-urilor folosind casetele librariei.
- Suport pentru backup virtual full sintetic pe sistemul de backup destinatie fara necesitatea de a trimite save set-uri prin retea.
- Suport pentru save-stream-uri paralele pentru clineti Linux si Unix
- Suport pentru operatiuni de clonare setate sa porneasca dupa salvarea fiecarui save-set.
- Disaster Recovery Managent rapid si sigur.
- Abilitatea de a controla echipamentul de replicare din aceasi consola grafica si posibilitatea de a administra copiile Disaster Recovery.
- Echipamentul ofera deduplicarea datelor:
    - Pentru fisiere de orice dimensiune.
    - O zona singulara de deduplicare pentru toate datele stocate, independenta de tipul de date (Exchange, Oracle, fisiere etc.).
    - Segmente de dimensiuni variabile.
- Acces multi-protocol:
    - Minim 4 proturi Ethernet Gigabit
    - Suport pentru CIFS, NFS, OST,NDMP
    - Agregarea link-urilor, reduntata pentru link-urile Ethernet
    - Minim 2 porturi Fibre Channel pentru acomodatea Librarie Virtuale
    - Posibilitatea de utilizarea simultana a tututror protocoalelor in acelasi timp
- Caracteristici interne si integritatea datelor:
    - RAID 6
    - NVRAM pentru prevenirea pierderii datelor in cazul unui eveniment neprevazut precum pierderea alimentarii cu energie electrica.
    - Sistem de Fisiere cu auto-regenerare, verificarea activa si neintrerupta a datelor stocate
    - Capacitatea de snapshot la nivelul echipamentului
    - Suport pentru operatiuni de curatarea a sistemului de fisiere in cadrul ferestrei de backup
    - Capacitatea de implicare a puterii de procesare in procesul de curatare
    - Functionalitate de call-home direct catre producator pentru suport proactiv
- Disaster Recovery prin replicare:
    - Suport pentru replicare unu-la-unu si bidirectionala

  - Replicarea poate sa foloseasca datele deduplicate pentru a trimite numai unitati de bloc unice
  - Mecanismul de replicare permite reglarea si optimizarea latimii de banda
- Securitatea Datelor:
  - Criptarea datelor nefolosite este optionala
  - Criptarea stream-ului de replicare
  - Accesul utilizatorului pe baza de roluri atribuite
- Administrare si raportare
  - Consola grafica si CLI
  - Raportare in timp real a indicilor de performanta
  - Rapoarte privind capacitatea, tendinte si evenimete
  - Gestionarea cotelor - echipamentul poate alerta sau stopa sistemul de backup in cazul depasirii limitelor de spatiu impuse
- Echipamentul trebuie sa ofere capacitate totala de minim de 12TB, bazandu-se pe discuri SATA, protejate de RAID6.

Cerinte cu privire la datele care vor fi protejate si a mediilor de stocare:

- Soluția trebuie să asigure suport pentru volumul total al datelor ce trebuie protejate, care este de minim 12TB;
- Soluția trebuie să permită utilizarea librariilor de benzi si in acest scop se va prezenta o lista de compatibilitate, lista in care trebuie sa se regaseasca libraria de benzi ofertata.

Cerintele cu privire la SLA-uri:

- Soluția trebuie să aiba in vedere optimizarea si micsorarea ferestelor de backup prin tehnici specifice de automatizare, planificare si executie a task-urilor necesare. Soluția trebuie să asigure functii specifice de back-up pentru toate tipurile de informatii : date statice, date vitale si informatii critice.
- Soluția trebuie să genereze rapoarte cu privire la operaţiunile de salvare / restaurare;
- Furnizorul trebuie sa asigure suport printr-un partener local certificat de catre producator pentru a acorda suport 24x7.

Cerinte speciale:

- Soluția de backup trebuie sa dispuna de module specializate de backup/restaurare Bare Metal a serverelor oferite in cadrul solutiei.
- Soluția trebuie să permită replicarea pentru situatiile de tip disaster recovery la nivel de job.
- Soluția trebuie să asigure module dedicate protectiei infrastructurii virtuale (VMWare si HyperV).

5.3.3.7. *Soluţia antivirus*

Sistemul antivirus este dedicat instalarii pe platformele de procesare tip server si client oferite in cadrul solutiei. El trebuie sa fie usor de instalat, configurat si administrat, si sa ofere protectie de cel mai inalt nivel impotriva virusilor, a programelor spion si a rootkit-urilor, reducand astfel efortul necesar administrarii serverelor.

Sistemul antivirus trebuie sa indeplineasca urmatoarele cerinte tehnice:

- Actualizare automată şi programabilă prin internet la intervale de timp programate sau la cerere.
- Scanare în timp real a fişierelor, atât la deschiderea acestora cât şi la închidere; posibilitatea scanarii la cerere şi a serverului pe care este instalat.
- Cu ajutorul unei baze de date complete cu semnaturi de spyware şi a euristicii de detecţie a acestui tip de programe, produsul va trebui sa ofere protecţie anti-spyware şi să permită prevenirea furtului de date confidenţiale.
- Administrarea să poată fi făcută centralizat din cadrul consolei de management globale sau independent;
- Posibilitatea scanării la alegere doar a fişierelor având extensiile specificate de administrator.
- Posibilitaţi de acţiuni multiple la detecţia unui virus (disinfect, delete, mutare in carantina);
- Sa ruleze pe sistemele de operare ofertate;
- Să permită importul si exportul tuturor setarilor din toate modulele programului la nivel de client antivirus;
- Să tina cel putin log-uri ale evenimentelor si cererilor de scanare la cerere;
- Să permită atentionarea administratorului, daca scanarea la cerere a fost intrerupta de utilizator;
- Să aiba posibilitatea de a seta perioada de stocare a logurilor;
- Să aiba posibilitatea setarii automate sau manuale, pentru optimizarea fisierelor log;
- Să aibă posibilitatea adaugarii automate sau manuale a fisierelor in carantina;
- Să aibă posibilitatea expedierii automate si manuale a fisierelor infectate sau suspecte catre laboratorul de analiza antivirala al producatorului;
- Să aibă optiuni pentru a crea task-uri programate;
- Sa afiseze informatii despre configuratia statiei pe care este instalat. Vor fi afisate cel putin sistemul de operare, tipul de procesor si RAM-ul instalat pe statia respectiva;
- Setarile produsului antivirus trebuie să poată fi protejate cu o parola pentru a nu fi modificate decat de catre administratorii solutiei;
- Să poată trimite notificari administratorului solutiei prin SMTP si mesaje in LAN;
- La nivel de statie sa nu afiseze mesaje utilizatorului, dar sa informeze administratorul solutiei.
- La nivel de statie sa ofere informatii detaliate despre vesiunea instalata, cat si despre modulele integrate respectiv: kernel, semnaturi de virusi, engines.
- In cazul unei notificari de virus, sa avertizeze sonor utilizatorul.Soluția să permită activarea sau dezactivarea optiunii de avertizare sonora.

- Sa permită personalizarea/preconfigurarea de pachete antivirus (client) inainte de instalare in functie de cerintele administratorului. Aceasta operatiune se va efectua in urma unei singure actiuni din partea administratorului.
- Serviciul antivirus sa ruleze ca serviciu local;
- Produsul antivirus sa scaneze in mod automat, orice dispozitiv mobil de stocare la momentul introducerii in portul USB si se vor scana fisierele de tip AUTORUN.INF de pe dispozitivele de stocare.
- Să aibă posibilitatea de a genera din interfata client sau consola de management a unui fisier de tip log detaliiat, cu toate serviciile ce ruleaza pe respectiva statie, pentru identificarea si detalierea fiecarui servicu respectiv fisier cat si nivelul filtrarii in functie de gradul de risc.Fisierul log să poată fi exportat si trimis catre analiza.
- Să aibă posibilitatea,din interfata client sau consola de administrare de a genera CD/DVD/USB-stick boot-abile, cu versiunea antivirus la zi in vederea devirusarii calculatoarelor in mod “offline”.
- Sa ofere functie de autoprotectie, impotriva dezactivarii sau coruperii solutiei antivirus de catre diferite coduri malware.
- Clientul antivirus, sa prezinte in interfata de administrare locala vizualizarea activitatii in mod grafic in timp real atat a fisierelor aflate local cat si a activitatii din retea.
- Clientul antivirus să permită la vizualizarea activitatii din interfata de administrare locala setarea perioadei pe care se doreste vizualizarea raportului.
- Sa se poata activa sau dezactiva functia de NAP Network Access Protection sau echivalent;
- Utilizatorul din interfata client să poată vizualiza toate procesele care se executa si sa solicite informatii suplimentare de la producator despre fiecare proces referitoar la: nivelul de risc, numar utilizatori, nume aplicatie, detalii despre proces (locatie, dimensiune, descriere, companie, versiune fisier, nume produs) si ora la care s-a descoperit.
- La cerere, utilizatorul să poată verifica reputatia unui fisier oferind informatii despre: nivelul de risc, numar utilizatori, nume aplicatie,detalii despre proces (locatie, dimensiune, descriere, nume companie, versiune fisier, nume produs) și data la care s-a descoperit.
    - Clientul antivirus din interfata de administrare locala să permită o vizualizarea statistica centralizata pentru:

- Protectie antivirus si antispyware;
- Protectia in timp real a sistemului de fisiere;
- Protectie client email;
- Protectie acces WEB.

- Soluția de securitate să poată bloca mesajele de notificare, cand o aplicatie ruleaza in modul FULL SCREEN. De asemenea blocarea notificarilor să poată fi dezactivata in mod automat dupa un anumit timp definit in minute.
- Aplicatia trebuie Să aibă scanner rezident care sa monitorizeze in timp real aplicatiile care sunt lansate/rulate;
- Scanner-ul rezident trebuie sa ofere posibilitatea setarii optiunii de a porni sau nu automat la pornirea sistemului (PC-ului);
- Scanner-ul rezident trebuie Să aibă posibilitatea de a fi oprit manual;
- Scanner-ul rezident trebuie sa ofere posibilitatea setarii unui mod de scanare optimizat;
- Pentru a putea eficientiza lucrul cu PC-ul, produsul trebuie sa ofere posibilitatea de a seta stadiul in care sa fie scanate fisierele de catre modulul resident, respectiv la deschiderea fisierului, la crearea, respectiv executia lui, oprirea calculatorului.
- Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie ;
- Scanner-ul rezident al produsului antivirus trebuie să faca cel putin scanarea dupa semnaturi, euristic, spyware, adware si aplicatii ce pot reprezenta potentiale pericole;
- Scanner-ul rezident al produsului antivirus trebuie să ofere posibilitatea configurarii modulului euristic pe 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus ;
- Configurarea scanner-ului rezident al aplicatiei trebuie să permită excluderea de la scanare anumite foldere/ fisiere sau extensii specificate si posibilitatea setarii acestei reguli cu caracter temporar și / sau permanent;
- Scanner-ul rezident al aplicatiei antivirus trebuie să facă scanarea: sectoarelor de boot la accesare, a suportilor magentici/optici și a rețelei ;
- Scanner-ul rezident al aplicatiei trebuie sa ofere posibilitatea setarii mutarii in carantina a fisierului infectat .
- Produsul de securitate trebuie sa ofere posibilitatea de a putea defini reguli pentru unitatile portabile(memorii USB), CD/DVD, FireWire, Imaging Device(scaner,camere web), Imprimante USB, Bluetooth Device, Memory Card Reader, LPT/COM, regulile trebuie să poată fi facute dupa urmatoarele criterii: Tip Dispozitiv, Numar Serie, Producator-Vanzator, Model, si sa se poata aplica drepturi de citire si scriere, sau access refuzat pentru utilizatori definiti locali sau LDAP;
- Din clientul antivirus, utilizatorul trebuie să poată defini limite de scanare a obiectelor in functie de dimensiune fisier si durata maxima de scanare pentru fisierele respective.

- Din setarile clientului antivirus, utilizatorul trebuie să poată defini nivelul de scanare al arhivelor ce contin alte arhive si setarea dimensiunii acestora.
- Produsul antivirus trebuie să permită executarea fisierelor activarea functiei de euristica avansata. Aceasta functie trebuie sa se poata activa independent de setarea generala a produsului antivirus, si trebuie sa actioneze strict numai la executarea fisierelor.
- Produsul antivirus trebuie să permită activarea functiei de euristica avansata numai pe unitatii media portabile. Aceasta functie trebuie sa se poata activa independent de setarea generala a produsului antivirus, si va actiona strict numai la executarea fisierelor de pe unitatii media portabile;
- Soluția de securitate trebuie să permită analiza in mod activ comportamentul fisierelor, registrilor, proceselor si să poată preveni orice modificare fara o notificare.
- Aplicatia antivirus trebuie sa dispuna de cel putin optiunea de scanare a porturilor POP3 si HTTP;
- Pentru optimizarea resurselor ocupate de Soluția antivirus trebuie sa fie posibila setarea scanarii ambelor porturi sau doar a unuia dintre ele (cel folosit), in functie de necesitatile utilizatorului statiei;
- Produsul antivirus trebuie sa dispuna de optiunea pentru detectarea automata a portului POP3 si optiune pentru setarea manuala a portului in cazul in care nu este folosit cel default POP3 (110);
- Produsul antivirus trebuie sa dispuna de optiunea pentru detectarea automata a portului HTTP, setarea manuala a portului in cazul in care nu sunt folosite variante default si posibilitatea de a detecta automat comunicarea HTTP pe alte porturi;
- Produsul antivirus trebuie sa dispuna de optiunea de a modifica subiectul e-mail-urilor infectate primite pe statie. Mesajul trebuie să poată fi modificat conform preferintelor administratorului solutiei antivirus;
- Produsul antivirus trebuie sa dispuna de optiuni de a adauga in corpul e-mail-ului a unui mesaj care sa ateste faptul ca e-mail-ul a fost scanat si rezultatul scanarii;
- Produsul antivirus trebuie sa ofere optiuni de configurare pentru scanarea tuturor tipurilor de fisiere, indiferent de extensie si indiferent daca au sau nu extensie pentru fisierele care sunt scanate pe POP3 si HTTP;
- Configurarea scanner-ului aplicatiei astfel incat sa fie excluse de la scanarea POP3 si HTTP anumite extensii specificate;
- Protectia POP3 si HTTP a produsului trebuie să permită configurarea modulului euristic pe 2 nivele pentru a putea optimiza in functie de caz folosirea resurselor de catre aplicatia antivirus si timpul de scanare a fisierelor;

- La scanarea POP3 si HTTP produsul antivirus trebuie sa efectueze scanarea dupa semnaturi, euristic, spyware, adware si alte aplicatii ce pot reprezenta potentiale pericole;
- La scanarea HTTP produsul antivirus trebuie să poată interzice automat descarcarea fisierului infectat;
- Produsul antivirus trebuie Să aibă posibilitatea configurarii actiunilor care vor fi intreprinse la detectarea codului viral, in functie de tipul obiectelor infectate, la nivel POP3 si HTTP.
- Setarea actiunilor si modului de lucru la scanarea POP3 trebuie să poată fi facuta doar pentru acestea, nu trebuie sa fie facuta generic pentru toatea componentele produsului antivirus la nivelul statiei de lucru;
- Produsul trebuie Să aibă posibilitatea detectarii automate a modificarilor setarilor de retea si posibilitatea modificarii setarilor sale (daca este necesar) pentru a functiona corespunzator .
- Produsul antivirus, trebuie să permită scanarea traficului securizat SSL pentru protocolul HTTPS cat si pentru POP3S si IMAPS.
- Soluția antivirus trebuie sa-si poata face update-ul bazei de date cu semnaturi de virusi la intervale configurabile incapand de la un 1 minut;
- Update-ul trebuie să poată fi facut de pe Internet/ LAN/ alte medii de stocare;
- Produsul antivirus trebuie să poată detecta automat tipul de conexiune la Internet pentru a putea beneficia de fisiere de update adecvate tipului de conexiune;
- Produsul antivirus trebui Să aibă posibilitatea introducerii unei adrese de Internet/ Intranet de la care sa faca actualizarea componentelor aplicatiei;
- Updateul/Upgradeul trebuie să poată fi facute atat automat cat si manual (la cerere);
- Produsul antivirus trebuie să poată face detectatea automata a Proxy Server-ului daca acesta exista;
- Produsul antivirus trebuie sa ofere posibilitatea setarii unui utilizator si a unei parole cu care sa se log-eze in LAN pentru a face update-ul (altul decat utilizatorul curent);
- Update-ul din LAN trebuie sa se poata face cu ajutorul share-ului de pe sisteme Microsoft sau prin HTTP;
- Produsul antivirus trebuie să poată fi setat sa dea o notificare inainte de update/upgrade;
- Produsul antivirus trebuie Să aibă optiuni de configurare astfel incat sa nu fie necesara repornirea PC-ului/ serverului dupa actualizarea componentelor antivirusului.
- Produsul antivirus sa nu necesite repornire a calculatorului la upgrade.
- Din clientul antivirus trebuie sa se poata reveni la o baza de semnaturi anterioara in cazul in care se constata alerte de tip false-positive.

- Producatorul trebuie sa fie certificat pe plan international (ex. ICSA Labs, Virus Bulletin 100% Awards, CheckMark, AV Comparatives etc);
- Furnizorul trebuie sa fie certficat ca partener al producatorului sau reprezentantului in Romania al producatorului;
- Producatorul trebuie sa apara in lista Microsoft (List of antivirus software vendors)

http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx

Soluția antivirus trebuie sa fie licentiata pentru toate echipamentele de procesare date ofertate in cadrul solutiei, precum si pentru statiile utilizatorilor sistemului, dar nu mai putin de 350 de statii de lucru si 1000 de utilizatotri de posta electronica.

5.3.3.8. *Servere şi stocare centralizată*

Resursele de procesare vor fi asigurate de un șasiu de servere blade echipat cu 9 servere. Șasiul va fi echipat cu switch-uri Ethernet şi switch-uri SAN FC 8Gbps. Alimentarea şasiului va fi asigurată cu surse de alimentare hotplug şi redundante în schemă N+N sau N+1 care să permită alimentarea din două circuite electrice diferite. Cerintele detaliate ale echipamentelor de tip sasiu si server blade se regasesc in tabelele de mai jos.

Șasiu servere – 1 buc

Format	Sasiu rackmountable maximum 10U, cu suport pentru cel putin 12 noduri de calcul cu procesoare CISC x86
Caracteristici de inalta disponibilitate	Midplane de inalta disponibilitate, complet pasiv cu conectori pentru alimentare electrica, management si I/O pentru serverele blade. Trebuie sa suporte functii de tip hot-swap la nivelul fiecarui nod de calcul, switch-uri, module de management, surse de alimentare.
Surse de alimentare	Surse de alimentare interne in sasiu, hot-swap, cu posibilitatea de configurare a redundantei in N+N sau N+1, care sa asigure alimentarea redundanta in conditii de incarcare maxima a sasiului certificate 80 PLUS Platinum. Alimentare la 200-240V AC.
Sistem de ventilatie	De tip hot-swap, redundant, instalat intern in sasiu cu zone de racire pentru asigurarea racirii variabile a diferitelor zone din sasiu in functie de incarcare.
Module Switch	Suport pentru switch-uri interne Gigabit Ethernet, 10 Gigabit Ethernet, 16 Gbps Fibre Channel, Infiniband FDR
Conectivitate Retea Ethernet	Minim 2 x Switch Gigabit Etherne cu o latime de banda de cel putin 150 Gbps fiecare si oferind in total: minim 72 de porturi interne Gigabit, minim 16 porturi externe Gigabit, minim 4 porturi externe 10 GbE, minim 2 porturi 10GbE pentru stacking intern si 2 porturi 10 GbE CX4 pentru stacking extern

Conectivitate SAN	Minim 2 x Switch SAN Fibre Channel 8 Gbps, fiecare switch cu un numar de minim 18 porturi interne FC 8 Gbps si cel putin 8 porturi externe 8 Gbps. Cate 8 transceivere SFP 8 Gbps FC instalate in porturile externe ale fiecarui switch.
Management sistem	2 x modul de management centralizat, hot swap. Modulele de management trebuie sa dispuna fiecare de 2 x USB 2.0, 2 x Ethernet RJ45, 1 x Serial RS-232, 1 x port RJ45 dedicat pentru management; **Interfața de management centralizat:** • Sistemul trebuie să beneficieze de o interfață de management centralizat capabilă să administreze și să controleze toate resursele și mecanismele integrate: - blade-uri (mașini fizice); - interfețe I/O; • Sistemul trebuie să suporte adăugare și integrarea ulterioară a blade-urilor, toate putând fi controlate de la aceeași interfață de management; • Interfața trebuie să fie accesibilă cu o consolă și ca serviciu WEB pe porturi dedicate; **Administrarea centralizată a serverelor fizice si virtuale:** • interfata unificata pentru sarcinii administrative (start, stop, reboot); • o singura interfata de vizualizare a resurselor fizice si virtuale; • interfata de monitorizare sa fie bazata pe cel putin 3 componente: - vizualizarea evenimentelor – cum ar fi caderea unui echipament hardware, operatiuni de comutare automata a serverelor si rezultatul fiecarei operatiuni efectuate; - operatiuni recente – afisarea progresul diferitelor operatiuni efectuate; - monitorizarea retelei – posibilitatea de a vizualiza si corela retelele virtuale si fizice, prin intermediul hartii integrate; • să poată furniza date despre consumul de energie, iar acestea să poată fi afisate in forma unui grafic sau să poată fi exportate intr-un format csv, pentru o analiza ulterioara; • monitorizare centralizata mixta pentru servere fizice si virtuale;

	• sa functioneze in medii multi-hypervisor; • sa suporte migrarea in timp real pentru minim platformele hypervisor x86: VMware vSphere, Microsoft Hyper-V, Citrix XenServer, KVM, Oracle VM sau echivalente; • sa suporte setarea automata de resurse multiple intr-o operatiune de grup importand un fisier, in format csv, de definire a sistemului, care sa contina toate setarile si informatiile privind configuratia; • să permită operatiuni de migrare in timp real a serverelor virtuale, declansate in mod uniform pentru toate produsele hypervisor suportate, direct din consola de administrare si care sa se realizeze fara timp de nefunctionare si cu suport pentru echilibrarea dinamica a incarcarii; • sa pastreze pozitia initiala a fiecarui client al masinii virtuale și să permita migrarea inapoi in orice moment in locatia lor originala; • sa inglobeze funcționalitatea de a comuta complet gazdele masinii virtuale, incluzand toate elementele in functiune ale masinii virtuale , catre un server de rezerva; • comutarea să poată fi initializata manual sau automat prin funtia de auto-recuperare; • sa suporte back-up si restaurare completa a imaginii boot disk-ului incluzand sistemul de operare si alte date stocate pe acel disk; • sa ofere o functie integrata de clonare a serverului care să permită distributia unei imagini clonate, catre unul sau mai multe servere fizice; • imaginile sa fie gestionate centralizat si stocate de catre serverele de administrare; • auto-recuperarea serverelor cazute, fara interventia operatorului; • sa ofere o disponibilitate crescuta prin folosirea unor servere de rezerva cu sisteme fizice si servere cu gazde virtuale; • sa suporte virtualizare I/O pe servere, fara sa tina cont de tipul acestora (rack, tower si blade) • sa foloseasca tehnologia SAN-boot in combinatie cu tehnologia de virtualizare I/O pentru o disponibilitate crescuta; • sa inglobeze functia de Virtualizare a I/O permitind administartorului sa adauge, sa mentina sau sa elimine servere fara sa afecteze setarile

	retelei si fara sa fi nevoie de re-cablare; • Să aibă functia de "HBA Address Rename Service" sau echivalent; • sa suporte boot-area serverelor din sistemul de stocare al retelei atasate via Fibre Channel cat si boot-area serverelor de pe un disk local; • să permită configurarea retelelor fizice si virtuale; • sa ofere un modul de diagnoza a conexiunilor de retea, intre toate resursele administrate; • Interfata (aplicatia) de administrare centralizata trebuie sa includa licentele necesare pentru a acoperi numarul maxim de servere blade instalabile in sasiu;

Servere tip blade – 9 buc

Arhitectura	nod de calcul , compatibil cu şasiul de mai sus, cu minim două sloturi pentru procesoare;
Procesor	Minim 2 x procesoare multicore în arhitectură x86-64 cu total de minim 12 nuclee de procesare la o frecventa de minim 2,6 GHz fiecare și cu minim 2,5 MB memorie cache pentru fiecare nucleu de procesare
Memorie interna	Minim 192 GB PC3-12800 1600MHz ECC DDR3, suport pentru ChipKill, min. 24 sloturi de memorie, expandabil pana la minim 1500 GB, suport pentru memorii la viteza de 1600 Mhz Suport pentru ECC, Advanced ECC, memory mirroring si hot-spare memory, sau echivalent
Hard disk	Minim 2 x 100 GB SSD
Video	Controller video integrat
Interfete networking	4 porturi Gigabit Ethernet sau 2 porturi 10 Gigabit Ethernet
Fibre channel adapter	8 Gbps, dual port
Sloturi I/O	2 x PCI-Express Gen. 3.0
Management de sistem	Procesor de management integrat
Compatibilitate sisteme de operare	Serverul trebuie sa fie compatibil, certificat de producător si sa dispună de suport pentru următoarele sisteme de operare: Microsoft Windows Server 2008 R2 si 2012 R2 cu ultimele SP, SUSE Linux Enterprise Server 11, Red Hat Enterprise 6, Vmware vSphere 5

Sistem de stocare pe discuri – 1 buc

Sistemul de stocare pe discuri va trebui sa indeplineasca urmatoarele cerinte tehnice:

- Să permită stocarea redundanta a datelor simultan in doua locatii geografic diferite;
- Să permită replicarea datelor dintr-o locatie in alta;
- Să permită virtualizarea capacitatilor de stocare existente in fiecare locatie;

In acest sens, pentru fiecare locatie in parte, echipamentele ce compun Soluția de stocare pe discuri trebuie sa indeplineasca minim urmatoarele cerinte:

Controller SAN	Echipamentul trebuie Să aibă doua controller-e SAN activ-activ simetric, redundante, hot-swap.
Controller NAS	Echipamentul trebuie sa dispuna de suport pentru upgrade cu cel putin 4 controlere NAS integrate in sasiul echipamentului de stocare, independente hardware de controlerele SAN, dar cu management integrat, redundante, hot-swap
Protocoale suportate pentru accesul la date	Echipamentul ofertat trebuie Să aibă suport pentru: 8 Gbps FC, 1 & 10 Gbps iSCSI, 10Gbps FCoE, CIFS (SMB3), NFS v4, pNFS, FTP, SFTP folosind interfete dedicate Ethernet 1 Gbps si 10 Gbps.
Porturi instalate (conectivitate)	Echipamentul ofertat trebuie sa dispuna de cel putin: 8 porturi FC 8Gbps (4 porturi per controller SAN) echipate cu transceivere SFP
Memorie Cache	Cel putin 48 GB pentru SAN (24 GB per controller SAN). Echipamentul va avea instalat o extensie a memoriei cache cu o capacitate de 1000 GB brut, utilizabila simultan de catre SAN si NAS, atat pentru operatiuni de citire, cat si pentru operatiuni de scriere, configurata in mirroring cu hot-spare, folosind min. 10 discuri in tehnologie flash/SSD. Memoria cache va fi protejata cu baterie de backup sau metode echivalente;
Nivele RAID suportate	0, 1, 10, 5, 6.
Numar host-uri suportate	Cel putin 1024 host-uri SAN
Numar maxim LUN-uri	Cel putin 2048
Hard disk-uri instalate	Echipamentul va avea instalate la livrare cel putin: 48 discuri SAS 2.0 de 600 GB la 10000 rotatii pe minut

Suport extensie capacitate de stocare	Suport pentru cel putin 500 de discuri in sistem; Suport pentru module de expansiune de inaltime 3U, capacitate 15 hard disk-uri de 3,5”, conectivitate duala SAS la 6Gbps; Suport pentru module de expansiune de inaltime 2U, capacitate 25 hard disk-uri de 2,5”, conectivitate duala SAS la 6Gbps; Modulele de expansiune trebuie sa se conecteze la echipamentul de stocare prin magistrale de date redundante, cu latime de banda de cel putin 24 Gbps (SAS 6Gbps 4-lanes). Adaugarea unităților de expansiune va putea fi realizată online fără întreruperea conexiunilor cu unitățile de expansiune deja instalate.; Alimentare cu energie electrică redundantă - 2 surse de alimentare pentru fiecare sertar al sistemului
Tipuri de discuri suportate	SSD: 100, 200, 400 GB; SAS: 300, 600 GB SAS 6Gbps 15.000 RPM; 900GB, 1.2TB SAS 6Gbps 10.000 RPM; NL-SAS: 1, 2, 3, 4TB NL-SAS 6Gbps, 7.200 RPM

Facilitati de management	Sistem de management si monitorizare integrat in echipament trebuie sa fie accesibil de la distanta prin interfata grafica web-based, CLI; sa ofere acces securizat SSL/TSL si integrare LDAP; Sistemul de management trebuie sa asigure integrarea nativa cu platformele de virtualizare (VMware, Hyper-V): • Aplicatia de management a echipamentului de stocare trebuie să permită vizualizarea masinilor virtuale ce rezida pe volume alocate catre hipervizor; • Integrarea cu aplicatia de management a mediului virtual, care trebuie să permită provizionarea de capacitate de stocare, din aplicatia de management a mediului virtual; • Accelerarea hardware a operatiunilor ce au loc intre hipervizor si sistemul de stocare prin degrevarea unor procese de la nivelul hipervizorului si preluarea lor la nivelul echipamentului de stocare. Aceasta functionalitate trebuie să permită accelerarea mutarii unei masini virtuale intre doua volume de date ale hipervizorului si accelerarea efectuarii unei copii identice a unei masini virtuale; • support pentru VAAI si VASA; Sistemul trebuie sa includa capabilitatea de monitorizare si management a multiplelor echipamente din aceeasi gama intr-o singura instanta a interfetei, atat pentru serviciile SAN, cat si pentru cele NAS; Sistemul de management trebuie sa asigure suport inclus pentru analiza si monitorizare de performanta, precum si monitorizarea si prioritizarea accesului la date al diferitelor servere;

Optimizarea capacitatii de stocare	Suport inclus pentru alocarea catre servere a unei capacitati de stocare mai mare decat cea fizic disponibila (virtual provisioning); Suport inclus pentru compresia in-line a volumelor de date, atat la nivel de bloc, cat si la nivel de fisier; Suport inclus pentru deduplicarea datelor in volumele cu acces atat la nivel de bloc, cat si la nivel de fisier; Pentru imbunatatirea performantelor sau a timpilor de raspuns la nivelul aplicatiilor, echipamentul ofertat trebuie sa includa suport pentru: • definirea de volume de date pe masive ce suporta discuri in tehnologii diferite (SSD + SAS + NL-SAS), organizate in matrici cu nivele de protectie RAID diferite(spre ex.: masiv format din matrici de discuri SSD in RAID 1 + discuri SAS in RAID 5 + discuri NL-SAS in RAID 6); • optimizarea automata a plasarii datelor pe cele 3 tipuri de discuri ale unui volum de date in functie de gradul de accesare a blocurilor de date, aceasta insemnand ca datele cele mai des accesate trebuie sa fie plasate de catre echipament pe SSD-uri, iar datele mai putin accesate sa fie mutate pe discurile SAS sau NL-SAS; • redistribuirea datelor intre matricile de discuri atunci cand sunt adaugate discuri suplimentare, pentru cresterea capacitatii utile.
Protectie date	Echipamentul trebuie Să aibă incorporate baterii ce asigura protectia controller-elor si a memoriei cache la caderile de curent prin salvarea automata a datelor din cache pe discuri inainte de oprirea echipamentului; Se va asigura suport, prin licentiere ulterioara, pentru a realiza copii complete ale datelor, sau bazate pe imaginea acestora la un anumit moment de timp. Spatiul rezervat copiilor de date trebuie să poată fi configurat pe discuri separate fata de cele unde stau datele de productie. Sistemul trebuie să permită realizarea de copii ale oricarei copii de date („snaps of snap”). Copiile de date complete, sau bazate pe imagini, trebuie să poată fi accesate atat in mod „read”, cat si in mod „write”. Se va asigura suport pentru minim 255 de copii ale fiecarui volum de date (LUN); Echipamentul de stocare trebuie sa includa suport nativ pentru migrarea datelor pe/de pe un alt echipament de stocare.

Replicare date	Ehipamentul de stocare ofertat trebuie sa includa o solutie cu suport software si hardware pentru realizarea de copii de siguranta a datelor la distanta – prin replicarea sincrona, asincrona a datelor. Se va lua in calcul replicarea unui volum de date minim de 12TB din locatia principala in locatia secundara. Soluția de replicare trebuie sa fie instalata pe o platforma hardware dedicata, diferita de serverele si echipamentele de stocare existente si sa suporte replicarea datelor de pe echipamente de stocare de la diversi producatori (incluzand IBM, Netapp, EMC, HDS, HP etc). Arhitectura solutiei trebuie sa fie tip cluster. Soluția de replicare a datelor la distanta trebuie sa dispuna de o tehnologie de jurnalizare a tuturor operatiunilor de scriere care să permită restaurarea datelor la orice moment de timp. Copiile de siguranta trebuie să poată fi grupate per aplicatie, pentru a asigura consistenta recuperarii datelor aplicatiilor interdependente. Pentru utilizare eficienta a benzii de transmisie dintre centrele de date, Soluția de replicare trebuie sa includa suport pentru replicarea doar a datelor modificate si transmiterea numai a blocurilor de date unice (deduplicare) si comprimate (compresie).

Virtualizare echipament de stocare	Echipamentul de stocare ofertat trebuie sa includa o solutie cu suport software si hardware pentru virtualizarea echipamentelor de stocare de date existente. Soluția trebuie să permită virtualizarea, migrarea si replicarea volumelor de date ce rezida pe echipamentele de stocare de la diversi producatori (EMC, IBM, HP, NetApp, Hitachi, etc.), fara restrictii de licentere bazate pe producatorul echipamentului, clasa din care face parte acesta sau numarul de echipamente virtualizate. Se va lua in calcul virtualizarea unui volum minim de date de 25 TB in fiecare din cele doua locatii. Soluția trebuie să includa 4 controllere SAN, redundante, hot-swap si să poată fi scalata pana la 8 controllere SAN ce partajeaza aceiasi memorie cache. Upgrade-urile software si hardware trebuie sa se poata realiza online, fara intreruperea accesului la date. Suport pentru conectivitate Fibre Channel 8 Gbps Cel putin 32 porturi FC 8Gbps (8 porturi per controller SAN) echipate cu transceiver-e SFP: min. 16 porturi pentru back-end si 16 porturi pentru front-end. Memorie cache de tip RAM de cel putin 128 GB scalabila la 256 GB. Prin mecanismele de virtualizare incluse, sistemul de stocare propus trebuie să permită migrarea si replicarea datelor intre sisteme de stocare produse de diversi producatori. Mecanismul de virtualizare trebuie să permită distribuirea spatiului de stocare pe mai multe sisteme de stocare fizice independente, fara ca acest lucru sa impuna restrictii. Soluția trebuie să permită virtualizarea echipamentelor de stocare externe existente, conectabile prin interfete FC, switch-uri SAN. Un volum logic virtual LUN prezentat serverelor trebuie să poată fi alocat simultan pe doua sisteme de stocare diferite, indiferent de producatorul acestora, in regim de mirroring, in asa fel incat, in situatia in care un sistem de stocare din back-end se defecteaza, volumul sa fie disponibil si accesibil fara intreruperea traficului de productie.

	Soluția trebuie să permită distribuirea capacitatii virtualizate, permitand ca un volum virtual sa fie compus din volume logice (LUN-uri) prezentate dintr-unul sau mai multe echipamente de stocare. Volumele logice (LUN-urile) trebuie poata fi configurate in oglinda (mirror), concatenate (inlantuite) sau distribuite (striping) pentru a crea un volum virtual (accesibil de catre host-uri). Suport inclus pentru definirea unui volum virtual bazat pe un volum logic (LUN) creat pe echipamentul de stocare din back-end fara alterarea datelor existente. Metadatele asociate volumului virtual trebuie să poată fi stocate pe volume dedicate, separate de volumele logice importate in echipamentul de virtualizare propus. Suport inclus pentru extinderea dinamica, ori de cate ori este nevoie, a spatiului de stocare al unui volum virtual prin adaugarea capacitatii necesare și apoi selectarea dintr-o listă de volume disponibile. Suport inclus pentru a muta datele intre diverse echipamente de stocare din back-end fara downtime la nivel server, aplicatie. Soluția trebuie să dispuna de surse de alimentare si sisteme de ventilație redundante, hot-plug
Sisteme de operare minim suportate	Windows Server 2008 R2, Windows Server 2012 R2, Microsoft Hyper-V, VMware ESXi, RedHat Enterprise Linux, Novell Suse Enterprise Linux, Solaris 10 Sparc&x86, HP-UX, IBM AIX, Citrix Xen Server; Echipamentul de stocare trebuie sa includa licentele necesare accesului sistemelor de operare suportate.

Accesorii incluse	2 x SAN Switch fiecare cu 48 de porturi FC 8Gbps universale (D, E, F, M, EX, N) active si echipate cu tranceivere SFP cu conectori LC, auto-sensing 2, 4, 8Gbs FC: - ISL Trunking - Switch-ul trebuie să permită configurarea a pana la 8 porturi 8Gb/s per ISL trunk prin licenta optionala; - Performanta - full-line switching: 2.125 Gb/s line speed, full-duplex; 4.25 Gb/s line speed, full-duplex; 8.5 Gb/s line speed, full-duplex; - Banda agregata - 768 Gbps end-to-end full duplex - Servicii fabric suportate - Monitoring and Alerting Policy Suite (MAPS); Flow Vision; Advanced Performance Monitoring (Top Talkers for E_Ports, F_Ports, and Fabric mode); Adaptive Networking (Ingress Rate Limiting, Traffic Isolation, QoS); Bottleneck Detection; Advanced Zoning (default zoning, port/WWN zoning, broadcast zoning); Dynamic Fabric Provisioning (DFP); Dynamic Path Selection (DPS); Enhanced BB credit recovery; Fabric Watch; FDMI; Frame Redirection; Frame-based Trunking; FSPF; Integrated Routing; IPoFC; ISL Trunking; Management Server; NPIV; NTP v3; Port Fencing; Registered State Change Notification (RSCN); Reliable Commit Service (RCS); Server Application Optimization (SAO); Simple Name Server (SNS); Virtual Fabrics (Logical Switch, Logical Fabric); - Management - HTTP, SNMP v1/v3 (FE MIB, FC Management MIB), SSH; Auditing, Syslog; Advanced Performance Monitoring; Command Line Interface (CLI); SMI-S compliant; - Securitate - SSL, SSH v2, HTTPS, LDAP, RADIUS, Role-Based Access Control;
Garanție	Garanția hardware a echipamentelor din compunerea echipamentului de stocare va fi de minim 36 luni. Garantia hardware va fi asigurata cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe saptamana, cel mai tarziu a doua zi lucratoare – Next Business Day), care sa garanteze diagnosticarea echipamentului sau modulului defect si inlocuirea acestuia in maxim 3 zile lucratoare, fara alte costuri; Totodata, se va asigura pentru minim 36 de luni acces 24x7 in centrul de asistenta al producatorului, cu posibilitatea raportarii problemelor aparute in functionare si solicitarea rezolvarii acestora functie de severitate. De asemenea se va asigura dreptul de a face update-uri si upgrade-uri la toate componentele software (sistem de operare, firmware, etc).

Echipamentele hardware vor fi integrate in fiecare din cele doua locatii, intr-un ansamblu cabinet tip RACK, echipat cu PDU-uri pentru doua surse de alimentare diferite, solutie UPS redundanta si consola locala TFT tip KVM, cu minim urmatoarele specificatii tehnice:

Denumire	**Echipament Cabinet modular de tip RACK**
Înălțime utilă	• Capacitate utilă de minim 42 unitati rack;
Uși și panouri laterale	• Uși și panouri laterale demontabile; • Posibilitatea de schimbare a sensului de deschidere a usii fata; • Posibilitatea de a securiza la nivel fizic echipamentele aflate in interior folosind incuietori cu chei speciale pentru ușile față-spate și panourile laterale; • Să ofere acces facil pentru instalara/dezinstalarea echipamentelor prin inlaturarea temporara a usilor; • Rack-ul va fi prevazut cu intrari/iesiri pentru cabluri electrice, date, RF prin locasuri special concepute in acest scop;
Ventilare	• Ventilare libera cu usi fata-spate perforate in proportie de minim 80 %; • Unitatile rack neocupate, vor fi acoperite cu panouri false, pentru a garanta ventilare cat mai buna;
Compatibilitate	• Echipamentul cabinet sa fie compatibil cu echipamentul de tip sasiu server lamelar si echipamentele de stocare, in ideea de a se asigura o compatibilitate optima intre dispozitive
Incarcare	• Sa suporte o incarcare de minim 1000 Kg;
Denumire	**Sursa neintreruptibila de tensiune tip UPS in configuratie redundanta**
Iesire	• Structura de alimentare de tip UPS de tip on-line dubla conversie, monofazata (1/1) ; • Capacitatea de putere : de minim 10KVA ; • Voltaj nominal iesire : 230V ; • Distorsiuni Voltaj nominal : max. 3% ; • Frecventa de iesire : 50 – 60 Hz (+/- 3 Hz); • Forma de unda : sinusoidala ; • Conectori iesire : 4 x IEC 320 C13, 4 x IEC 320 C19, 4 x IEC jumpers ;
Intrare	• Voltaj nominal de intrare : 230V ; • Frecventa de intrare : 50 – 60 Hz (+/- 5Hz detectie automata) ; • Gama tensiunilor de intrare : 160 – 280V ;
Baterii si timp de functionare	• Componentele interne active ale unitatii UPS, inclusiv bateriile, vor fi de tip hot-swap si vor permite deservirea (inclusiv inlocuirea acestora) fara oprirea sarcinii ; • Eficienta la incarcare maxima : min. 92% ; • Autonomia UPS-ului : min. 50 minute la o incarcare de 75% ;
Protectie	• Unitatea UPS va fi echipata cu functie interna activa de comutare neasistata, automata si transparenta pe bypass fara oprirea sarcinii atunci cand componentele interne de conversie si corectie ale unitatii nu

	fac fata sau prezinta erori de functionare ;
Management	• Interfata tip DB-9 RS-232 • Panou de control tip LED cu funtie de avertizare vizuala pentru urmatoarele stari ale echipamentului: functional, functionare pe baterie, indicator de inlocuire a bateriilor, supraicarcare si indicator pentru modul bypass; • Alarma sonora: cu moduri distincete de atentionare pentru trecerea in modul de functionare pe bateriisi baterie scazuta; • Unitatea UPS va fi echipata cu modul intern amovibil de management in retea (SNMP sau asimilat) ;
Mediu functionare	• Temperatura: 0 – 40 C; • Umiditate: 0 – 95%; • Zgomot: 55 db; • Caldura disipata: max. 2300 BTU/h
Dimensiune	• Montabil in Rack de 19 ‘’ , inaltime de maxim 6 RU ;
Denumire	**Componeta distributie tip PDU**
Conectori	• Pentru alimentarea echipamentelor se vor folosi unitati de tip Server PDU dupa cum urmeaza: • PDU-uri in cantitate suficienta astfel incat sa ofere un total de minim 6 x conectori 16A si 10 x conectori 10A • Alimentarea echipamentelor se va realiza din doua surse diferite de alimentare • Nu este acceptabila cascadarea pe mai mult de doua niveluri de distributie
Denumire	**Consola locala tip KVM**
Monitor	• Minim 17 inch; • Suport pentru afisare de rezolutii native de (min.) 1280x1024 ; • Contrast 450 :1 (TYP) ; • Luminozitate 200cd/m2
Tastatura	• Tastatura standard cu minim 87 taste si touchpad cu 2 butoane si functie de scrolling;
Dimensiuni	• Montabil in rack 19 inch , kit pentru montare inclus ; • Consola va ocupa, pliata, un spatiu optim de 1U in rack ;

5.3.3.9. *Echipamente de interconectare - minim 6 buc*

Interconectarea serverelor va fi asigurată de switch-urile din interiorul șasiului de servere blade. Suplimentar, pentru conectarea restului de echipamente se vor folosi switch-uri 10/100/1000 Base-T Ethernet cu câte 40 porturi RJ45 si patru porturi SFP care să permită popularea cu porturi 10 Gbps. Performanțele asigurate de fiecare switch vor fi de minim 100 Mpps throughput. Switch-urile trebuie sa asigure următoarele capabilități layer 2:

- Numar minim de adrese MAC per sistem: 30000

- Suport pentru pachete mari: Min 9216 bytes
- Numarul de VLAN-uri: Min 4000
- Functionalitate Per-VLAN Spanning Tree Plus (PVST)
- IEEE 802.1D: Spanning Tree Protocol
- IEEE 802.1Q: VLAN tagging
- IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP)
- IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

Precum și următoarele capabilități layer 3:

- Protocoale de routare: RIPv1/v2, BGP
- Rute statice.

5.4. Managementul utilizatorilor şi accesul la sistem

În cadrul sistemului integrat SIMISC trebuie sa fie disponibile mecanisme şi interfeţe de administrare şi configurare a tuturor claselor şi instanţelor de entităţi asociate rolurilor, grupurilor şi profilelor de utilizatori, prin intermediul utilizării componentei de administrare. Astfel, SIMISC trebuie să permită autentificarea tuturor utilizatorilor în conjunctie cu nivelurile de securitate prezente la toate nivelele arhitecturale.

Administratorii reprezintă o categorie aparte de utilizatori, acestia accesează zona de management a sistemului, şi trebuie sa aibă configurate roluri şi profile corespunzătoare astfel încât să aibă acces la toate datele şi modulele aplicaţiei. Ei trebuie sa fie prevăzuţi şi cu drepturi în subsistemul de administrare, pentru a avea acces în vederea monitorizării, întreţinerii şi configurării sistemului. În contextul controlului accesului, doar administratorii trebuie sa aibă dreptul de a specifica roluri pentru utilizatori şi drepturile de acces ale acestora.

Utilizatorilor li se vor acorda permisiuni în mod individual sau pe grup. Apartenenţa la un grup va acorda tuturor utilizatorilor din grupul respectiv drepturi echivalente. Un utilizator trebuie să poată aparţine simultan la unul sau mai multe grupuri. Drepturile trebuie să poată fi moştenite. De asemenea, sistemul trebuie să permită noţiunea de subgrup, care reprezintă posibilitatea ca un grup să fie membru într-un alt grup. Administrarea conturilor de utilizator trebuie efectuata respectând următoarele cerinţe:

- Sistemul asignează fiecărui cont de utilizator un identificator unic.
- Sistemul va oferi reguli configurabile pentru crearea identificatorilor unici.
- Sistemul va include capabilitatea de a exporta/importa utilizatori.

- Sistemul oferă posibilitatea de a aproba în mod automat orice solicitare printr-un set de reguli şi politici.

Sistemul trebuie sa ofere functionalitatea de a vizualiza o solicitare de cont care a fost trimisă şi datele asociate cu acea solicitare.

Sistemul de management al utilizatorilor trebuie sa fie licentiat astfel incat sa nu fie limitat la numarul de utilizatori care pot fi definiti in cadrul sistemului informatic solicitat.

5.5. Securitatea sistemului

Sistemul informatic trebuie protejat impotriva incercarilor deliberate sau accidentale de acces neautorizat la datele pe care acestea le inmagazineaza. Sistemul trebuie să permită urmatoarele facilitaţi:

- Ierarhizarea in grupuri a utilizatorilor finali;
- Autentificarea in sistem printr-un mecanism de tip „Single Sign-On", permiţind accesul utilizatorului in toate modulele pentru care dispune de drepturile necesare dupa introducerea numelui de utilizator şi a parolei o singura data in cadrul unei sesiuni de lucru;
- Asigurarea securitaţii tuturor interfeţelor sistemului informatic, prevenind accesul utilizatorilor neautorizaţi la sistem;
- Raportarea pe baze periodice a detaliilor privitoare la accesul in sistem al utilizatorilor;
- Să poată fi definite drepturi de acces (vizualizare/ actualizare) la informaţie pentru utilizatori/ roluri/ grupuri;
- Pentru fiecare rol, in funcţie de specificul activitaţii acestuia, se vor stabili componentele sistemului informatic care trebuie sa acopere activitatea curenta. Se va realiza asocierea intre salariatul care lucreaza şi utilizatorul declarat in cadrul aplicaţiei, caruia i s-a acordat un set de drepturi de acces la informaţiile din baza de date. Toate tranzacţiile efectuate de utilizatori vor fi inregistrate in fişiere speciale;
- Se vor furniza funcţionalitaţi de administrare care să permită oferirea sau revocarea drepturilor de acces, accesul la informaţii pe baza de parole.
- Drepturile de acces se vor acorda diferenţiat in funcţie de: modul, operaţie, grad de securizare a informaţiei, nivel organizaţional;
- Furnizorul sistemului informatic integrat trebuie sa asiste clientul in realizarea unei politici de securitate a organizaţiei;
- Sistemul va permite administrarea drepturilor pentru grupuri de utilizatori la nivel de module, funcţii şi operaţii;

- Sistemul va permite lucrul in paralel cu toate aplicaţiile şi a mai multor utilizatori simultan in aceeaşi aplicaţie, chiar in acelaşi ecran;
- Sistemul va gestiona şi va rezolva probleme de acces concurent la resurse, alegind politica in funcţie de specificul aplicaţiei. Sistemele şi bazele de date nu vor permite generarea de inconsistenţe in date din cauza accesului concurent.

Implementarea policiticilor de securitate se va face cu echipamente dedicate funcțiilor de securitate. Fiecare categorie de echipamente va fi asigurată cu cel puțin două produse identice configurate redundant. Principalele categorii de echipamente care nu trebuie să lipsească din soluția de securitate sunt descrise în tabelele următoare:

5.5.1. Echipamente tip firewall - 2 buc activ/activ

Caracteristici performante	Cerinte minimale
Arhitectura sistemului	Asigura in timp real protectie retelei printr-o combinatie de antivirus, filtrare web, firewall, vpn, detectia si prevenirea dinamica a intruziunilor, controlul aplicatiilor, prevenirea scurgerii informatiilor sensibile. Sistemul nu trebuie licentiat per numar de utilizatori (nu exista numar limitat de utilizatori).
Numar de porturi	• Minim 10 porturi 10/100/1000 Base-T Ethernet • Minim 2 porturi USB 2.0
Functionalitati de securitate mnimale	• Performanta firewall: 8 Gbps • Performanta IPS: 1,2 Gbps • Performanta VPN IPSEC: 4 Gbps • Numar de tunele IPSec VPN concurente: 1800 • Performanta SSL VPN: 180 Mbps • Utilizatori SSL VPN: 450 • Performanta Antivirus prin proxy: 180 Mbps • Numar de conexiuni concurente: 1800000 • Numar de conexiuni pe secunda: 45000 • Politici de securitate: 8000 • Instante virtuale: 7

Caracteristici hardware	• Spatiu de stocare: Min 32 GB • Surse redundante de alimentare • Montabil in rack, dimensiune 1U • Suport pentru clustering HA activ-activ si activ-pasiv
Caracteristici Layer 3 si Layer 2	Sistemul trebuie sa ofere functionalitatea de definire rutere/firewall-uri virtuale (in instante separate), in care fiecare Să aibă tabela proprie de rutare. Echipamentul poate ruta traficul pe baza adreselor IP sursa si destinatie. • Protocoale de routare: RIPv1/v2, OSPF, BGP si PIM • Rute statice • Suport VLAN (802.1q) • Functionalităti NAT, PAT si Transparent Bridge • Suport SNMP
Functionalitati de securizare si control al traficului	• Detectie si protectie impotriva atacurilor de tip IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan, Java Applet, Cookies si ActiveX • Conexiuni VPN protejate impotriva Replay Attacks • Limitarea noilor sesiuni deschise de la aceeasi adresa IP • Actualizarea bazei de date de semnaturi manuala si automata • Detectia protocoalelor si anomaliilor de protocol • Firewall de tip stateful • Autentificare utilizatorilor definiti local sau extern prin RADIUS/LDAP/TACACS+ • Politici de filtrare bazate pe identitatea utilizatorului/servicii folosite si sistemul de operare de statie folosit • Limitare/garantare/prioritizare a benzii de trafic prin politici • Protectie Antivirus (pentru protocoalele SMTP, POP3, IMAP, HTTP, FTP, IM, HTTPS, POP3S, IMAPS, SMTPS) • Prevenirea intruziunilor (IPS si IDS) • Inspectie continut WWW cu filtre web pe baza de categorii

	de website-uri • Control al aplicatiilor • Prevenirea scurgerilor de date confidentiale
Configurare si management	• Configurare prin port serial (RS-232) sau remote (telnet, ssh), GUI prin HTTPS. Sistemul trebuie să poată fi configurat de mai multi administratori, fiecare cu profil individual de acces • Administratorii trebuie sa fie autentificati cu parole statice sau dinamice (RADIUS, RSA SecureID) • Trebuie sa fie posibil upgrade-ul de firmware, salvarea si restaurarea configuratiei de pe USB
Certificate	Acuratetea filtrarii componentelor trebuie sa fie demonstrata de urmatoarele certificate: ICSA: Firewall, IPSec, SSL VPN, IPS, Antivirus
Garantie si suport	Minim 3 ani inclusiv semnaturi IPS, antivirus, filtrare web, NGFW, inclusiv updateuri software, NBD

5.5.2. Echipamente tip firewall de aplicatii - 2 buc

Caracteristici performante	Cerinte minimale
Numar de porturi	• Minim 6 porturi 10/100/1000 Base-T Ethernet din care minim 4 porturi care să permită functionalitatea de bypass hardware • Minim 2 porturi SFP • Port consola RS-232
Functionalitati de securitate mnimale	• Permite detectarea si blocarea atacurilor asupra aplicatiilor web; • Să permită identificarea si blocarea traficului generat de masinile de tip bot; • Să permită blocarea pe baza de reputatie a surselor cu potential malitios de tip malware, spam, phishing, DDoS, proxy anonim; • Să permită auditul accesului catre aplicatiile web; • Să permită detectarea incercarilor de fraudare din web; • Să permită analiza avansată a incidentelor și să ajute investigatia criminalistica in cazul incidentelor de securitate; • Să ofere protectie DDoS pentru atacuri la nivel retea si aplicatie; • Să permită controlul accesului clientilor dupa blacklist si whitelist configurabile de adrese IP;

	• Suport Web Application Scanner & Vulnerability Assesments • Sa furnizeze rapoarte ale vulnerabilitatilor identificate in functie de severitate si pe categorii de vulnerabilitati • Protectie Anti Web Defacement – restaurarea continutului original al unei aplicatii web protejate in cazul modificarii malitioase al acestuia • Validarea conformitatii RFC HTTP a traficului procesat • Alerte configurabile prin mesaje email, loguri Syslog • Suport SNMP
Protecţie împotriva următoarelor atacuri informatice	• Controlul ratei de acces; • Controlul tentativelor esuate de acces; • Atacuri de tip brute force; • Atacuri de supraincarcare a bufferelor; • Atacuri de manipulare a cookie-urilor; • Manipularea cererilor catre alte pagini; • Utilizarea scripturilor pentru manipularea cererilor http; • Supraincarcarea cu conexiuni de tip SYN; • Supraincarcarea prin conexiuni de viteza mica; • Atacuri de manipulare a URL-urilor; • Atacuri cu pachete codate; • Atacuri de manipulare a formularelor; • Atacuri de manipulare a campurilor ascunse; • Atacuri de manipulare a headerelor pachetelor HTTP; • Validarea pachetelor HTTP conform RFC; • Atacuri de injectie de comanda pentru sistemul de operare; • Atacuri cu trafic recursiv in cadrul fluxului HTTP; • Atacuri prin transferul de fisiere de la distanta; • Atacuri de manipulare a schemelor; • Atacuri realizate cu ajutorul motoarelor de cautare; • Atacuri cu injectie de comenzi SQL; • Atacuri de tip XML prin manipularea parametrilor.
Capabilitati de manipulare a continutului si securitate informatica	• Să permită rescrierea URL-urilor • Să permită modificarea cererilor si raspunsurilor HTTP • Să permită balansarea traficului catre mai multe servere reale • Să permită particularizarea mesajelor de eroare • Sa ofere functionalitate de invatare automata pe baza traficului inspectat pentru crearea profilelor de protectie
Optiuni pentru autentificarea utilizatorilor	• Autentificare cu utilizatori definiti local • Autentificare cu utilizatori definiti extern prin RADIUS, LDAP si NTLM • Suport pentru autentificarea utilizatorilor prin certificate digitale X.509 • Suport penru single-sign-on a utilizatorilor pe aplicatiile web protejate
	• Rapoarte ale vulnerabilităților identificate în funcție de

Alte capabilități suportate	severitate şi pe categorii de vulnerabilități; • Rapoarte ale vulnerabilităților comune; • Rapoarte ale vulnerabilităților aplicațiilor; • Sumar al scanărilor; • Previne expunerea ilicită a paginilor web; • Funcționalitate de auto învățare pentru crearea profilelor de trafic.
Accelerare hardware	• Load balancing; • SSL offload; • Compresia datelor şi multiplexarea conexiunilor TCP.
Caracteristici hardware	• Throughput minim 700 Mbps • Latenta maxim o milisecunda • Minim 2x 2TB HDD • Montabil in rack, dimensiune 2U • Utilizatori nelimitati • Surse redundanta de putere hot-swap • Suport SNMP
Garantie si suport	Minim 3 ani NBD, cu updateuri si semnaturi incluse

5.5.3. Echipamente tip firewall baza de date - 2 buc

Caracteristici performante	**Cerinte minimale**
Numar de porturi	• Minim 6 porturi 10/100/1000 Base-T Ethernet; • Minim 2 porturi SFP;
Functionalitati de securitate mnimale	• Să permită detectarea vulnerabilitatior bazei de date si permite blocarea accesului la ele din exterior; • Să permită auditul accesului catre baza de date; • Să permită analiza avansata a incidentelor si ajuta investigatia criminalistica in cazul incidentelor de securitate; • Să permită captarea activitatea utilizatorilor in lucrul cu baza de date; • Să permită generarea de alerte prin SMTP, SNMP si SYSLOG; • Sa asigure aplicarea politicilor de securitate atat in mediu virtualizat cat si in medii standard; • Să permită crearea de politici pentru protectia datelor prin metode automate in urma monitorizarii bazelor de date; • Sa detecteaze in mod automat datele cu caracter sensibil ce sunt stocate in bazele de date monitorizate; • Furnizeaza informatii pentru remedierea vulnerabilitatilor identificate la scanarea bazelor de date; • Sa genereaze rapoarte predefinite si personalizabile privind rezultatele auditului bazelor de date si activitatea utilizatorilor.
Moduri de instalare	• Sniffer la nivel de retea, culegerea de date si monitorizarea sunt realizate fara impact asupra bazelor de date

	monitorizate; • Audit nativ, culegerea de date si monitorizare sunt realizate prin interogare directa a bazelor de date prin retea; • Audit pe baza de agenti, culegerea de date si monitorizare sunt realizate prin utilizarea de agenti instalati pe serverele bazelor de date;
Baze de date suportate si sisteme de operare	• Baze de date ce pot fi folosite ca repository: Apache Derby, Microsoft SQL Server, Oracle, PostgreSQL; • Baze de date suportate: DB2; Microsoft SQL Server; MySQL; Oracle; Sybase ASE;
Caracteristici hardware	• Licenta pentru minim 30 de baze de date; • Minim 2x 2TB HDD; • Boot Image: minim 1GB USB; • Surse redundante de putere hot-swap; • Montabil in rack, dimensiune maxima 2U; • Echipamentul trebuie sa fie certificat CE/FCC Class A;
Garantie si suport	• Minim 3 ani NBD, inclusiv updateuri software si semnaturi.

5.5.4. Echipamente de criptare comunicații - 2 buc

Caracteristici performante	**Cerinte minimale**
Componenta hardware	• 2 porturi 1000Base-X pentru date echipate cu conectori SFP gigabit de cupru • 1 port 10/100BaseT dedicat functiilor de management • 1 port serial de consola (RS232) • Indicator de alimentare, alarma si stare • Montare in rack de 19 inch • Dimensiune minima 1U
Specificatii de retea oferite	• Suport Ethernet • Pastrarea etichetelor VLAN • Pastrarea etichetelor MPLS • Suport pentru pachetele IPv4 • Suport pentru pachetele IPv6
Specificatii de criptare oferite	• Suport pentru criptare AES 256, modul CBC • Suport pentru criptare 3DES • Autentificare prin HMAC-SHA-256-96 • Criptarea in tunel ESP cu pastrarea header-ului • ESP transport mode (criptarea payload-ului la Layer 4) • Suport pentru criptare la Layer 2 • Suport pentru politica de criptare care sa includa adresa ip sursa si/sau adresa ip destinatie • Suport pentru politica de criptare care sa includa port sursa si/sau port destinatie • Suport pentru politica de criptare bazata pe identificatori de protocol

	• Suport pentru politica de criptare bazata pe identificatori VLAN • Suport pentru politica de criptare care sa contina adrese de multicast
Functii de management al echipamentului	• Out of band management • Suport syslog • Suport SNMP v2c si SNMP v3 • Acces la interfata administrativa folosind certificate digitale X.509 v3 • Acces la interfata administrativa folosind SSL • Acces la interfata administrativa folosind SSH • Jurnalizare si auditare integrate
Certificare	• Echipamentul trebuie sa fie certificat FIPS 140-2 Level 2 • Echipamentul trebuie sa fie certificat Common Criteria EAL4+
Sursa de alimentare	100-240V
Garantie	Minim 36 de luni inclusa in configuratia propusa. Suportul si garantia trebuie sa fie asigurate in Romania.

5.6.Confidenţialitatea datelor

Accesul la date trebuie sa fie permis doar prin intermediul serviciilor oferite de sistemul SIMISC, pe baza drepturilor avute in sistem, accesul direct la datele din bazele de date trebuie sa fie restrictionat fara exceptie. De asemenea, accesul trebuie sa fie reglementat prin politicile de securitate, aferente fiecarui utilizator. Implementarea acestora trebuie sa asigure respectarea prevederile legale in ceea ce priveste libertatea cetatenilor, dreptul la viata libera si procesarea informatiilor cu caracter personal.

6. Managementul de proiect

Dată fiind complexitatea din punct de vedere tehnic a proiectului, se subcontractează următoarele activităţi generale de management al proiectului:

- Elaborare rapoarte de progres;
- Suport pentru fundamentarea şi elaborarea Cererilor de rambursare;
- Managementul financiar al proiectului;
- Arhivarea documentaţiei proiectului;

Managementul de proiect este o activitate permanentă, care se derulează pe întreaga perioadă de desfăşurare a proiectului.

6.1.Activităţi

Activităţile menţionate în cele ce urmează, trebuie considerate ca fiind cerinţe minime, iar dacă alte activităţi relaţionate sunt necesare în vederea realizării obiectivelor contractului, acestea vor face parte din responsabilitatea Consultantului pentru managementul proiectului.

În cadrul proiectului, principalele acţiuni de management de proiect unde Consultantul va fi implicat, sunt următoarele:

6.1.1. Management financiar

- Elaborarea unui registru de cheltuieli pentru înscrierea cronologică a tuturor cheltuielilor efectuate, defalcate în cheltuieli eligibile şi cheltuieli neeligibile, precum şi a detaliilor documentelor justificative şi a datelor efectuării plăţilor, în vederea gestionării eficiente a bugetului alocat, până la rambursarea sumelor solicitate;
- Monitorizarea cheltuielilor din cadrul proiectului în comparație cu cheltuielile planificate;
- Elaborarea cererilor de rambursare, precum şi a rapoartelor financiare ale proiectului. Vor fi elaborate 2 cereri de rambursare intermediară în lunile 10 si 14 de implementare a proiectului si o cerere de rambursare finală în luna 18 de proiect.
- Pregătirea dosarului de rambursare în conformitate cu cerinţele specificate în contract, conţinând toate documentele justificative necesare verificării eligibilităţii cheltuielilor efectuate.
- Asigurarea activităţilor de management financiar pentru îndeplinirea de către Beneficiar a tuturor obligaţiilor şi condiţiilor prevăzute în Contractul de finanţare. Activităţile specifice care se vor derula în acest sens vor include:
    - Elaborarea previziunilor privind fluxurile de plăţi şi a graficului de rambursare astfel încât să fie respectate condiţiile impuse în Contractul de finanţare;
    - Verificarea documentelor de plată depuse în cadrul contractelor de prestare de servicii.

6.1.2. Elaborarea rapoartelor de progres

- Elaborarea rapoartelor de progres, în conformitate cu cerinţele prevăzute în Ghidul Solicitantului şi în Contractul de finanţare, care vor fi depuse în termenele stabilite conform contractului, împreună cu celelalte documente solicitate în mod expres în contractul de finanţare. Rapoartele vor fi elaborate conform prevederilor contractuale, şi vor fi suficient de detaliate, astfel încât să furnizeze o imagine clară asupra progresului înregistrat de proiect, atât din punct de vedere tehnic cât şi financiar;
- Elaborarea oricăror alte rapoarte solicitate în Ghidul Solicitantului și de către Beneficiar.

Evaluarea şi raportarea rezultatelor finale va consta în aprecierea periodică a măsurii în care au fost atinse obiectivele şi s-au obţinut rezultatele preconizate, utilizând resursele prevăzute în proiect. În acest sens, Consultantul va întocmi rapoarte pe întreaga perioadă de derulare a contractului, care trebuie să acopere toate activităţile proiectului şi vor puncta toate rezultatele obţinute.

Se vor elabora urmatoarele rapoarte de progres:

- 3 Rapoarte de progres care insotesc cererile de rambursare intermediare;
- 4 rapoarte de progres trimestrial;

- Rapoarte lunare de activitate;
- 1 Raport de progres final - acesta va fi transmis înainte de încheierea duratei de implementare a proiectului și va însoți ultima cerere de rambursare.

Conţinutul rapoartelor trebuie sa respecte întocmai cerinţele specificate în Ghidul Solicitantului şi în Contractul de finanţare. Acestea vor fi depuse la Beneficiar la termenele stabilite conform Ghidul Solicitantului şi contractului, împreună cu cererile de rambursare şi toate celelalte documente solicitate în mod expres în contractul de finanţare.

Rapoartele trebuie sa contina o pagină iniţială ce va include: numele contractului, codul contractului sau referinţe, titlul raportului, data emiterii şi perioada acoperită, numele şi adresa Furnizorului.

Alte rapoarte:

- Raportul iniţial - în termen de maxim 20 de zile de la data intrării în vigoare a contractului. Acest raport va detalia acţiunile necesare realizării activităţilor din contract, precizând lista detaliată a livrabilelor (rapoartelor) aferente fiecărei acţiuni şi termenele de livrare, ce vor fi monitorizate de Beneficiar. Raportul va cuprinde de asemenea pe lângă activităţile derulate, principalele constatări privind situaţia existentă, problemele critice identificate şi principalele măsuri care se impun pentru rezolvarea acestora, precum şi informaţiile necesare referitoare la strategia şi planul de acţiune al dezvoltării proiectului. Ca anexă se prezintă programul de activitate al Consultantului. Orice modificări ulterioare ale acestui program vor trebui supuse aprobării Beneficiarului;
- Rapoartele lunare de activitate - în termen de maxim 5 zile lucrătoare de la sfârşitul fiecărei luni, cu prezentarea detaliată a acţiunilor realizate conform planului de activităţi şi graficului de implementare ale Proiectului în luna respectivă şi activităţile care urmează să fie realizate în luna imediat următoare;
- Rapoarte ad-hoc – în maxim 5 zile lucrătoare de la solicitarea Beneficiarului, dacă va fi cazul.

Predarea şi acceptanţa rapoartelor

Toate rapoartele vor fi întocmite în limba română şi vor fi transmise spre aprobarea Beneficiarului. Beneficiarul va aproba rapoartele sau va prezenta observaţiile sale în termen de maxim 5 zile lucrătoare de la data primirii fiecărui raport (10 zile lucrătoare pentru raportul final). Consultantul va opera modificări în rapoarte, corespunzător observaţiilor Beneficiarului, în termen de maxim 5 zile lucrătoare de la data primirii acestora. Beneficiarul va proceda la acceptarea sau respingerea rapoartelor, după caz, în termen de 5 zile lucrătoare de la data primirii acestora în forma revizuită.

Notă: *Dacă durata de implementare a contractului este modificată (prin prelungire sau reducere) pentru motive independente de voinţa parţilor, atunci numărul livrabilelor va fi actualizat în funcţie de perioada contractuală şi graficul de predare al rapoartelor, fără costuri suplimentare.*

6.1.3. Arhivarea documentelor aferente proiectului

Conform regulamentelor comunitare, circuitul auditului (pista de audit) reprezintă stabilirea fluxurilor informaţiilor, atribuţiile şi responsabilităţile referitoare la acestea, precum şi arhivarea documentaţiei justificative complete pentru toate stadiile desfăşurării unei acţiuni, care să permită totodată reconstituirea operaţiunilor de la suma totală până la detalii individuale şi invers. Pista de

audit este deci o înregistrare cronologică a activităţilor din proiect pentru a permite reconstrucţia şi examinarea succesiunii de evenimente şi/sau schimbări. În acest sens, trebuie sa fie întreprinse următoarele măsuri:

- Pregătirea şi asigurarea unei piste de audit adecvată prin măsuri de păstrare şi arhivare a documentelor astfel încât acestea să nu fie alterate de factorul uman şi de timp, prin întreprinderea următoarelor activităţi:
    - Exemplarele originale ale facturilor şi documentelor care atestă efectuarea plăţilor vor fi păstrate de către beneficiar, la locaţia proiectului;
    - Documentele elaborate în cadrul proiectului vor fi păstrate astfel: 1 exemplar original şi 1 copie în format fizic, cât şi în variantă electronică;
    - Rapoartele, cererile de rambursare şi alte documente oficiale solicitate de către OIPSI vor fi elaborate în original şi în numărul de copii stabilite prin contractul de finanţare, care vor fi predate la OIPSI, câte o copie certificată a acestora păstrându-se la sediul proiectului;
    - Arhivarea se va face la finalizarea proiectului, dosarul complet cu documentele în original vor fi păstrate într-un spaţiu protejat, împreună cu un CD/DVD cu toate documentele scanate, acesta rămânând la locaţia proiectului pe perioada legală de arhivare şi păstrare (5 ani post-implementare).

6.1.4. Alte activităţi

- Monitorizarea permanentă a proiectului și a tuturor activităţilor proiectului și elaborarea de rapoarte lunare de stare cu privire la derularea activităţilor proiectului;
- Managementul timpului prin planificarea activităţilor proiectului pentru încadrarea în graficul de implementare aprobat prin Contractul de finanţare, precum și monitorizarea progresului in cadrul proiectului, comparat cu planificarea prin cuantificarea unitatilor de timp/efort care au fost alocate pentru fiecare activitate din cadrul proiectului;
- Managementul riscurilor (identificare, analiză, planificare, urmărire) prin întreţinerea unui Registru de Riscuri şi planificarea măsurilor de prevenire şi reducere a impactului riscurilor;
- Managementul acceptanței prin oferirea de suport Autorității Contractante cu privire la obținerea acceptanțelor pentru toate livrabilele (partială și finală);
- Managementul calităţii prin întreţinerea unui Registru de Calitate în care să se înscrie toate problemele apărute pe durata derulării proiectului (în cadrul testelor de acceptanţă) şi prin urmărirea rezolvării acestor probleme;
- Managementul problemelor;
- Asistență în vederea atingerii indicatorilor de performantță ai proiectului;
- Transferul de cunoştinţe în domeniul managementului de proiect către membrii echipei de proiect din partea Beneficiarului;
- Managementul schimbării prin pregătirea şi aplicarea unei proceduri de tratare a cererilor de schimbare prin care să se asigure introducerea controlată a schimbărilor în cadrul ciclului de analiză-proiectare-dezvoltare-implementare-testare-acceptanţă;
- Managementul comunicării prin punerea în aplicare a unui plan de comunicare de proiect;

- Asistență pentru asigurarea managementului contractelor din cadrul proiectului, în colaborare cu Beneficiarul;
- Elaborarea oricăror altor documente, precum notificări, acte adiţionale, clarificări, modificări de grafic de execuţie sau grafic de rambursare etc., dacă îi este solicitat.

6.2.Obligaţiiile Consultantului

Rolul Consultantului trebuie fie, pe lângă asigurarea suportului către Beneficiarul proiectului pentru implementarea în bune condiţii a proiectului, şi să asigure transferul de cunoştinţe în domeniul managementului de proiect către membrii echipei de proiect.
Responsabilităţile Consultantului în cadrul contractului de consultanță sunt cel puțin următoarele:

- Execuţia la timp a activităţilor stabilite în contract cu suportul nemijlocit al Beneficiarului;
- Acordarea suportului solicitantului pentru implementarea în condiţii optime a proiectului cât şi know-how-ul în domeniul managementului de proiect, prin prezenţa sa ori de câte ori este nevoie la locaţia proiectului, ceea ce va acţiona în direcţia consolidării competenţelor echipei de proiect din partea instituţiei solicitante în sfera managementului de proiect;
- Păstrarea confidenţialitaţii tuturor informaţiilor şi datelor la care a avut acces în cadrul proiectului. Toate informaţiile şi datele culese în cadrul acestui contract vor putea fi publicate doar cu aprobarea scrisă a Beneficiarului;
- Gestionarea contractului şi asigurarea legăturii cu celelalte contracte din cadrul proiectului prin raportarea la celelalte activităţi ale proiectului, astfel încât acesta din urmă să fie implementat conform Contractului de finanţare;
- Furnizarea, în timp util, a informaţiilor. Consultantul trebuie să îşi asume responsabilitatea pentru pregătirea tuturor documentelor, materialelor, redactării de documente clare şi solicitări precise de date, indicând data la care aşteaptă informaţiile solicitate, luând în calcul timpul de răspuns necesar pentru Beneficiar, astfel încât să nu se afecteze suplimentar programul de lucru al Beneficiarului şi respectiv, implementarea contractului conform calendarului stabilit;
- Elaborarea tuturor documentelor cu respectarea cerinţelor prevăzute de Contractul de finanţare, Ghidul solicitantului şi legislaţia în domeniu;
- Furnizarea unei echipe de experţi calificaţi, pentru a realiza sarcinile cerute prin acest Caiet de sarcini.

7. RESURSE

7.1.Personal și instruire

Instruirea trebuie sa se realizeze de către contractorul serviciilor de dezvoltare sistem SIMISC și trebuie sustinuta în limba română, furnizorul de instruire urmând a emite certificate de participare pentru toţi cursanţii.

Activitățile de instruire trebuie sa includa trei tipuri de utilizatori ai sistemului:

- Administratori – trebuie sa beneficieze de nivelul tehnic cel mai ridicat din punct de vedere al cunoştinţelor disemniate pe durata instruirii. La finalul perioadei de

instruire, administratorii, în calitate de responsabili ai activității de mentenanță după finalizarea implementării, este necesar ca administratorii SIMISC să poată asigura cel puțin desfășurarea următoarelor activități:

- Administrarea nomenclatoarelor generale şi a celor specifice activităților operative ale MAE;
- Administrarea modulului de securitate şi a drepturilor utilizatorilor; configurarea rapoartelor;
- Administrarea serverului de aplicaţie;
- Administrarea instrumentelor de back-up/recovery;
- Administrarea instrumentelor de arhivare/ restore;
- Analiza performanţelor sistemului şi tunning-ul sistemului prin intermediul statisticilor serverului de baze de date şi de aplicaţie şi prin schimbarea diverşilor parametri ai sistemului.

- Utilizatori cheie – trebuie sa beneficieze de un nivel tehnic mediu din punct de vedere al cunoştinţelor disemniate pe durata instruirii. Metoda de instruire utilizată pentru acest tip de utilizatori trebuie sa respecte principiile metodologiei "Train of trainers" (formare de formatori), având în vedere că ulterior finalizării perioadei de implementare a proiectului, utilizatorii cheie vor avea responsabilitatea de instruire a noilor utilizatori ai sistemului. De asemenea, la finalul perioadei de instruire, este necesar ca utilizatorii cheie ai SIMISC să poată asigura cel puțin desfășurarea următoarelor activități:
  - Instruirea noilor utilizatori finali;
  - Adăugarea/modificarea/ştergerea datelor în cadrul sistemului;
  - Gestionarea nomenclatoarelor;
  - Consultarea rapoartelor specifice;
  - Generarea de rapoarte dinamice, altele decât cele predefinite și construite de către furnizor.
- Utilizatori finali – vor beneficia de un nivel tehnic corespunzător necesarului de cunoştinţe în vederea operării curente a soluției implementate.

Tip instruire	Număr utilizatori	Durata instruire
Instruirea utilizatorilor finali	140	20 sesiuni de instruire, 1 zi/sesiune de instruire
Instruire utilizatori cheie	20	2 sesiuni de instruire, 3

		zile/sesiune de instruire
Instruire administratori	5	1 sesiune, 3 zile/sesiune de instruire

De asemenea, furnizorul serviciilor de instruire trebuie sa puna la dispoziţia utilizatorilor o documentaţie de instruire în limba română, atât în format fizic, cât și în format electronic, care trebuie sa includa materiale în limba română, pe categorii de utilizatori:

- Manuale/ghiduri de administrare pentru persoanele care vor administra sistemul;
- Manuale/ghiduri de configurare și manuale/ghiduri pentru instruire pentru persoanele care vor asigura instruirea noilor utilizatori ai aplicației;
- Manuale/ghiduri de utilizarepentru utilizatorii ce vor asigura operarea curentă a soluției implementate.

Ofertantii trebuie sa prezinte procedura dupa care vor realiza instruirea utilizatorilor. Procedura de training trebuie sa contina cel putin urmatoarele informatii:

- Descrierea cursurilor si a rezultatelor asteptate;
- Modalitatea de evaluare a cursurilor;
- Modalitatea de evaluare a cursantilor;
- Formulare utilizate.

Ofertantul declarat castigator va avea obligatia de a asigura salile de instruire dotate corespunzator, cateringul pentru fiecare zi de curs, transportul, cazarea si cheltuielile aferente instructorilor in locatiile indicate de catre Beneficiar pentru realizarea instruirii. Costurile de deplasare, cazare, diurne si transport pentru cursanti vor fi asigurate de catre Beneficiar.

Pentru a asigura posibilitatea de instruire continua indiferent de fluctuatia de personal a beneficiarului, ofertantul trebuie sa furnizeze cursurile de instruire a utilizatorilor si in format SCORM pentru a putea fi importate in solutiile de e-learning comune.

7.2.Resurse materiale

Resursele materiale deţinute de catre Beneficiar şi utilizate pentru buna implementare a proiectului sunt:

- Sediul solicitantului, precum și dotările necesare pentru întâlnirile echipei de proiect și desfășurării activităților acestora;
- Baza logistica: mobilier (birouri, scaune, dulapuri pentru o parte din membrii echipei) și echipamente IT (8 calculatoare și 3 imprimante);

- Mijloacele de comunicație (telefonie fixă, fax și conexiune internet);
- Site-ul solicitantului (www.mae.ro), pentru o comunicare și promovare eficienta și completă a rezultatelor proiectului;
- Lista de contacte ale solicitantului;
- Mijloace necesare pentru desfășurarea programelor de instruire „in house" (sala de training, videoproiector, planșa de proiecție, etc.).

7.3.Cerinţe minime de personal

Atât Furnizorul cât şi Beneficiarul trebuie să asigure cadrul profesional adecvat desfăşurării proiectului în bune condiţii. Fiecare va pune la dispoziţie toţi specialiştii necesari pentru îndeplinirea scopului şi obiectivelor proiectului.

Furnizorul are obligaţia de a propune spre mobilizare o echipă formată din experţi calificaţi pentru realizarea activităţilor prevăzute în caietul de sarcini si va fi responsabil pentru activitatea experţilor şi pentru obţinerea rezultatelor contractului. Experţii propuşi vor avea calificarea şi experienţa profesională necesare pentru acoperirea cu succes a tuturor activităţilor indicate în caietul de sarcini. Astfel, Furnizorul va pune la dispoziţia autorităţii contractante o echipă formată din personal cu competenţe şi experienţă dovedite, capabil să ducă la bun sfârşit cu succes sarcinile definite prin prezentul caiet de sarcini, astfel ca, în final, să contribuire la îndeplinirea obiectivului general şi a obiectivului specific ale proiectului, în condiţiile respectării cerinţelor de calitate şi a termenelor stabilite şi încadrarea în bugetul prevăzut.

Echipa de proiect va fi formată cel puţin din specialistii cheie nominalizati in cadrul fisei de date a achizitiei.

7.4.Responsabilităţile experţilor principali

Responsabilitățile experților din echipa de implementare a sistemului informatic sunt prezentate in cele ce urmează:

Manager de proiect:

- Managementul proiectului conform unei metodologii recunoscute, respectiv activitati de organizare a proiectului, planificare, executie, monitorizare, control si inchidere a proiectului;
- Coordonarea echipei de implementare a sistemului informatic pentru realizarea activităţilor de analiza, design, dezvoltare, configurare, testare, implementare, integrare, instruire, asistenţă tehnică, etc.;
- Punct principal de contact pentru comunicarea cu Beneficiarul;

- Implementarea si gestiunea calităţii serviciilor IT în raport cu necesităţile proiectului si ale Beneficiarului;
- Alocarea resurselor proiectului împreună cu coordonatorii tehnici de proiect;

Arhitect sistem informatic

- Colaborarea cu factorii de răspundere, experții în materie și personalul implicat în proiect, pentru a defini arhitectura de tip enterprise a soluției în conformitate cu strategia instituției, procesele, informațiile și tehnologia potrivit conceptelor architecturii de tip enterprise;
- Definirea arhitecturii de integrare a componentelor sistemului;
- Definirea arhitecturii de securitate a sistemului;
- Identificarea riscurilor și a problemelor tehnice precum și a soluțiilor de rezolvare a acestora.

Analist de sistem

- Analiza proceselor de lucru (business analysis) conform unei metodologii de lucru recunoscute;
- Analiza procedurilor și a regulamentului de organizare și funcționare al Beneficiarului în vederea stabilirii funcționalităților sistemului;
- Participarea la ședințele de analiză cu responsabilii din partea Beneficiarului;
- Realizarea documentației de analiză și specificații a soluției;
- Realizarea de analize spatiale si generalizare avansată în asistarea procesului decizional din cadrul institutiei;
- Definirea unor procese pentru centralizarea datelor spatiale din diferite surse, si automatizarea unui flux de lucru de analiza;
- Realizarea manualelor de utilizare a soluției;
- Suport pentru utilizatorii cheie din partea Beneficiarului în timpul testelor funcționale;

Expert dezvoltare portal

- Dezvoltare aplicatii software pe baza documentelor de analiza, specificatii functionale, specificatii tehnice, arhitectura sistem;
- Dezvoltarea aplicatiilor WEB;
- Testare unitara (interna);

- Suport acordat utilizatorilor cheie pentru testarea functionala;
- Rezolvare disfuncționalități (bug-uri);

Expert implementare soluție de analiză şi raportare

- Analiza datelor şi necesităţilor de analiză şi raportare pe baza analizei generale de business;
- Crearea modelelor de date/metadate pentru analiză si raportare;
- activităţi de proiectare, dezvoltare şi implementare a soluţiei de analiză si raportare;
- Instalarea şi configurarea soluţiei de analiză si raportare;
- Dezvoltarea rapoartelor;
- Documentarea pentru utilizarea soluţiei de analiză și raportare.

Expert administrare baze de date

- Realizare tuninig şi optimizare baze de date;
- Implementarea strategiei pentru copii de siguranţă şi recuperarea datelor, elaborarea procedurilor de recuperare;
- îmbunătăţirea performanţelor bazelor de date şi realizarea configurărilor de detaliu;
- Diagnosticarea problemelor bazelor de date şi repararea acestor probleme;
- Supervizarea testelor bazei de date;
- Suport pentru solutionarea problemelor tehnice si functionale la nivelul bazelor de date;
- Integrarea componentelor sistemului cu baza de date;
- Importul si exportul de date necesar pentru iniţializarea sistemului folosind instrumentele bazei de date si limbajul SQL

Expert testare sisteme informatice

- Planificarea activităţilor de testare;
- Testarea funcţionalităţilor sistemelor dezvoltate şi implementate conform unei metodologii de testare recunoscută;
- Elaborarea planurilor, scenariilor şi cazurilor de test;
- Livrarea rapoartelor de testare;

- Coordonarea activităţilor de testare ale echipei de testare;
- Realizarea testelor de acceptanţă specifice;
- Asigurarea că sistemul funcţionează corect din punct de vedere al respectării cerinţelor, consistenţei datelor, al constrângerilor de timp, al validărilor de date şi al gestiunii erorilor, inclusiv pentru funcţionalităţile existente care au fost extinse sau modificate.

Expert securitate sisteme informatice si infrastructura IT

- Implementarea echipamentelor de securitate informatică;
- Evaluarea sistemului implementat pentru conformitate cu standardele deschise de securitate informatică;
- Planificarea activităţilor de testare în ceea ce priveste asigurarea securității soluției;
- Evaluarea vulnerabilităților sistemului implementat;
- Actualizarea manualului de securitate și a procedurilor de securitate ale Beneficiarului;
- Identificarea și exploatarea controlată a vulnerabilitatilor sistemului înainte de punerea în producție;
- Teste de penetrare pentru componenentele expuse la internet;

Expert arhitect infrastructura hardware

- Contribuie la întocmirea planurilor de instalare și punere în funcţiune a sistemului;
- Instalarea și configurarea echipamentelor hardware livrate;
- Supervizarea funcţionării echipamentelor în perioada testelor;
- Suport pentru solutionarea problemelor tehnice pentru echipamentele hardware;
- Elaborarea documentaţiei cu privire la echipamentele hardware inclusiv a documentaţiei de administrare;
- Crearea arhitecturii generale hardware luând în considerare echipamentele ofertate şi reţeaua existentă la beneficiar;
- Proiectarea detaliată a arhitecturii reţelei pentru sistemul implementat;
- Elaborarea planului de instalare şi configurare în raport cu constrângerile tehnice şi corelat cu componente software ale sistemului;
- Elaborarea documentaţiei de configurare a tuturor elementelor reţelei pentru sistemul informatic;

- Documentarea arhitecturii sistemului.

Responsabilităţile experţilor din echipa de implementare a proiectului sunt prezentate în cele ce urmează:

Manager de proiect

- Monitorizarea implementării proiectului;
- Elaborarea planului revizuit de activităţi şi identificarea principalelor jaloane (milestones) ale proiectului, precum şi înaintarea spre aprobare Coordonatorului de proiect propus de Solicitantul finanțării;
- Elaborarea Rapoartelor de progres ce vor fi semnate de către Coordonatorul de proiect şi înaintate spre aprobare către O.I.P.S.I.;
- Monitorizarea managementului financiar, incluzând verificarea cheltuielilor;
- Elaborarea sistemului de arhivare a documentelor şi asigurarea pistei de audit aferente;
- Asistenţă în elaborarea cererilor de rambursare;
- Coordonarea activităţilor de informare şi publicitate aferente fiecărei etape a proiectului;
- Asigurarea accesului uşor la documentaţia proiectului în vederea realizării auditurilor financiare şi tehnice parţiale şi finale.
- Asigura coordonarea implementarii Sistemului Informatic pentru Managementul Integrat al Serviciilor pentru Cetateni

Manager financiar

- Elaborarea, împreună cu Coordonatorul de proiect, a planului de cheltuieli;
- Verificarea disponibilităţii resurselor financiare necesare iniţierii proiectului;
- Verificarea cheltuielilor;
- Verificarea aspectelor financiare ale contractelor de achiziţii publice;
- Elaborarea dosarului de rambursare;
- Contribuţie la elaborarea rapoartelor de progres;
- Asigurarea accesului la documentaţia financiar-contabilă pentru auditorul extern;
- Transfer de cunoştinţe specifice de management financiar către echipa de implementare;

Experti IT

- Participarea la recepţia echipamentelor hardware achiziţionate;
- Monitorizarea activităţilor de implementare a soluţiei/soluţiilor software achiziţionate;
- Raportarea către Managerul de proiect şi către Coordonatorul de proiect privind implementarea sistemului informatic.

Note:

1. Furnizorul este responsabil de organizarea experţilor, componența echipelor de experţi, profilul generic al acestora și efortul estimat. Experții echipei de proiect au fost stabiliți la un nivel minim prin raportare la durata de execuție a contractului maxim acceptată, sens în care operatorii economici vor asigura corelarea propunerii tehnice și a calendarului de implementare a contractului cu echipa de proiect propusă, suplimentând după caz componenta acesteia cu un personal de suport adecvat, astfel încât pe baza documentelor prezentate să rezulte fezabilitatea/sustenabilitatea propunerii tehnice. Toți membrii echipelor de implementare trebuie să fie vorbitori de limba romană. Furnizorul poate utiliza și experți care să lucreze în alte limbi cu condiția să aibă suficienți traducători pentru limba romană. Prin urmare, se pot utiliza și alti experti (non-cheie) pentru a completa echipa, dar aceștia vor trebui să lucreze sub îndrumarea experților cheie. Astfel, este răspunderea ofertanților de a furniza orice personal auxiliar necesar, pentru asigurarea îndeplinirii corespunzătoare a obligațiilor contractuale pe toată durata acestui contract. Pentru acești experți, ofertantul va prezenta rolul și responsabilitățile acestora.

2. Furnizorul se obligă să respecte legislația în vigoare care reglementează condițiile la locul de muncă pe parcursul elaborării ofertei și derulării Contractului. Furnizorul va realiza prevederile contractuale cu respectarea principiului egalității de șanse și dezvoltării durabile.

3. Furnizorul trebuie să asigure:

- *Sprijinul și echipamentele adecvate (hardware și software) pentru toți experții;*
- *Servicii administrative suficiente, de secretariat și de interpretare, pentru a da posibilitatea experților să se concentreze asupra responsabilităților principale;*
- *Spațiul de lucru aferent desfășurării activităților experților principali și secundari (dacă este cazul);*
- *Consumabilele de birou.*

8. IMPLEMENTAREA SISTEMULUI INFORMATIC

8.1. Activitatea de management de proiect pentru implementarea sistemului informatic

Activitatea de management de proiect trebuie să se desfasoare conform unui cadru (framework) de management de proiect recunoscut international de către organisme profesionale specifice de Project Management.
Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei proprii de management de proiect pe care o va utiliza în cadrul proiectului.
Ofertantul trebuie să prezinte în cadrul propunerii tehnice planul de proiect pentru prestarea serviciilor pe toată durata contractului. Planul de proiect trebuie să conțină toate activitățile precum și etapele/subetapele determinante de realizare a activităților, dependentele dintre activități, jaloanele de proiect (milestones), rezultatele activităților si alocarea resurselor în vederea prestării serviciilor ofertate astfel încat sa fie atinse obiectivele proiectului. Ofertantul trebuie să propună planul de proiect cât mai detaliat posibil și să răspundă cerințelor de etapizare și înscriere în termenele de realizare ale proiectului. În perioada de inițiere a proiectului, ulterior semnării contractului, planul de proiect poate fi modificat doar cu aprobarea Beneficiarului.
Implementarea intregului sistem trebuie să acopere următoarele:

- Analiza;
- Proiectare;
- Dezvoltare/configurare inclusiv testare interna;
- Implementare (deployment);
- Testare si teste de acceptanta;
- Intrarea in productie.

Planul care va fi prezentat impreuna cu oferta trebuie sa acopere toate tipurile de activitati mentionate mai sus.
Ofertantul trebuie sa prezinte in cadrul propunerii tehnice modalitatea in care se va realiza raportarea progresului pentru activitatile din cadrul proiectului.
Ofertantul trebuie sa prezinte in cadrul proiectului modalitatea prin care se va realiza comunicarea intre participantii la proiect.
Ofertantul va prezenta in cadrul propunerii tehnice modul in care se va gestiona rezolvarea problemelor care pot sa apara pe parcursul proiectului. Se va descrie procesul de management al problemelor si formularele care vor fi utilizate pentru managementul problemelor, escaladarea si rezolvarea acestora.
Ofertantul va prezenta in cadrul propunerii tehnice planul de acceptanta care va fi utilizat in cadrul proiectului pentru receptiile/acceptantele partiale si receptia/acceptanta finala. Se va prezenta planul impartit pe etape precum si formularele aferente receptiilor/acceptantelor partiale si receptiei/acceptantei finale.
Ofertantul va prezenta in cadrul propunerii tehnice si modalitatea de tratare a schimbarilor in cadrul proiectului. Se va prezenta procedura de management al schimbarilor precum si formularele care vor fi utilizate in cadrul acestui proces pe durata proiectului.
Avand in vedere complexitatea si durata proiectului, ofertantii trebuie sa ia in considerare necesitatea prestarii unui numar corespunzator de zile-om pentru activitatile proiectului prin

alocarea expertilor necesari. In vederea atingerii obiectivelor proiectului, furnizorul poate suplimenta numarul de resurse alocat activitatilor pe perioada derularii proiectului.

- Planul de management al riscurilor – Aceasta sectiune va contine cel putin urmatoarele: identificarea, descrierea si argumentarea riscurilor care pot afecta executia contractului;
- recomandari de reducere/eliminare a riscurilor identificate, fara afectarea cerintelor caietului de sarcini.

8.2.Analiza

Rolul principal al fazei de analiza este de a intelege corect nevoile utilizatorilor inainte de proiectarea si implementarea unui sistem care sa le indeplineasca.
In vederea implementarii sistemului, furnizorul va trebui sa execute activitati de analiza care sa asigure premizele unei implementari eficiente. Informatiile care stau la baza procesului de analiza sunt:

- Contractul, pentru termene si conditii;
- Caietul de sarcini si propunerea tehnica, pentru aria de acoperire a proiectului;
- Cerintele clientului colectate si evaluate in timpul acestei faze.

Beneficiarul va acorda tot sprijinul necesar pentru intelegerea cat mai buna si completa a contextului in care va fi implementat sistemul.
Ofertantii trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapei de analiza.
Analiza se va efectua dupa caz la sediul Beneficiarului sau la Furnizor si va avea ca finalitate un pachet de specificatii functionale agreat de comun acord cu acesta.

Proiectare

Rolul principal al fazei de proiectare este de a descrie la un nivel suficient de detaliu sistemul care urmeaza a fi implementat.
In vederea implementarii sistemului, Furnizorul va trebui sa execute activitati de proiectare care sa asigure premizele unei implementari eficiente.
Proiectarea sistemului trebuie sa ofere o solutie optima, urmarindu-se usurinta si eficienta realizarii si implementarii solutiei, in cadrul restrictiilor de ordin tehnic, organizatoric sau financiar. In procesul de proiectare, implicarea Beneficiarului este esentiala in confirmarea cerintelor informationale si a prioritatilor din organizatie, realizandu-se in acest mod intelegerea si pregatirea pentru acceptanta noului sistem. De aceea, este esential ca Furnizorul sa comunice frecvent cu echipa Beneficiarului pe tot parcursul derularii proiectului.
Documentul/documentele de specificatii, rezultate in urma activitatilor de analiza si proiectare, vor descrie Soluția in detaliu, vor contine informatii privind toate functionalitatile necesare si vor sta la baza stabilirii si realizarii testelor de acceptanta.
In urma activitatilor de analiza si proiectare, pentru a se obtine un sistem final operational se vor desfasura activitati de dezvoltare, configurare, testare si implementare (deployment).

8.3.Dezvoltare, configurare și testare internă

Ofertantii trebuie sa descrie in detaliu metodologia dupa care vor derula activitatile de dezvoltare/configurare si testare interna si vor demonstra integrarea acestor proceduri cu procedurile de analiza si proiectare.

Ofertantii trebuie sa prezinte instrumentele folosite in desfasurarea activitatilor de dezvoltare, configurare si testare interna.
Ofertantii trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapelor de dezvoltare/configurare si testare interna.

8.4.Implementare

Ofertantii trebuie sa descrie in detaliu metodologia dupa care vor derula activitatile de implementare (deployment).
Ofertantii trebuie sa prezinte impreuna cu oferta procedurile de implementare din cadrul propriei organizatii si vor demonstra integrarea acestor proceduri cu procedurile referitoare la dezvoltare/configurare si testare interna.
Ofertantii trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapei de implementare.

8.5.Teste de acceptanță

Ofertantii vor prezenta in detaliu metodologia si procedurile dupa care vor derula activitatile specifice de testare de acceptanta. Metodologia va fi adaptata specificului acestui proiect.

Ofertantii vor demonstra ca metodologia propusa si procedurile pe care le vor utiliza acopera integral tematica proiectului astfel incat sa fie posibila testarea tuturor functionalitatilor identificate in etapa de analiza si proiectare.

In cadrul contractului Ofertantul va trebui să deruleze cu Autoritatea Contractanta mai multe etape de inspecții și teste în vederea recepționării și acceptării produselor, serviciilor și lucrărilor. În vederea clarificării modului în care Autoritatea Contractantă înțelege derularea proceselor de mai sus aceasta a definit în continuare următorii termeni:

1. Recepția : Procesul prin care un produs sau un livrabil sau un serviciu sau o lucrare este acceptat sau respins de catre o comisie nominalizata a Autorității Contractante. Acceptarea/Respingerea se va constata prin emiterea de catre Autoritatea Contractanta a documentului denumit „**proces verbal de recepție**” din care va rezulta ce se acceptă / respinge și criteriile în baza carora comisia a decis aprobarea/respingerea produsului sau livrabilului sau serviciului sau lucrarii. În cadrul fiecarei etape/fază se va derula cel putin o recepție sau dacă este cazul mai multe recepții aferente produselor / livrabilelor / serviciilor / lucrărilor iar fiecare astfel de recepție va fi documentată corespunzător. În cazul in care Autorității Contractante emite un proces verbal de recepție prin care respinge o livrare a Ofertantului atunci Autoritatea Contractanta va enunța în document în clar motivul/motivele pentru care respinge livrarea. Ofertantul are obligația de a reface / înlocui pe cheltuia proprie și de a solicita o noua recepție. În cadrul noului proces de recepție Autoritatea Contractanta va putea emite noi observații doar la punctele la care anterior a emis observații.

2. Acceptanta Provizorie: Este data (momentul în timp) la care Autoritatea Contractanta emite catre Ofertant documentul “**proces verbal de acceptanță provizorie**”. Documentul va fi emis în baza tuturor proceselor verbale de recepție care au fost aprobate. Documentul va atesta că Ofertantul și-a indeplinit toate obligațiile rezultate din caietul de sarcini, că toate produsele au fost livrate, că toate serviciile au fost prestate și că toate lucrările au fost recepționate iar de la această dată începe

perioada de garanție și suport în perioada de garanție. Documentul "**proces verbal de acceptanță provizorie**" nu va fi emis daca un produs sau un livrabil sau un serviciu sau o lucrare a fost respins de catre Autoritatea Contractanta și ulterior nu a mai fost acceptat/aprobat printr-un nou proces verbal de recepție.

3. Acceptanta Finală: Este data (momentul în timp) la care Autoritatea Contractanta emite catre Ofertant documentul "proces verbal de acceptanță finală". Documentul va fi emis în baza procesului verbal de acceptanță provizorie și în baza proceselor verbale de recepție aprobate de catre Autoritatea Contractantă pentru fiecare luna din perioada de garanție.

8.6.Intrarea în producție

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

Planul prezentat trebuie sa țină cont de legaturile logice între subsisteme astfel încât să se asigure de o trecere in producție coerenta și cu impact minim în derularea activităților operationale ale Achizitorului.

8.7.Suport în perioada de garanție

Ofertantii trebuie sa descrie in detaliu metodologia dupa care vor derula activitatile de suport în perioada de garanție.

Ofertantii trebuie sa prezinte impreuna cu oferta procedurile si instructiunile de lucru de suport din cadrul propriei organizatii.

Ofertantii trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapei de suport. Descrierea trebuie sa contina cel putin urmatoarele informatii:

- Formularul/formularele care vor fi utilizate pentru fiecare livrabil;
- Descrierea continutului fiecarui livrabil;
- Modul in care va fi interpretat continutul livrabilelor.

Pentru gestionarea activitatii de suport in perioada de garantie, Furnizorul trebuie să pună la dispozitia Beneficiarului o aplicatie software de gestionare a tichetelor, care să poată fi folosita de toti utilizatorii.

Timpii de răspuns (recepţionare a tichetului) sunt măsuraţi din momentul notificării unei solicitări valide transmise de către Beneficiar şi înregistrate (preluate) de Furnizor. Timpul de răspuns trebuie să fie de maxim 24 de ore indiferent de ziua din saptamana si de programul de lucru al ofertantului. Remedierea defectelor se va face respectand urmatorii timpi:

- Nivel de severitate critic (sistem total nefuncțional) – timp maxim pentru Soluția provizorie de 1 zi, si remediere de 3 zile.

- Nivel de severitate mare (disfunctionalitate ce afectează majoritatea funcţionalităţilor sistemului iar utilizarea acestuia este compromisa) – timp maxim pentru Soluția provizorie de 2 zile, si remediere de 5 zile.

- Nivel de severitate mica (disfunctionalitate care afectează o funcţie sau un proces, dar funcţionarea întregului sistem nu este afectată semnificativ) – timp maxim pentru Soluția provizorie de 3 zile, si remediere de 10 zile.

Timpii de implementare soluţie provizorie sau remediere sunt măsuraţi din momentul notificării de recepţionare transmise de către Furnizor şi momentul acceptării de către Beneficiar, exceptând timpul de aşteptare în care Beneficiarul furnizează informaţii suplimentare necesare rezolvării incidentului.

Aplicatia pentru gestionarea tichetelor trebuie sa indeplineasca urmatoarele caracteristici:

- Aplicatia trebuie sa ofere posibilitatea inregistrarii solicitarilor de suport si alocarea unui identificator unic fiecarei solicitari;
- Aplicatia trebuie sa ofere posibilitatea de definire a unor categorii de apeluri de asistenta;
- Aplicatia trebuie sa ofere posibilitatea de definire si de incadrare a solicitarilor in categorii: defect, eroare, solicitare de informatii, cerere de schimbare.
- Aplicatia trebuie sa ofere posibilitatea de inregistrare a datelor de identificare ale apelantului - include atribuirea incidentului unei persoane care raporteaza in aplicatia software (inginerul de suport), persoana care solutioneaza incidentul (de la orice nivel), persoana care a raportat un incident. Toate datele prezente aici includ atat date personale, cat si date de contact, activitate curenta etc., aceasta aplicatie putand fi personalizata sa primeasca detalii diferite pentru aceste puncte de reper in mod diferit si definit in totalitate de catre un administrator de aplicatie.
- Aplicatia trebuie sa ofere posibilitatea de inregistrare a descrierii problemei si de atasare a unor documente suplimentare. Aplicatia software să permită atasarea oricaror tipuri de fisiere (doc, xls, jpg, xml etc.) precum si postarea a unor capturi de ecran din aplicatii.
- Aplicatia trebuie sa ofere posibilitatea de alocare a unui criteriu de urgenta. Aplicatia software să permită clasificarea incidentelor in functie de tipul stabilit, putand sa emita notificari pe mail privind alocarea incidentelor catre persoanele implicate in incident.
- Aplicatia trebuie sa ofere posibilitatea de alocare automata a unor coduri de incident care sa indice cauza probabila a incidentului. Aplicatia software trebuie sa aloce coduri unice fiecarui incident. Aplicatia software trebuie să permită de asemenea si gruparea pe module a incidentelor.
- Aplicatia trebuie sa ofere posibilitatea de gestionare a informatiilor despre personalul de suport caruia i se pot aloca spre rezolvare incidentele. Aplicatia software contine implicit toate datele de contact si deci persoanele, care pot fi considerate alocabile sau care pot aloca un incident. Aceste date pot fi folosite in mod facil in cazul unui audit.
- Aplicatia trebuie sa ofere posibilitatea inregistrarii automate a datei si a orei primirii unei solicitari de asistenta.
- Aplicatia trebuie sa ofere posibilitatea de definire a criteriilor de calitate si performanta pentru rezolvarea diferitelor categorii de solicitari de asistenta.
- Aplicatia trebuie sa ofere posibilitatea de atentionare automata in momentul depasirii unor praguri temporale de rezolvare a diferitelor categorii de solicitari de asistenta.
- Aplicatia trebuie sa ofere posibilitatea de definire a unor fluxuri de evolutie a solicitarilor de suport, in cazul in care ele trec prin mai multe nivele de competenta pana in momentul finalizarii.
- Aplicatia trebuie sa ofere posibilitatea de escaladare a cererilor de suport.

- Aplicatia trebuie sa ofere posibilitatea de inregistrare a datelor de contact pentru responsabilii pentru activitatile de suport de nivel 1, 2 si 3 pentru diferitele componente ale sistemului informatic.
- Aplicatia trebuie sa ofere posibilitatea de definire a unor rapoarte personalizate folosind criterii cum ar fi: tipul de incident, nivelul de urgenta, timpul de rezolvare, persoana si locatia de unde a fost semnalat un incident, modulul sau functia care a cauzat incidentul, numarul de incidente, etc.
- Aplicatia trebuie sa ofere posibilitatea să permită in orice moment accesul la baza de date a personalului autorizat al sistemului pentru verificarea modului de tratare a incidentelor si pentru rularea de rapoarte de performanta a serviciului de suport. Accesul trebuie sa fie permis numai pentru citire si nu va fi conditionat in niciun fel de catre operatorii sau administratorii serviciului.

8.8.Asigurarea şi controlul calităţii pe durata proiectului

Serviciile solicitate pe durata contractului trebuie să asigure obţinerea rezultatelor aşteptate la un nivel calitativ adecvat.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice o descriere a procedurilor de asigurare şi control al calităţii aplicabile proceselor pe care le derulează in activitatea curentă. Se va prezenta o copie a manualului calităţii semnată de către reprezentantul legal al ofertantului.

Ofertantul trebuie să aloce în planul detaliat de implementare timpi suficienţi de verificare şi validare din punct de vedere calitativ pentru produsele livrate, serviciile prestate şi lucrările executate în cadrul contractului şi pentru revizuirea livrabilelor/documentelor rezultate. Ofertantul va lua in considerare necesitatea prestării unui număr corespunzator de zile-om pe durata proiectului, de către personalul specializat în asigurarea şi controlul calităţii prin alocarea expertilor cheie si non-cheie.

Trebuie sa fie incluse in oferta urmatoarele proceduri de lucru: Procedura de asistenta tehnica, mentenanta si suport, Procedura de livrare, Procedura de recepție/acceptanta provizorie/acceptanta finala, Procedura de sedinte, Procedura de management al schimbarii, Procedura de dezvoltare, Procedura de proiectare, Procedura de control al livrarilor, Procedura de testare a livrabilelor (inclusiv cele de tip software), Procedura de implementare sistem.

Ofertantii trebuie sa includă in oferta si varianta preliminara a planului de calitate pentru derularea proiectului. Planul de calitate trebuie sa contina cel putin urmatoarele informatii:

- Descrierea fazelorși etapelor din cadrul proiectului;
- Descrierea pachetelor de lucru si a livrabilelor rezultate in urma prestarii serviciilor;
- Descrierea criteriilor de acceptanta pentru livrabile, pachete de lucru, faze, etape, etc;
- Formulare care vor fi utilizate in cadrul proiectului.

8.9.Garanţie

Serviciile de garantie aferente proiectului trebuie sa fie asigurate de către ofertant pentru o perioadă de minim 36 de luni de la data emiterii certificatului de acceptanţă provizorie (finalizării implementării sistemului).

Garantia pentru componentele hardware din cadrul proiectului, oferita la fata locului trebuie sa fie disponibila in toate zilele lucratoare (24x7). Ofertantul castigator va trebui sa se prezinte la fata locului pentru constatarea defectiunii in maxim 4 ore de la semnalarea acesteia de catre Beneficiar, diagnosticarea defectiunii se va face in maxim 8 ore de la constatarea acesteia, iar inlocuirea sau repararea componentelor hardware defecte se va face conform SLA-ului asumat in cadrul ofertei.

Ofertantii vor descrie in oferte planul detaliat privind garantia hardware asigurata in cadrul proiectului.

In cazul defectarii enitatilor de stocare (HDD-uri), acestea nu se vor returna furnizorului ci vor fi distruse de catre beneficiar.

În cadrul perioadei de garanție se vor asigura:

- Rezolvarea erorilor software (bug-urilor) care nu au fost identificate în timpul implementării și care apar în faza de producție;
- Intreținerea și buna funcționare a sistemului furnizat în parametrii agreați (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- Update-ul automat pe intreaga perioada de garantie a bazelor de date cu semnaturi si vulnerabilitati din echipamentele si software-ul ofertat (semnaturi antivirus, semnaturi din echipamentele firewall etc.);
- Update-ul la ultima versiune de soft din echipamentele ofertate (firmware-uri etc);
- Sustinerea SLA-urilor asumate in cadrul ofertei, precum si a celor cerute in mod explicit acolo unde este cazul;
- Intervenție conform timpilor asumați în oferta tehnică pentru efectuarea tuturor reparațiilor necesare asupra produselor software dezvoltate și pentru aducerea acestora la starea operațională.
- Analiza impactului schimbărilor;
- Dezvoltarea și testarea necesare pentru implementarea corecțiilor;
- Instalarea de noi versiuni ale aplicațiilor dezvoltate în urma efectuării corecțiilor și actualizărilor;
- Actualizarea manualelor de utilizare și altor documente în urma efectuării corecțiilor acolo unde este necesar;

- Gestionarea tuturor incidentelor va fi realizată prin intermediul aplicației software de gestionare a tichetelor.

8.10. Asistenţa post implementare

Se solicita servicii de suport post-productie aferente sistemului implementat pentru o perioada de minim 36 luni (intreaga perioada de garantie ofertata) de la trecerea in productie a sistemului informatic (semnarea acceptantei provizorii).

Pentru a asigura o buna functionare a sistemului informatic, ofertantul va asigura pe durata suportului post-productie, prezenta unei echipe de specialisti la sediul Autoritatii Contractante, daca va fi cazul.

Ofertantii vor descrie detaliat in oferta tehnica modul in care vor asigura serviciile de suport post-productie pentru sistemul informatic.

8.11. Dreptul de proprietate

Dreptul de utilizare/licenţa asupra solutiei informatice dezvoltate trebuie ofertat fara nici o restrictie.

Beneficiarului ii va fi cedat dreptul de prorietate asupra codului dezvoltat in cadrul sistemului, Implementatorul neputand reutiliza codul scris fara acordul Beneficiarului.

8.12. Sustenabilitatea proiectului

Beneficiarul investiţiei, Ministerul Afacerilor Externe, este entitatea care va asigura operarea sistemului pentru o perioadă de cel puţin 5 ani după implementarea proiectului.

Ministerul Afacerilor Externe, în calitate de instituție publică cu personalitate juridică, aflat în coordonarea Ministrului Afacerilor Externe, finanțat integral de la bugetul de stat, va prevedea în procesul de fundamentare al bugetului anual sumele necesare asigurării operării şi întreţinerii solutiei la parametri optimi de funcționare.

Activităţile preconizate a se implementa în cadrul proiectului fac parte dintr-un plan de acţiune mai larg derulat de către instituţia beneficiară care vizează asigurarea unei mai bune funcţionări a instituţiei prin automatizarea activităţii interne. Acest fapt va asigura continuarea şi extinderea lor dincolo de perioada de implementare a proiectului.

Personalul instituţiei va fi instruit pentru a utiliza şi pentru a întreţine sistemul implementat, urmând a fi asigurate totodată servicii specifice de mentenanţă conform contractului încheiat cu furnizorul sistemului integrat, precum şi garanţie si suport pentru echipamentele achiziţionate prin proiect.

Serviciile de întreținere corectivă care vor fi prestate in perioada de garanției sunt compuse din:

- Rezolvarea bug-urilor care nu au fost identificate în timpul implementării şi care apar în faza de producţie;

- Intreţinerea şi buna funcţionare a sistemului furnizat în parametrii agreaţi (funcțional, performanţă, disponibilitate, integritatea datelor);
- Instalarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- Actualizarea manualelor de utilizare și a altor documente rezultate în urma efectuării corecțiilor;
- Toate incidentele vor fi gestionate prin intermediul aplicației software de gestionare a tichetelor.

Serviciile de intretinere evolutiva, sunt servicii suplimentare, ce nu sunt acoperite de bugetul acestui proiect, iar in acest caz Ministerul Afacerilor Externe va aloca din bugetul propriu sumele necesare in cazul aparitiei acestor situatii.

Serviciile de întreținere evolutivă sunt similare serviciilor prestate în perioada de implementare a proiectului și vor consta în:

- Analiză (inclusiv Analiza proceselor);
- Proiectare;
- Dezvoltare, configurare şi testare internă;
- Implementare (deployment);
- Testarea și testele de acceptanță;
- Punere în producție;
- Asigurarea și controlul calităţii pe durata contractului.
- Realizarea de actualizări periodice care vor consta în adăugarea de module noi în funcţie de necesităţile utilizatorilor;
- Extinderea aplicaţiei care va presupune asigurarea, în cadrul portalului dedicat acesteia, a unor servicii online în funcţie de necesităţile identificate în rândul utilizatorilor, astfel încât mediul online să devină mai cuprinzător;
- Reorganizarea activităţii cu ajutorul noilor tehnologii prin integrarea de noi instrumente informatice care să acopere şi alte segmente din activitatea instituţiei.

8.13. Livrabile

La finalizarea contractului de servicii, furnizorul trebuie sa:

- Predea autorităţii contractante toate echipamentele și sistemele necesare functionarii solutiei;

- Predea autorităţii contractante documentaţia aferentă acestora;
- Puna la dispoziţia beneficiarului toate înregistrarile aferente prezentului contract, pentru a fi transferate către acesta.
- Echipamentele ofertate nu trebuie sa fie la sfarsitul vietii comerciale, adica "end of life" sau "end of sale" conform informatiilor producatorului fiecarui echipament in parte.

8.14. Ofertare

Ofertanţii trebuie sa întocmeasca propunerea tehnică şi financiară cu respectarea prevederilor stabilite în cadrul fisei de date a achizitiilor din cadrul documentatiei de atribuire.

Ofertantul trebuie să răspundă punctual la toate cerinţele cuprinse în prezentul caiet de sarcini şi să detalieze în cadrul propunerii tehnice modalitatea şi mijloacele concrete prin care serviciile ofertate îndeplinesc aceste cerinţe, astfel încât comisia de evaluare să aibă posibilitatea evaluării acesteia în mod obiectiv.

Propunerea tehnică se va întocmi într-o manieră organizată, astfel încât procesul de evaluare a ofertelor să permită identificarea facilă a corespondenţei informaţiilor cuprinse în ofertă cu specificaţiile tehnice din caietul de sarcini. Oferta tehnica trebuie sa fie prezentata intr-un format care să permită selectarea textului si copierea acestuia. Toate referintele (link-urile) către site-uri Internet trebuie să fie in format hyperlink (gata de click). In acest sens propunerea tehnica trebuie sa fie incarcata si intr-un format editabil sau care să permită selectarea textului si copierea acestuia.

Propunerea tehnică va cuprinde cel puţin elementele mentionate in cadrul fisei de date a achizitiei, precum si prezentarea în detaliu cu privire la serviciile ofertate prin raportare la cerintele stabilite în prezentul caiet de sarcini. Cerintele din cadrul acestui capitol sunt completate de cele din cadrul sectiunii IV.4.1. Modul de prezentare a propunerii tehnice din fisa de date a achizitiei.

Omisiunea sau neîndeplinirea corespunzătoare a oricărei dintre cerinţele prezentului caiet de sarcini va duce la respingerea ofertei ca neconformă. Astfel, lipsa unui răspuns sau prezentarea unor descrieri nerelevante prin raportare la cerințele prezentului caiet de sarcini va duce la descalificarea ofertantului. De asemenea, un simplu răspuns (afirmație) de confirmare din partea operatorului economic cu privire la respectarea cerinţelor din caietul de sarcini, fără precizarea exactă a modalităţii de îndeplinire, nu va fi acceptat. În acest sens se solicită din partea ofertantilor și intră în răspunderea acestora prezentarea dovezilor concrete în sprijinul oricăror afirmaţii care se pot încadra în categoria exemplului anterior menționat.

Operatorii economici vor oferta toate materialele și echipamentele prevăzute în caietul de sarcini, iar acolo unde este cazul, vor propune echipamente suplimentare pentru a îndeplini cerințele enunțate în caietul de sarcini.

In scopul probarii în mod concludent de catre ofertanţi a indeplinirii cerintelor privind funcţionalităţile minime solicitate, autoritatea contractanta isi rezerva dreptul de a solicita în cadrul etapei de evaluare a ofertelor desfasurarea unei sesiuni demonstrative. In acest scop, ofertantii vor

utiliza propriile resurse tehnice. In cursul sesiunii demonstrative se va solicita prezentarea interactiva a functionalitatilor prevazute in documentatia de atribuire.

Duratele fazelor și datele de început și sfarșit ale activităților menționate graficul de implementare si panul detaliat de implementare vor putea fi actualizate de catre Ofertant la semnarea contractului în conformitate cu data efectiva de începere a contractului.

Nota:

Specificatiile tehnice definite in cadrul prezentului caiet de sarcini corespund necesitatilor si exigentelor autoritatii contractante. Avand in vedere specificitatea acestui proiect, autoritatea a descris necesarul de livrabile si servicii intr-un nivel de detaliu necesar operatorilor economici interesati, permitand identificarea obiectului acestui contract de achizitie publica.

Toate specificatiile, serviciile si cerintele mentionate si solicitate in cadrul acestui caiet de sarcini sunt insotite de mentiunea „sau echivalent”.

Intocmit,

Verificat,