CAIET DE SARCINI

pentru achizitia de

„Infrastructura hardware si software de baza, servicii de dezvoltare si implementare a sistemului informatic SIAMC propus prin proiect (analiza, proiectare, implementare, testare sistem informatic, inclusiv portal web, precum si instruirea personalului care va utiliza si administra sistemul informatic dezvoltat), respectiv servicii de consultanta in vederea realizarii analizei legislative si institutionale pentru identificarea oportunitatilor de imbunatatire a proceselor de lucru din cadrul IM”

in cadrul proiectului

“*COMBATEREA MUNCII LA NEGRU SI SPORIREA SECURITATII MUNCII IN ROMANIA PRIN IMBUNATATIRI DE STRUCTURA SI PROCES IN CADRUL INSPECTIEI MUNCII*” - COD SMIS 48591

Cuprins

1. SCOPUL ACHIZITIEI....4
1.1. Conformitatea cu obiectivele Strategiei "Agenda digitala pentru Romania" si ale Strategiei nationale de securitate cibernetica....4
2. CERINTE PRIVIND SERVICIILE DE CONSULTANTA....7
2.1. Descrierea contextului....7
2.2. Activitati generale ale etapei de consultanta....7
2.3. Activitati specifice ale etapei de consultanta....8
2.4. Rezultate asteptate....9
2.5. Aspecte generale....9
3. CERINTE PRIVIND IMPLEMENTAREA SISTEMULUI INFORMATIC SIAMC....10
3.1. Cerinte generale....10
3.2. Prevederi de securitate....11
3.3. Cerintele functionale ale sistemului....12
3.3.1. Functionalitati front-office si back-office....12
3.3.2. Integrarea componentelor....16
3.3.3. Integrarea cu sisteme existente....16
3.3.3.1. Integrarea cu sistemul REGES....17
3.3.3.2. Integrarea cu sistemul de la ONRC....19
3.3.3.3. Integrarea cu sistemul de la ANAF....19
3.3.3.4. Integrarea cu sistemul de la DEPABD....19
3.3.3.5. Integrarea cu sistemul de la ORI....20
3.3.3.6. Integrarea cu sistemul de la ANOFM....20
3.3.3.7. Integrarea cu sistemul de la CNPP....20
3.3.3.8. Integrarea cu sistemul de la ANPIS....21
3.4. Parametrii tehnici....21
3.5. Arhitectura functionala a sistemului....23
3.5.1. Portal - sectiune publica....24
3.5.2. Modul de gestiune sesizari on-line de la public....25
3.5.3. Portal - sectiunea privata....25
3.5.4. Modul de Raportare si Business Intelligence cu capabilitati de geo-referentiere....25
3.5.5. Modul control preventiv euristic....27
3.5.6. Modul de consemnare activitati de control....27
3.5.7. Modul de gestiune activitati de teren....28
3.5.8. Modul gestiune centralizata accidente de munca....29
3.5.9. Modul transformare si preluare date din REGS, de la ANAF, DEPABD si ONRC...29
3.6. Arhitectura tehnica....30
3.6.1. Cerinte de baza....31
3.6.2. Componentele sistemului integrat SIAMC....33
3.6.3. Infrastructura hardware....33
3.6.3.1. Cerinte generale echipamente hardware si sistem de comunicatii....34
3.6.3.2. Securizarea sistemului de comunicatii....35
3.6.3.3. Sasiu servere lamelare....36
3.6.3.4. Servere lamelare....37
3.6.3.5. Echipament de stocare centralizata....37

3.6.3.6. Infrastructura de gazduire a echipamentelor....41
3.6.3.7. Infrastructura de alimentare cu energie electrica protejata cu UPS-uri....41
3.6.3.8. Firewall....41
3.6.3.9. Firewall aplicatie....42
3.6.3.10. Echipament analiza logurilor....43
3.6.3.11. Managementul echipamentelor....44
3.6.3.12. Managementul echipamentelor mobile....45
3.6.3.13. Aer conditionat pentru camera serverelor....49
3.6.3.14. Terminale mobile....49
3.6.4. Cerinte sisteme software de baza....50
3.6.4.1. Sisteme de operare....51
3.6.4.2. Software pentru platforma de baza de date....58
3.6.4.3. Software pentru platforma portal si colaborare....63
3.6.4.4. Software pentru platforma GIS....71
3.6.4.5. Software pentru platforma antivirus....79
3.6.4.6. Software pentru platforma fluxuri control si preventie....81
3.6.4.7. Software pentru platforma de Raportare si Business Intelligence....88
3.6.4.8. Software pentru platforma de transformare si preluare date....90
3.6.4.9. Platforma de certificate digitale....93
3.6.4.10. Platforma monitorizare infrastructura HW....96
3.6.4.11. Platforma backup si restaurare....98
3.7. Managementul utilizatorilor si accesul la sistem....100
3.8. Securitatea sistemului....101
3.9. Confidentialitatea datelor....102
4. IMPLEMENTAREA PROIECTULUI....103
4.1. Management de proiect....103
4.2. Analiza....104
4.3. Proiectare....106
4.4. Dezvoltare, configurare si testare interna....107
4.5. Implementare (deployment)....107
4.6. Instruire....108
4.7. Testarea si testele de acceptanta....112
4.8. Asistenta tehnica si suport....114
5. LIVRAREA SI RECEPTIA LIVRABILELOR....118
6. DURATA DE EXECUTIE A PROIECTULUI....119
7. GARANTIE....120
8. MENTENANTA SI SUSTENABILITATE....121
9. PREZENTAREA PROPUNERII TEHNICE....123
ANEXA 1....126

1. SCOPUL ACHIZITIEI

Scopul prezentului caiet de sarcini este achizitia de produse si servicii pentru implementarea sistemului informatic SIAMC care este componenta principala a proiectului "*Combaterea muncii la negru si sporirea securitatii muncii in Romania prin imbunatatiri de structura si proces in cadrul Inspectiei Muncii*" COD SMIS 48591, proiect finantat prin fonduri europene - Programul Operational Sectorial Cresterea Competitivitatii Economice, Axa Prioritara III "Tehnologia Informatiei si Comunicatiilor pentru sectoarele privat si public", Domeniul Major de Interventie 2 „Dezvoltarea si cresterea eficientei serviciilor publice electronice", Operatiunea 1 „Sustinerea implementarii de solutii de e-guvernare si asigurarea conexiunii la broadband, acolo unde este necesar", APEL 5.

Obiectivul general al acestui proiect este cresterea eficientei, eficacitatii si calitatii serviciilor oferite la nivel national de catre Inspectia Muncii (IM) prin eficientizarea activitatilor interne ale institutiei utilizand mijloace specifice tehnologiei informatiei si comunicatiei.

Produsele si serviciile care vor fi achizitionate se impart in urmatoarele categorii:

- servicii de consultanta in vederea realizarii analizei legislative si institutionale pentru identificarea oportunitatilor de imbunatatire a proceselor de lucru din cadrul IM;
- produse si servicii pentru implementarea sistemului informatic SIAMC dupa cum urmeaza:
    - servicii de dezvoltare si implementare a sistemului informatic SIAMC (analiza, proiectare, implementare, testare sistem informatic, inclusiv portal web, precum si instruirea personalului care va utiliza si administra sistemul informatic dezvoltat);
    - produse de infrastructura hardware si software de baza.

1.1. Conformitatea cu obiectivele Strategiei "Agenda digitala pentru Romania" si ale Strategiei nationale de securitate cibernetica

Acest proiect este in conformitate cu obiectivele Strategiei Agenda digitala pentru Romania, precum si cu Strategia nationala de securitate cibernetica. Proiectul se adreseaza Domeniului de actiune 1 – e-Guvernare, interoperabilitate, securitatea retelelor si sistemelor informatice, cloud computing si media sociale, din cadrul Strategiei Agenda digitala pentru Romania.

Implementarea proiectului va duce la sporirea gradului de transparenta al actelor administratiei publice prin informatizarea serviciilor publice, intrucat propune servicii ce faciliteaza accesul cetatenilor la informatii si documente de interes public, le ofera posibilitatea de a consulta legislatia din domeniul muncii, de a consulta stadiul achizitiilor publice si de a depune sesizari si reclamatii.

De asemenea, cetatenii in general si angajatii in special, precum si organizatiile, vor avea un acces sporit la servicii publice digitalizate prin cresterea numarului de servicii publice ce vor putea fi accesate online pentru consultarea informatiilor publice, inregistrarea si urmarirea stadiului de rezolvare a petitiilor prin definirea obiectivelor strategice, aliniere organizationala, executie strategica in baza initiativelor stategice, inchidere a buclei de management, pe baza masurarii, invatarii, testarii schimbarilor si adaptarii obiectivelor strategice ceea ce va duce la cresterea accesului la servicii publice digitalizate.

Deoarece proiectul are in vedere implementarea unei platforme destinata atat inregistrarii online a sesizarilor si preluarii online a petitiilor, cat si gestionarii activitatii specifice a inspectorilor de munca, acesta va conduce la imbunatatirea guvernantei asupra implementarii serviciilor publice informatizate.

Prin asigurarea interoperabilitatii intre sistemul SIAMC si sistemele altor institutii, precum cele de la ONRC, ANAF si DEPABD, pentru preluarea de date relevante activitatii inspectorilor IM/ITM, se va obtine o crestere a eficientei administratiei publice si scaderea cheltuielilor administratiei publice.

Referitor la strategia de securitate cibernetica a Romaniei scopul acesteia este de a defini si de a mentine un mediu virtual sigur, cu un inalt grad de rezilienta si de incredere, bazat pe infrastructurile cibernetice nationale, care sa constituie un important suport pentru securitatea nationala si buna guvernare, pentru maximizarea beneficiilor cetatenilor, mediului de afaceri si ale societatii romanesti, in ansamblul ei. In acest context, acest proiect abordeaza prevederile cu privire la securitatea serviciilor si a datelor ce vor fi disponibile pe platforma online in cadrul capitolului „Prevederi de securitate”.

Prin masurile de securitate prevazute (a se vedea atat capitolul mentionat anterior cat si echipamentele speciale de securitate prevazute a se achizitiona) sistemul va impiedica atacurile cibernetice impotriva infrastructurii prevenind astfel intreruperea/afectarea acestora inainte de a putea constitui un pericol la adresa securitatii nationale. Accesarea neautorizata sistemului va fi

asigurata prin implementarea unei autentificari bazate pe certificate digitale (a se vedea capitolul „Platforma de certificate digitale”). Modificarea, stergerea sau deteriorarea neautorizata de date informatice ori restrictionarea ilegala a accesului la aceste date inclusiv a spionajului cibernetic va fi impiedicata prin mijloacele prevazute in capitolele amintite mai sus.

Prezenta documentatie propune masuri de exploatare a oportunitatilor identificate in Strategia nationala de securitate cibernetica, si anume:

- sustinerea politicilor si promovarea intereselor nationale;
- dezvoltarea si sustinerea mediului de afaceri;
- cresterea calitatii vietii prin dezvoltarea serviciilor oferite de societatea informationala;
- imbunatatirea cunoasterii si sustinerea deciziilor strategice nationale in era informationala prin asigurarea capacitatilor si instrumentelor cibernetice adecvate;
- cresterea nivelului de cunoastere si a capacitatii de predictie in scopul avertizarii timpurii privind riscurile si amenintarile la adresa securitatii nationale;
- cresterea capacitatilor tehnice si a competentelor resursei umane pentru realizarea obiectivelor de securitate nationala.

2. CERINTE PRIVIND SERVICIILE DE CONSULTANTA

Obiectivul etapei de consultanta il reprezinta **derularea de activitati de analiza institutionala si legislativa, comparativa si evolutiva, de natura sa identifice oportunitatile de imbunatatire aferente proceselor in care Inspectia Muncii are atributii.**

Activitatea consta in analiza cadrului legislativ si a activitatii derulate de institutia solicitanta pentru a identifica oportunitatile de imbunatatire a proceselor de lucru din cadrul Inspectiei Muncii.

2.1. Descrierea contextului

La momentul actual, elementele de planificare, executie, inregistrare rezultate, analize si monitorizari ulterioare asupra agentilor economici nu sunt realizate intr-un mod unitar, sincronizate cu obiectivele administratiei centrale si disponibile catre aceasta pentru vizualizarea unei imagini de ansablu in privinta aspectelor legale privind piata muncii din Romania.

Au fost identificate probleme in ceea ce priveste capacitatea tehnologica a inspectorilor de a accesa informatie relevanta din sistemele informatice ale institutiei, in timp real, pe teren, pentru eficientizarea activitatilor de control, documentarea adecvata a rapoartelor de control, procesele verbale de control sau referatelor specifice.

In plus, actiunile de control si monitorizare care implica investigatii largite din punct de vedere teritorial, la nivelul agentilor economici care isi desfasoara activitatile comerciale si de productie in mai multe judete, la nivel national si international sunt substantial influentate de viteza cu care informatiile raspandite la nivelul mai multor inspectorate teritoriale de munca pot fi accesate si agregate in sprijinul demersurilor inspectorilor de munca.

Eliminarea acestor neajunsuri nu este posibila in lipsa unor mecanisme moderne privind planificarea si coordonarea activitatilor din teren a inspectorilor, sprijin in timp real in vederea derularilor actiunilor de control, raportare, analiza si urmarirea actiunilor ulterioare, intreprinse atat de catre institutia Inspectia Muncii, cat si de catre agentii economici.

2.2. Activitati generale ale etapei de consultanta

Activitatile de analiza institutionala si legislativa, comparativa si evolutiva, de natura sa identifice oportunitatile de imbunatatire aferente proceselor in care Inspectia Muncii are atributii vor acoperi urmatoarele aspecte referitoare la procesele si fluxurile informationale din cadrul institutiei:

- analiza informatiilor si a serviciilor oferite de IM agentilor economici, regasite fie la nivelul administratiei centrale, fie la nivelul inspectoratelor teritoriale de munca;
- analiza proceselor si a fluxurilor de prelucrare informatii sau asigurare servicii existente, identificarea tuturor activitatilor procedurabile, specifice pe de o parte administratiei centrale, si pe de alta parte, inspectoratelor teritoriale de munca, si stabilirea unui set de procese unitare, actualizate;
- analiza beneficiarilor informatiilor sau serviciilor furnizate;
- elaborarea de propuneri privind imbunatatirea serviciilor oferite, noi fluxuri de informatii.

2.3. Activitati specifice ale etapei de consultanta

Se doreste realizarea la nivelul IM impreuna cu institutiile sale subordonate a unui cadru unitar de elaborare, implementare, control si imbunatatire a documentatiilor interne, pentru asigurarea in permanenta a conditiilor de conformitate cu cerintele reglementate de documentele de referinta in vigoare si pentru ca fiecare angajat sa dispuna permanent de informatiile necesare utilizarii corecte a documentatiei specifice activitatii pe care o desfasoara. In vederea atingerii obiectivelor etapei de consultanta, furnizorul acestor servicii trebuie sa intreprinda cel putin urmatoarele activitati:

- analiza stadiului existent al proceselor, procedurilor, circuitelor si a fluxurilor informationale, parametrizarea acestora si elaborarea unui raport de analiza al situatiei existente pentru toata aria de procese si fluxuri informationale din cadrul structurii IM;
- identificarea punctelor slabe, respectiv identificarea acelor elemente care se materializeaza in dificultati in procesele de indeplinire a misiunii si viziunii institutiei;
- analiza diferentelor dintre situatia existenta si situatia dorita;
- identificarea si prezentarea strategiei de abordare, metodele de analiza a proceselor, metode de optimizare a acestora in vederea obtinerii situatiei dorite;
- elaborarea documentelor care vor descrie actiunile necesare a fi intreprinse in vederea optimizarii proceselor si a fluxurilor informationale pornind de la situatia existenta, respectiv elaborarea unui document de analiza institutionala si legislativa, comparativa si evolutiva;

Documentul de analiza va fi elaborat intr-o forma unitara, realista si actualizata in concordanta cu nevoile descoperite si luand in considerare legislatia aplicabila in domeniu, in vederea atingerii indicatorilor de performanta stabiliti.

2.4. Rezultate asteptate

Serviciile prestate de catre Consultant vor asigura obtinerea urmatoarelor rezultate:

- un document de analiza institutionala si legislativa, comparativa si evolutiva, de natura sa identifice oportunitatile de imbunatatire aferente proceselor in care Inspectia Muncii are atributii.

2.5. Aspecte generale

- operatorul economic va derula toate activitatile mentionate in colaborare cu echipa IM. Beneficiarul va desemna o echipa coordonata de un responsabil care sa sprijine ofertantul in activitatea de analiza;
- pe parcursul implementarii contractului, este necesara o analiza a modului in care este realizata implementarea fiecarui proces, procedura, circuit sau flux pentru a detecta eventualele disfunctionalitati, dar si pentru a evidentia posibilitatile fiecaruia;
- Consultantul va pune la dispozitia reprezentantilor IM documentul de analiza institutionala si legislativa in format electronic si pe hartie.

3. CERINTE PRIVIND IMPLEMENTAREA SISTEMULUI INFORMATIC SIAMC

3.1. Cerinte generale

SIAMC va fi un sistem informational ce va sprijini masurile cu privire la domeniul muncii ce sunt luate de personalul autorizat al Inspectiei Muncii si al Inspectoratelor Teritoriale de Munca, sau de cetateni. Functiile SIAMC nu sunt o simpla ilustrare a documentatiei pe suport de hartie si a comunicarii, ci mult mai mult de atat: ele abordeaza prestarea de servicii si activitati din domeniul muncii ca pe un proces, in care sunt implicati diversi participanti, inclusiv cetatenii. De aici rezulta numeroase cerinte functionale privitoare la sistemele de informatii si la continutul documentelor.

SIAMC are ca scop implementarea functionalitatilor e-guvernare necesare pentru a da posibilitatea inregistrarii online a sesizarilor si preluarea online a petitiilor, pentru a face posibila consultarea continutului legislativ din domeniul muncii si a altor informatii inclusiv afisarea stadiului achizitiilor publice derulate de IM.

Prin implementarea sistemului, in zona back office, va fi posibila inregistrarea, evidenta si actualizarea controalelor efectuate de catre personalul calificat, inregistrarea, evidenta si actualizarea autorizatiilor de protectia muncii, gestiunea accidentelor de munca, prin inregistrarea, evidenta si actualizarea accidentelor de munca retinerea in baza si actualizarea informatiilor privitoare la accidentele de munca individuale si colective de catre inspectorii de munca. Prin intermediul sistemului se va face inclusiv monitorizarea dovezilor de aducere la indeplinire a masurilor dispuse de inspectorii de munca in urma efecturarii controlelor de catre inspectorii de munca. De asemenea acestia vor putea consulta online carnetele de munca, contractele de munca si anexele aferente in format electronic dar si dovezile de calcul a drepturilor salariale si vor avea sprijinul necesar pentru evidenta documentelor pe fluxurile de lucru specifice.

- SIAMC trebuie sa fie o sursa sigura de informatii disponibila la orice nivel teritorial expertilor si inspectorilor IM si ITM, ce se concentreaza asupra cetatenilor si a interactiunii cu mediul economic din Romania;
- SIAMC trebuie sa sprijine luarea de decizii prin accesul la informatii despre documentele de evidenta a muncii, atunci cand este nevoie, si include sprijinirea luarii de decizii intemeiate pe dovezi;

- SIAMC trebuie sa organizeze si automatizeze desfasurarea muncii; sistemul va garanta ca datele, informatiile si cunostintele sunt comunicate si evita intarzierea raspunsurilor si a centralizarii informatiilor, care la randul lor provoaca intarzieri si intreruperi ale activitatilor principale IM si/sau ITM ;
- SIAMC trebuie sa sprijine nu doar intocmirea de date specifice domeniului muncii ci si de date privind calculul contributiilor, managementul calitatii si analiza rezultatelor si de asemenea redactarea de date pentru sistemul public precum rapoartele privind relatiile de munca sau observarea sistemului de munca;
- SIAMC trebuie sa sprijine comunicarea de informatii privind domeniul muncii, pentru a se realiza o evidenta unica integrata si pentru a se asigura eficienta si o calitate imbunatatita, inclusiv din perspectiva cetatenilor.
- SIAMC trebuie sa fie integrat la toate nivelele de interes cu domeniul muncii, inclusiv pe plan legislativ si procedural si trebuie sa contina date si cunostinte relevante, asigurand aportul de informatii atat de la utilizatori cat si din interoperabilitatea tehnica si de continut cu sistemele relevante existente;
- SIAMC trebuie sa asigure cetatenilor si partenerilor din mediul de afaceri din Romania disponibiltatea informatiilor, accesul neingradit la informatiile personale, conform prevederilor legale in vigoare, si sa asigure mijloacele necesare de comunicare cu acestia.

3.2. Prevederi de securitate

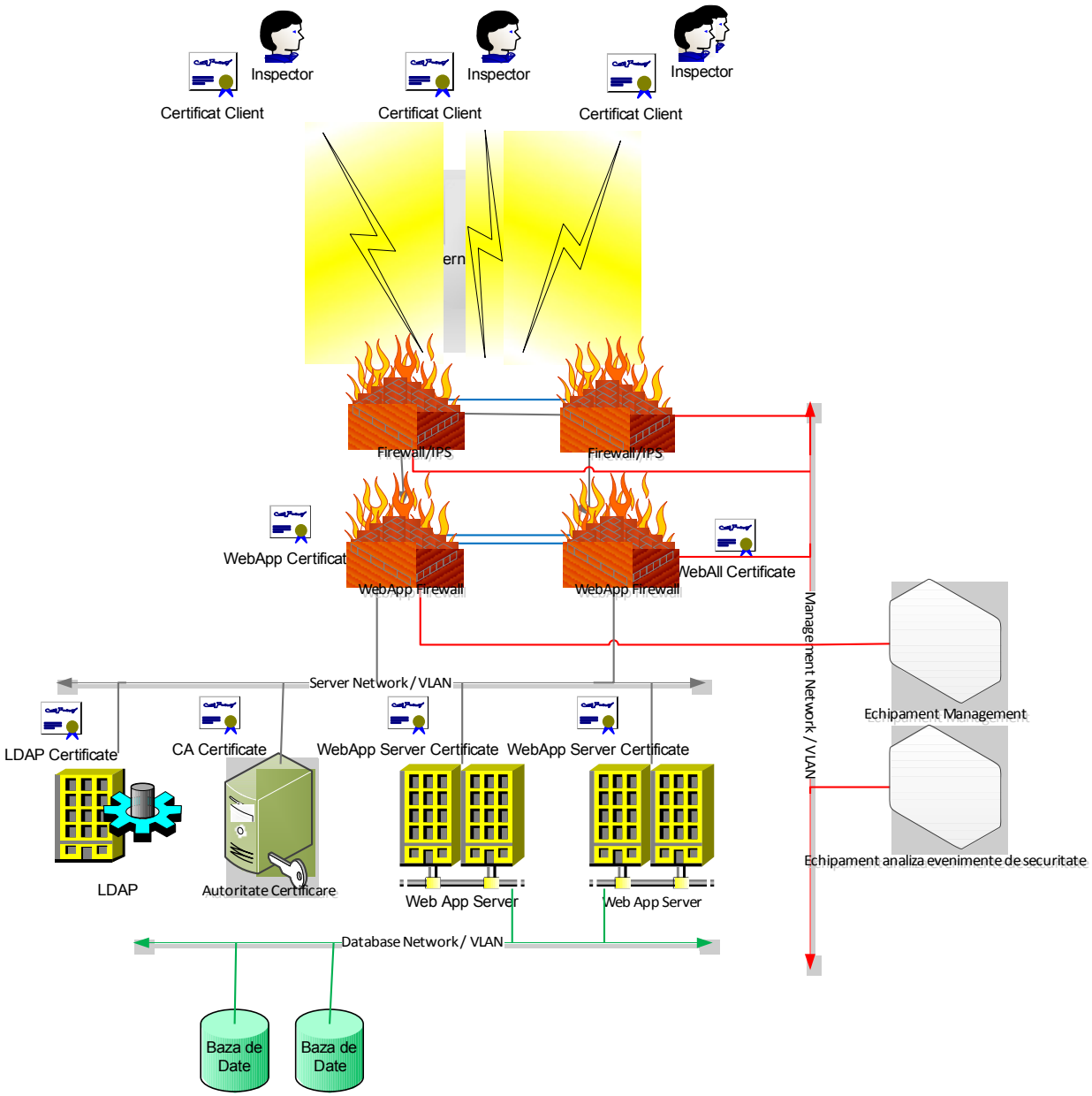
Luand in considerare natura confidentiala a datelor ce vor fi colectate, sistemul integrat SIAMC trebuie sa contina un sistem de securitate performant, ce suporta functionalitati de integrare si autentificare, care sa respecte obligatoriu cel putin cerintele minime de securitate prezentate in ORDINUL nr. 52 din 18 aprilie 2002 privind aprobarea Cerintelor minime de securitate a prelucrarilor de date cu caracter personal, emis de Avocatul Poporului.

Accesul utilizatorilor la interfata de colectare a datelor la nivelul sistemului central se va efectua securizat, prin utilizarea certificatelor digitale si/sau utilizator si parola.

Canalele de comunicatii utilizate pentru transfer vor fi securizate.

Aplicatia va permite autentificarea securizata prin dispozitive electronice (de ex. Token), precum si autentificari standard prin utilizator si parola. Furnizorul va oferi propuneri de politici de securitate a parolelor, modul de schimbare a acestora, tipul de caractere necesare in crearea unei parole precum si modul de criptare in baza de date.

SIAMC, Architectura de Securitate



3.3. Cerintele functionale ale sistemului

3.3.1. Functionalitati front-office si back-office

SIAMC este un pachet de functionalitati integrate pentru coordonarea electronica a proceselor din domeniul muncii, asa cum sunt mentionate in sectiunile ‘Arhitectura Functionala a

sistemului' si 'Arhitectura Tehnica'. Acestea pot fi la randul lor structurate, in functie de disponibilitatea in zonele cu acces public, in functionalitati front-office si functionalitati back-office. Functionalitatile front-office asigura comportamentul sistemului in afara institutiei, respectiv in relatia cu angajatorii, angajatii si/sau cetatenii. Functionalitatile back-office asigura fluxurile, procesele si continutul intern institutiilor IM si ITM, fiind accesibile doar personalului autorizat.

De asemenea, gruparea functionalitatilor in acest mod confirma nivelul ridicat de interactiune al angajatorilor, angajatilor si/sau cetatenilor cu sistemul SIAMC.

Din perspectiva disponibilitatii pentru public, respectiv zona front-office si zona back-office, functionalitatile generice ale sistemului care trebuie implementate de catre contractor sun cel putin urmatoarele:

Functionalitatile front-office:

- Posibilitatea inregistrarii online a sesizarilor. Functionalitatea va permite salariatilor sa transmita in format electronic o sesizare catre Inspectoratul Teritorial de Munca de care apartine in ceea ce priveste incalcarea de catre angajatori a prevederilor legislatiei muncii. Functionalitatea va fi disponibila in zona publica a portalului web (componenta centrala) si va fi accesibila doar in baza introducerii corecte a utilizatorului si a parolei;
- Afisarea stadiului achizitiilor publice. Prin intermediul acestei functionalitati cetatenii vor putea urmari informatiile publice aferente achizitiilor publice, precum stadiul, data initierii, data programata a finalizarii, etc. Stadiul achizitiilor publice va fi actualizat, astfel incat sa fie corect afisat in componenta centrala, respectiv in portalul web;
- Preluarea online a petitiilor. Functionalitatea va permite transmiterea online a petitiilor, fluxul disponibil cetatenilor fiind similar cu cel al transmiterii sesizarilor de catre angajati. De asemenea, functionalitatea va permite si urmarirea stadiului de rezolvare in care acestea se afla. Stadiul va fi actualizat automat, in conformitate cu evolutia interna a petitiei in cadrul institutiei;
- Consultarea continutului legislativ din domeniul muncii.

Functionalitati back-office:

- Inregistrarea, evidenta si actualizarea controalelor efectuate de catre personalul compartimentului responsabil, cu specificarea controalelor de fond si de sondaj. Informatiile privind aceste controale se refera la: unitatea controlata, tipul controlului,

actiune, data procesului verbal de control, alte informatii de interes. Procesele verbale de constatare si sanctionare contraventii vor putea fi incarcate in baza de date, ajutand astfel la crearea unei evidente complete a actiunii de control. Se pot incarca in sistem si toate informatiile privind neconformitatile constatate in urma controalelor efectuate;

- In cadrul proiectului se va realiza o harta GIS care va include: judete, UAT-uri, localitati. Sistemul va oferi posibilitatea de a marca pe harta pozitia geografica la care se regaseste unitatea controlata. In cadrul vizitelor pe teren, inspectorii vor avea posibilitatea de a introduce automat prin intermediul modulului dedicat al noului sistem pozitia geografica la care se gaseste unitatea controlata. Coordonatele spatiale vor fi preluate cu ajutorul modulului dedicat integrat al terminalelor mobile furnizate in cadrul proiectului. Prin pozitionarea pe harta a unitatilor controlate vor putea fi realizate ulterior rapoarte ce includ informatii spatiale ale unitatilor, locatia accidentelor de munca individuale etc.;
- Inregistrarea, evidenta si actualizarea autorizatiilor de protectia muncii, conform procesului de expertizare pe care il desfasoara Directia ‘Securitate si Sanatate in Munca’;
- Gestiunea accidentelor de munca, prin inregistrarea, evidenta si actualizarea accidentelor de munca retinerea in baza si actualizarea informatiilor privitoare la accidentele de munca individuale si colective. Datele care se vor pastra sunt legate de: informatii de identificare a unitatii unde s-a petrecut accidentul, numele celor accidentati, locul de munca, detalii despre ocupatie, vechime in munca, numarul victimelor, tipul accidentului, gravitatea lui, imprejurarile in care s-a petrecut, cauzele producerii, timpul in care s-a petrecut, consecintele accidentului, descrierea modului in care s-a produs accidentul etc.;
- Consultarea carnetelor de munca, a contractelor de munca si a anexelor aferente in format electronic;
- Consultarea electronica a dovezilor de calcul a drepturilor salariale si validarea automata a calculului;
- Monitorizarea dovezilor de aducere la indeplinire a masurilor dispuse de inspectorii de munca;
- Transmiterea, verificarea, aprobarea sau respingerea documentelor din fluxurile specifice;
- Monitorizarea sesizarilor in format electronic transmise de angajati, in ceea ce priveste incalcarea de catre angajatori a prevederilor legislatiei muncii;

- Evidenta Ordinelor de plata privind datoriile achitate la buget lunar conform legislatiei in vigoare;
- Evidenta Statelor de plata depuse de angajator lunar la fiecare ITM conform legislatiei in vigoare;
- Evidenta Carnetelor de munca depuse la ITM precum si detalii despre localizarea lor in cadrul depozitelor ITM;
- Evidenta Planurilor de control defalcate pe perioade de realizare, precum si tematica propusa;
- Evidenta Proceselor verbale de control;
- Evidenta Proceselor verbale de constatare si sanctionare a contraventiilor;
- Evidenta Actiunilor de consultanta in domeniul relatiilor de munca si cursurilor de perfectionare organizate;
- Rapoarte specifice, inclusiv:
  - ✓ Statistici privind numarul inspectorilor de munca, structurate pe domenii, conform Conventiilor 81 si 129 si Recomandarilor OIM;
  - ✓ Distributia teritoriala a inspectorilor de munca, conform Conventiilor 81 si 129 si Recomandarilor OIM;
  - ✓ Statistici privind unitatile supuse controlului Inspectiei Muncii, respectiv inspectoratelor teritoriale de munca, conform Conventiilor 81 si 129 si Recomandarilor OIM;
  - ✓ Statistici privind controalele, la nivel national si teritorial, conform Conventiilor 81 si 129 si Recomandarilor OIM;
  - ✓ Numarul si natura abaterilor de la prevederile legale, conform cerintelor conventiilor OIM;
  - ✓ Numarul si natura sanctiunilor aplicate pentru nerespectarea prevederilor legale, conform cerintelor conventiilor OIM;
  - ✓ Statistici privind unitatile autorizate sau avizate de inspectoratele teritoriale de munca in baza unor legi speciale;
- **Gestiunea petitiilor**, prin asigurarea inregistrarii in format electronic si scanarea acestora, configurarea si urmarirea fluxurilor petitiilor de la momentul inregistrarii pana

la eliberare si cunoasterea in orice moment a stadiului solutionarii, prin asigurarea mecanismelor de diferentiere a accesului pentru inregistrare, urmarire su descarcare;

- **Cautarea in dosarele electronice create**;
- **Conexarea documentelor**, va permite personalului Biroului Comunicare si Relatii cu Publicul, conexarea mai multor petitii, conform normelor procedurale in vigoare. Conexarea va asigura crearea unei legaturi logice intre doua sau mai multe petitii in format electronic;
- **Arhivarea manuala si automata** a documentelor in format electronic.

Functionalitatile back-office sunt accesate prin intermediul sectiunii private a portalului si sunt caracteristice modulelor si platformelor incluse in cadrul nivelului de logica de business.

Distribuirea accesului la resursele sistemului SIAMC va fi realizata in conformitate cu politicile de securitate ale institutiei.

3.3.2. Integrarea componentelor

Se solicita ca sistemul integrat SIAMC sa beneficieze de un nivel corespunzator de modularitate astfel incat sa ofere autonomia functionala a sistemelor componente (asa cum este prezentata in sectiunea ‚Arhitectura functionala a sistemului'). In acelasi timp insa, comunicarea dintre acestea trebuie sa asigure realizarea completa si eficienta a proceselor modelate la nivelul SIAMC, precum gestionarea carnetelor de munca, gestionarea petitiilor sau gestionarea fondurilor de cunostinte. La nivelul SIAMC, integrarea componentelor in sistem se va face respectand standardele in domeniu, dupa cum urmeaza:

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

Desi sistemul va fi unul de tip modular, el va functiona ca un tot unitar. Autentificarea in sistem se va face printr-un mecanism de tip „Single Sign-On", permitind accesul utilizatorului in toate modulele pentru care dispune de drepturile necesare dupa introducerea numelui de utilizator si a parolei o singura data in cadrul unei sesiuni de lucru.

3.3.3. Integrarea cu sisteme existente

SIAMC trebuie sa se integreze cu urmatoarele sisteme informatice functionale la nivelul institutiilor care pot furniza date utile Inspectiei Muncii: sistemul REGES al IM, sistemul informatic de la Registrul Comertului, sistemul de la nivelul ANAF, sistemul de evidenta a persoanelor DEPABD, sistemul de la Oficiul Roman pentru Imigrari, sistemul de la ANOFM,

sistemul de la Casa Nationala de Pensii Publice si sistemul de la Agentia Nationala pentru Plati si Inspectie Sociala.

Pe langa sistemele existente la nivelul institutiilor enumerate anterior, SIAMC trebuie sa ofere capabilitati de integrare si cu alte sisteme ale altor institutii, pe masura ce acest lucru este necesar.

3.3.3.1. Integrarea cu sistemul REGES

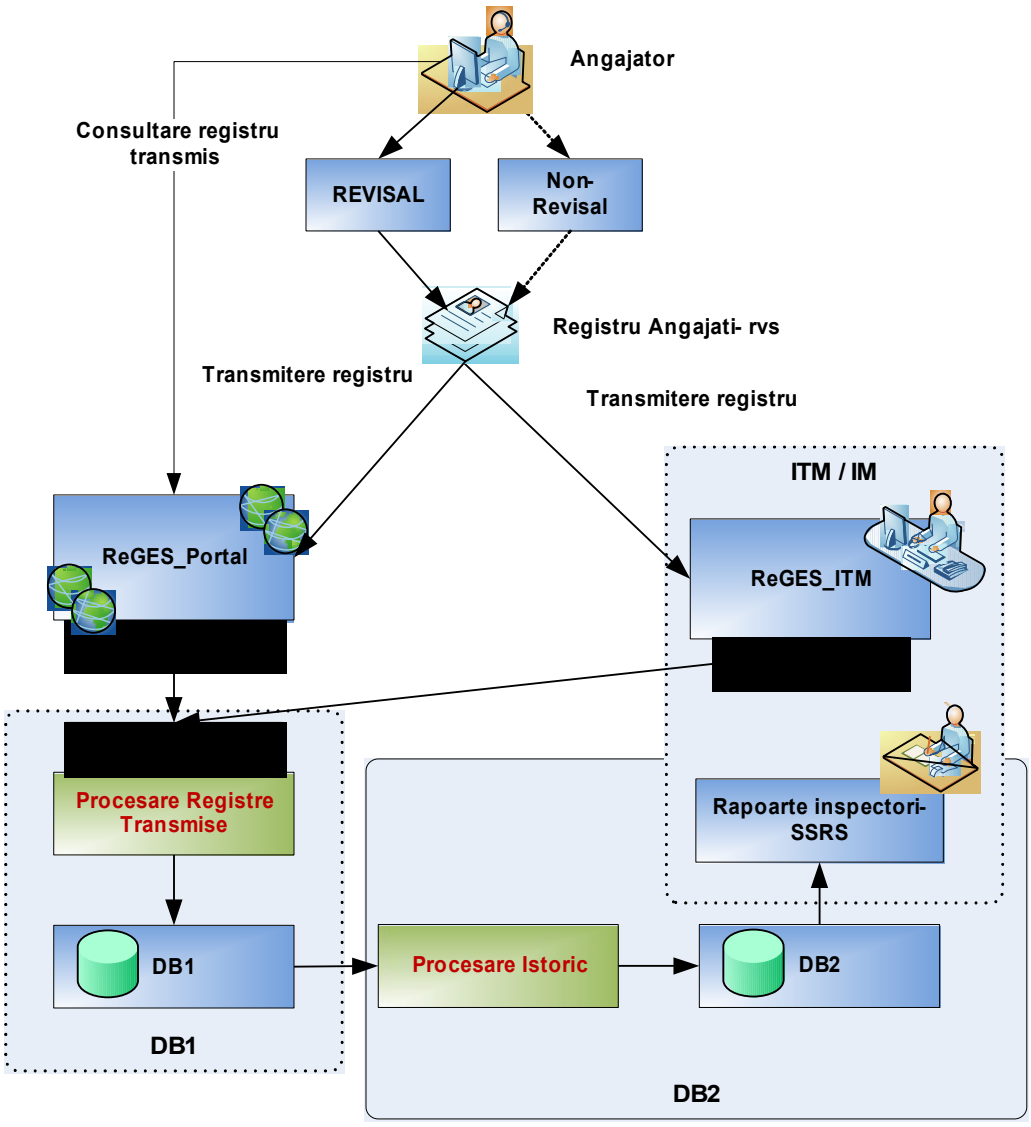
Sistemul REGES (Registrul general de evidenta a salariatilor) asigura informatizarea activitatii de intocmire, completare si actualizare a Registrului general de evidenta a salariatilor, in conformitate cu prevederile legale si Hotararii Guvernului nr. 161/2006 (pana la data de 31.07.2011) si H.G. nr. 500/2011 (dupa data de 01.08.2011). Registrul general de evidenta a salariatilor gestioneaza toti angajatorii cu salariatii si contractele de munca ale acestora din Romania.

Aplicatia Revisal este destinata angajatorilor pentru gestiunea contractelor si a salariatilor – aceasta aplicatie se instaleaza local pe statiile de lucru, iar prin intermediul ei se genereaza registrul ce se depune in sistemul Reges.

Portalul online este destinat angajatorilor pentru depunerea fisierelor online in sistemul REGES.

Sistemul REGES preia fisierele .rvs depuse online sau local cu informatiile ce contin starile actuale ale contractelor de munca, le proceseaza pentru a elibera codurile de incarcare si, ulterior, le proceseaza in vederea construirii istoricului angajatorului, salariatilor si a contractelor de munca. O functionalitate suplimentara a sistemului este de a oferi rapoarte statistice la cererea reprezentantilor Inspectiei Muncii, ce sunt generate manual din baza de date si sunt folosite pentru diferite petitii. De asemenea, sistemul REGES transmite automat noaptea statisitici catre ANOFM.

Arhitectura sistemului este prezentata sintetic in diagrama urmatoare:



Tehnologiile utilizate sunt: Microsoft Windows Server 2008 R2, Microsoft .Net Framework 3.5, Microsoft SQL Server 2008 R2, Microsoft Message Queuing (MSMQ), Microsoft ASP.NET MVC (Model View Controller), Microsoft Internet Information Services (IIS) for Windows Server.

Deoarece inspectorii utilizeaza in activitatile de control informatii stocate in sistemul REGES, precum angajatori, angajati, contracte de munca, este necesar ca SIAMC sa ofere functionalitati de integrare cu sistemul REGES. Componentele sistemului REGES comunica intern prin intermediul serviciilor, iar platforma tehnica a REGES permite extinderea acestor servicii.

Ofertantul declarat castigator va primi toate informatiile de detaliu necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul REGES nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.2. Integrarea cu sistemul de la ONRC

Se doreste integrarea SIAMC cu acest sistem, prin intermediul serviciilor web, pentru a asigura posibilitatea de preluare/validare date despre angajator detinute de sistemul de la Oficiul National al Registrului Comertului si necesare desfasusrarii activitatilor de control specifice IM/ITM. Pentru a putea fi implementate aceste preluari/verificari, trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si Registrul Comertului; acest cadru legal nu intra in responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la ONRC nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.3. Integrarea cu sistemul de la ANAF

Se doreste integrarea SIAMC cu acest sistem, prin intermediul serviciilor web, pentru a asigura posibilitatea de verificare a starii contributiilor depuse de angajatori la Agentia Nationala de Administrare Fiscala din cadrul Ministerului Finantelor Publice. Pentru a putea fi implementate aceste verificari, trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si ANAF; acest cadru legal nu intra in responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la ANAF nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.4. Integrarea cu sistemul de la DEPABD

Interogarea bazelor de date de la Directia pentru Evidenta Persoanelor si Administrarea Bazelor de Date trebuie sa se efectueze cu ajutorul unui serviciu web pus la dispozitie de noul sistem DEPABD si interogat de SIAMC in vederea verificarii datelor de identificare ale angajatilor. Pentru a putea fi implementate aceste verificari de trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si DEPABD; acest cadru legal nu intra in

responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la DEPABD nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.5. Integrarea cu sistemul de la ORI

Se doreste integrarea SIAMC cu acest sistem, prin intermediul serviciilor web, pentru a asigura posibilitatea de schimb de date cu privire la beneficiarii serviciilor ORI. Pentru a putea fi implementate aceste verificari, trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si ORI; acest cadru legal nu intra in responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la ORI nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.6. Integrarea cu sistemul de la ANOFM

Se doreste integrarea SIAMC cu acest sistem, prin intermediul serviciilor web, pentru a asigura posibilitatea de schimb de date cu privire la beneficiarii/potentialii beneficiari ai serviciilor ANOFM. Pentru a putea fi implementate aceste verificari, trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si ANOFM; acest cadru legal nu intra in responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la ANOFM nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.7. Integrarea cu sistemul de la CNPP

Se doreste integrarea SIAMC cu acest sistem, prin intermediul serviciilor web, pentru a asigura posibilitatea de schimb de date cu privire la beneficiarii/potentialii beneficiari ai serviciilor CNPP. Pentru a putea fi implementate aceste verificari, trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si CNPP; acest cadru legal nu intra in

responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la CNPP nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.3.3.8. Integrarea cu sistemul de la ANPIS

Se doreste integrarea SIAMC cu acest sistem, prin intermediul serviciilor web, pentru a asigura posibilitatea de schimb de date cu privire la beneficiarii/potentialii beneficiari ai serviciilor ANPIS. Pentru a putea fi implementate aceste verificari, trebuie sa se creeze mai intai cadrul legal in baza caruia se va defini protocolul intre IM si ANPIS; acest cadru legal nu intra in responsabilitatea ofertantilor. Ofertantul declarat castigator va primi toate informatiile necesare in etapa de analiza necesara impelementarii sistemului informatic solicitat.

Dezvoltarea serviciilor web expuse de sistemul de la ANPIS nu intra in atributiile Furnizorului sistemului care face obiectul prezentei achizitii. Acesta este responsabil numai pentru asigurarea capabilitatilor de integrare ale sistemului SIAMC.

3.4. Parametrii tehnici

Pentru asigurarea unui cadru optim de implementare a sistemului integrat SIAMC arhitectura si parametri tehnici trebuie sa respecte urmatoarele cerinte generale:

- Trebuie asigurata dotarea cu servere si echipamente pentru Data Center care sa furnizeze complet necesitatile de prelucrare a datelor, conform specificatiilor din sectiunea ‚Infrastructura hardware';
- Tehnologia web implementata trebuie sa implice resurse minime din partea statiilor de lucru, astfel incat sa permita personalului sa lucreze si pe calculatoare mai putin performante;
- Tehnologia web trebuie sa fie optimizata pentru accesarea de pe terminalele mobile livrate in cadrul proiectului pentru controalele efectuate pe teren prin intermediul modulelor dedicate transferului de date, integrate pe terminale, atat atat prin retele de tip Wi-Fi cat si folosind retea de telefonie mobila. Ofertantul va prezenta solutia proprie pentru tehologia folosita pentru a permite ambele tipuri de acces;
- Trebuie asigurata unicitatea informatiilor (fara informatii redundante, dublate, incomplete);

- Sistemul va dispune de manuale de operare a tuturor aplicatiilor software si a dispozitivelor hardware.
- Sistemul va fi conform sau va implementa standarde din domeniu astfel:
    - XML pentru transferul de date inter-aplicatii;
    - XSL pentru transformarea datelor dintr-o structura in alta;
    - SOAP/WSDL pentru apelul de proceduri inter-aplicatii;
    - SQL pentru interogarea bazelor de date;
    - LDAP pentru acces la solutia directory;
- **Disponibilitate -** Disponibilitatea datelor trebuie sa fie asigurata prin salvari zilnice; lucrul in cadrul sistemului trebuie sa fie tranzactional/ multiuser/ concurent. Sistemul trebuie sa fie modular si sa nu conditioneze functionarea unui subsistem de functionarea celorlalte subsisteme.
- **Scalabilitate si redundanta –** sistemul va dispune de facilitati de redundanta pentru a proteja beneficiarul de eventuale defectiuni care pot surveni in timpul functionarii.
- **Standardizare** - subsistemele si platforma hardware vor fi astfel proiectate pentru a respecta standardele de aplicatie in domeniu - 3 niveluri: baze de date, server de aplicatii si interfata utilizator. Dispunerea componentelor aplicatiilor pe echipamente se va face in conformitate cu specificul fiecarei componente: cele de baza de date pe serverul de baza de date, cele de aplicatii pe serverele de aplicatii, iar cele de interfata grafica pe calculatoarele operatorilor.
- **Interfata utilizator** - aplicatiile sistemului informatic trebuie sa foloseasca limba romana pentru toate meniurile, ecranele, rapoartele de aplicatie accesibile utilizatorului final. De asemenea, documentatia si materialele pentru instruire pentru utilizatorii finali vor fi livrate in limba romana. Aplicatiile vor asigura calitatea datelor introduse prin proceduri de validare (prin definirea campurilor obligatorii, a formatului acceptat pentru anumite campuri, a unor valori sau plaje de valori posibile pentru anumite campuri etc.) precum si prin verificarea si atentionarea utilizatorilor asupra incompatibilitatilor sau contradictiilor dintre inregistrari. Sa nu permita existenta datelor dublate, sa sesizeze datele inconsistente, datele lipsa sau deteriorate. Se va permite navigarea facila in si intre toate

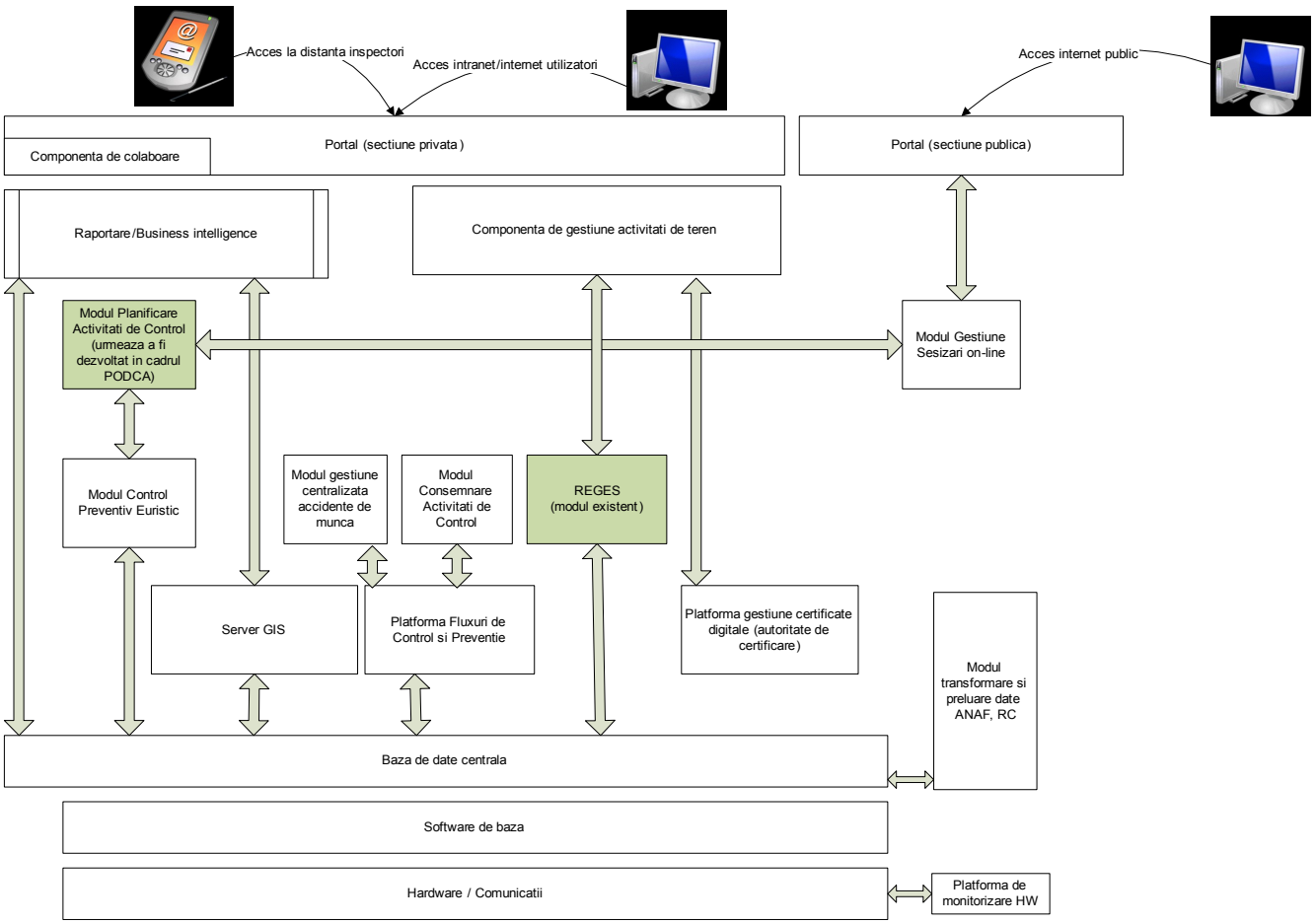
modulele si accesarea tuturor functiilor si comenzilor la care utilizatorul are acordate drepturi in cadrul aceleiasi sesiuni de lucru;

- **Scalabilitate si flexibilitate - s**calabilitate si flexibilitate in distribuirea sistemului, care sa permita extinderea sau modificarea structurii organizatorice a utilizatorilor. Sistemul va trebui sa prezinte un grad mare de parametrizare care sa permita modificari rapide si facile in cadrul aplicatiei Sa fie complet configurabil si capabil sa faca fata necesitatilor unui numar crescind de utilizatori.
- **Extensibilitate si integrare** - sistemul oferit trebuie sa permita integrarea cu functionalitati de semnare electronica si de verificare a semnaturilor documentelor gestionate de aplicatii; Sistemul trebuie sa permita extinderea cu alte functionalitati dorite de catre institutie, pentru aceasta fiind disponibile interfete de programare (API) publice si bazate pe standarde deschise (SOA, WEB-Services, XML); Toate interfetele intre module sau cu module externe vor fi realizate folosind protocoale in conformitate cu standardele descrise mai sus sau cu alte standarde neproprietare.

3.5. Arhitectura functionala a sistemului

Arhitectura solicitata este una multi-nivel, web-based, prin care toate functionalitatile sistemului vor putea fi accesate prin intermediul unui portal specializat, cu o sectiune privata, respectiv o sectiune publica.

Accesul la sistem trebuie sa fie posibil utilizand un browser web standard, atat de catre utilizatorii autorizati ai Inspectiei Muncii (prin intranet/internet), cat si de catre publicul larg (prin internet).



Arhitectura functionala

3.5.1. Portal - sectiune publica

Sectiune publica va fi deschisa publicului larg, si va face disponibile urmatoarele servicii:

- Serviciul de informare, prin care cetatenii vor avea acces la informatii referitoare la legislatie, servicii publice electronice in aria de competenta a IM, informatii de interes general, abonarea la newsletter;
- Afisarea stadiului achizitiilor publice;
- Consultarea continutului legislativ din domeniul muncii;
- Serviciul de inregistrare sesizari si reclamatii, cu prezentarea starii pe flux a acestora si termenul estimat de raspuns. Actiuni disponibile:
    - inregistrare sesizare, incarcare de documente atasate la sesizare;
    - trimiterea sesizare si primirea numarului de inregistrare a acesteia;
    - vizualizarea starii in care se gaseste sesizarea in fluxul de solutionare;

- primirea raspunsului de la IM care sa poata fi descarcat pe calculatorul personal sau printat direct din sistem.

3.5.2. Modul de gestiune sesizari on-line de la public

Aceasta componenta va asigura functionalitatile de back-end pentru inregistrarea sesizarilor si reclamatiilor receptionate prin intermediul sectiunii publice a portalului. Va asigura acordarea de numere unice de inregistrare sesizarilor, alocarea acestora catre actorii responsabili si posibilitatea de adaugare de documente/comentarii in vederea stabilirii unei rezolutii. Va permite de asemeni actualizarea statusului sesizarii de catre utilizatorii autorizati.

3.5.3. Portal - sectiunea privata

Sectune privata va fi disponibila exclusiv utilizatorilor autorizati din partea IM si va oferi acces la functionalitatile dedicate puse la dispozitie prin intermediul modulelor SIAMC descrise in continuare.

3.5.4. Modul de Raportare si Business Intelligence cu capabilitati de geo-referentiere

Acest modul va fi folosit pentru o vizualizare rapida si facila a informatiilor statistice si sintetice, structurate si grupate dupa criterii si caracteristici predefinite intr-o biblioteca de rapoarte sau configurabile de catre utilizator.

Capabilitati generale ale componentei de Raportare si BI:

- conectarea la surse de date de diferite tipuri;
- lucrul cu baza de date in timp real;
- agregarea si diseminarea datelor;
- mod de lucru simplu si usor de inteles;
- modelarea informatiilor in structuri multidimensionale;
- cautare rapida a informatiilor;
- posibilitatea de reprezentare geo-referentiata a datelor la nivel sintetic, precum si functionalitati de drill-down pana la nivel de informatii statistice primare.

Capabilitati tehnice si functionale ale componentei de Raportare si BI:

- usurinta in utilizare, de la definirea structurilor On-Line Analytical Processing (OLAP) la modalitatile de utilizare si prezentare a datelor si informatiilor colectate in sistem;
- posibilitatea definirii unor view-uri private, ce pot fi ulterior publicate;

- sistem de securitate bine definit si structurat, ce garanteaza accesul la datele confidentiale doar utilizatorilor care au setate drepturile respective (prin intermediul LDAP);
- posibilitatea definirii de rapoarte/situatii speciale, in functie de specific, pe langa cele deja predefinite;
- administrarea facila a sistemului de raportare;
- diseminarea informatiilor dupa mai multe criterii:
    - grupare dupa criterii stabilite de catre aplicatie sau utilizator;
    - insumare/agregare pornind de la operatii simple pana la definirea de indicatori statistici complecsi;
    - distribuirea informatiilor catre utilizatori dupa reguli de vizualizare definite in administrare;
- reprezentarea rapoartelor in diferite forme grafice, dupa preferintele si necesitatile utilizatorului;
- includerea in cadrul rapoartelor de informatii geografice pe baza obiectelor de pe harta;
- structurile OLAP folosite vor putea fi
    - editate de catre utilizatorii autorizati;
    - accesate prin servicii web;
    - expuse pe web prin pagini HTML, unde utilizatorul poate manipula dimensiunile cubului dupa necesitatile analizei;
- existenta istoricului pe rapoarte;
- executarea rapoartelor la anumite ore, definite de utilizatori;
- export in HTML, XML, EXCEL, PDF;
- accesarea rapoartelor prin interfete web si transmiterea lor prin e-mail, pe baza unor subscriptii prealabile;
- posibilitatea definirii de indicatori de performanta;
- va asigura posibilitatea de a combina informatiile structurate cu cele nestructurate;
- va dispune de notificari de alerta astfel incat tot personalul relevant sa primeasca informatia importanta imediat.

3.5.5. Modul control preventiv euristic

Acest modul va permite realizarea de analize automate, de la simplu la complex, bazate pe pattern-uri sau metode euristice, menite sa identifice si sa semnaleze, in vederea intreprinderii de actiuni automate sau manuale, a situatiilor de deviatie monitorizate.

Utilitatea acestui modul rezida in posibilitatea de tratare a celor mai frecvente situatii de neconformitate procedurala sau inconsistenta administrativa a datelor intalnite in activitatea curenta de supraveghere si control derulata de IM: situatii in care un agent economic nu inregistreaza rapoartele periodice referitoare la angajati si la masurile de protectia muncii aplicabile acestora, precum si situatiile legate de lucrarile efectuate si locatiile in care isi desfasoara activitatea de teren anagajatii agentului economic (in special in domeniul constructiilor, domeniul extractiv si de manipulare a masinilor si utilajelor grele).

Modulul va fi bazat pe un motor de reguli configurabile, ce vor folosi ca date de intrare parametrii selectabili din baza de date (exemplu: data ultimei raportari primite de la agentul economic, frecventa raportarilor pe o perioada predefinita, amplitudinea variatiilor in parametrii raportati etc).

Prin aplicarea regulilor de validare si notificare, vor fi identificate situatiile de neconformitate si va fi generata o lista de actiuni aplicabile prin metode automate sau manuale in vederea tratarii deviatiilor: emiterea de notificari pe mail catre agentii economici vizati, notificarea in vederea initierii unui apel telefonic catre administratorul companiei, planificarea de activitati de control etc.).

3.5.6. Modul de consemnare activitati de control

Acest modul va permite centralizarea rezultatelor activitatii de control la nivel national, prin inregistrarea, evidenta si actualizarea controalelor efectuate de catre inspectori prin modalitati clasice, aflate in functiune la acest moment (controale de fond si controale prin sondaj). Informatiile gestionate includ unitatea controlata, tipul controlului, actiune, data Procesului verbal de control, alte informatii de interes. Procesele verbale de constatare si sanctionare contraventii vor putea fi incarcate in baza de date, ajutand astfel la crearea unei evidente complete a actiunii de control. Se pot incarca in sistem si toate informatiile privind neconformitatile constatate in urma controalelor efectuate;

Vor fi disponibile urmatoarele functionalitati, fara limitare:

- ✓ Verificarea locala a contractelor individuale de munca;

- ✓ Inregistrarea, evidenta si actualizarea autorizatiilor de protectia muncii;
- ✓ Inregistrarea, evidenta si actualizarea informatiilor referitoare la accidentele de munca;
- ✓ Informatii specifice ANAF si RC pentru agentii economici verificati;
- ✓ Vizualizarea dovezilor de aducere la indeplinire a masurior dispuse de inspectori;
- ✓ Evidenta proceselor verbale de control;
- ✓ Evidenta proceselor verbale de constatare si sanctionare a contraventiilor;
- ✓ Inregistrarea rezultatelor activitatii de control.

3.5.7. Modul de gestiune activitati de teren

Inspectorii care deruleaza activitati de control in teren vor utiliza dispozitive mobile ce le vor permite accesul on-line la informatiile relevante menite sa sprijine activitatea de control: angajati cu contract de munca la un agent economic, rapoartele de instruire in domeniul protectiei muncii inregistrate de catre angajatori, date descriptive pentru agentii economici cu provenienta de la ANAF si Registrul Comertului etc.

Inspectorii vor avea de asemeni posibilitatea completarii proceselor verbale de constatare a abaterilor, precum si rapoartele de control specifice.

Aceste informatii vor sta la baza rezolutiilor de stabilire a sanctiunilor aferente abaterilor inregistrate.

Pentru a asigura opozabilitatea formularelor on-line completate la fata locului prin intermediul dispozitivelor mobile, vor fi utilizate certificate digitale calificate, prin care vor fi semnate documentele generate in cadrul controlului.

Inspectorii vor avea acces la distanta cel putin la urmatoarele informatii/functionalitati, fara limitare:

- ✓ Verificarea din teren (la distanta) a contractelor individuale de munca;
- ✓ Inregistrarea, evidenta si actualizarea autorizatiilor de protectia muncii;
- ✓ Inregistrarea, evidenta si actualizarea informatiilor referitoare la accidentele de munca;
- ✓ Informatii specifice ANAF si RC pentru agentii economici verificati;
- ✓ Vizualizarea dovezilor de aducere la indeplinire a masurior dispuse de inspectori;
- ✓ Evidenta proceselor verbale de control;
- ✓ Evidenta proceselor verbale de constatare si sanctionare a contraventiilor.

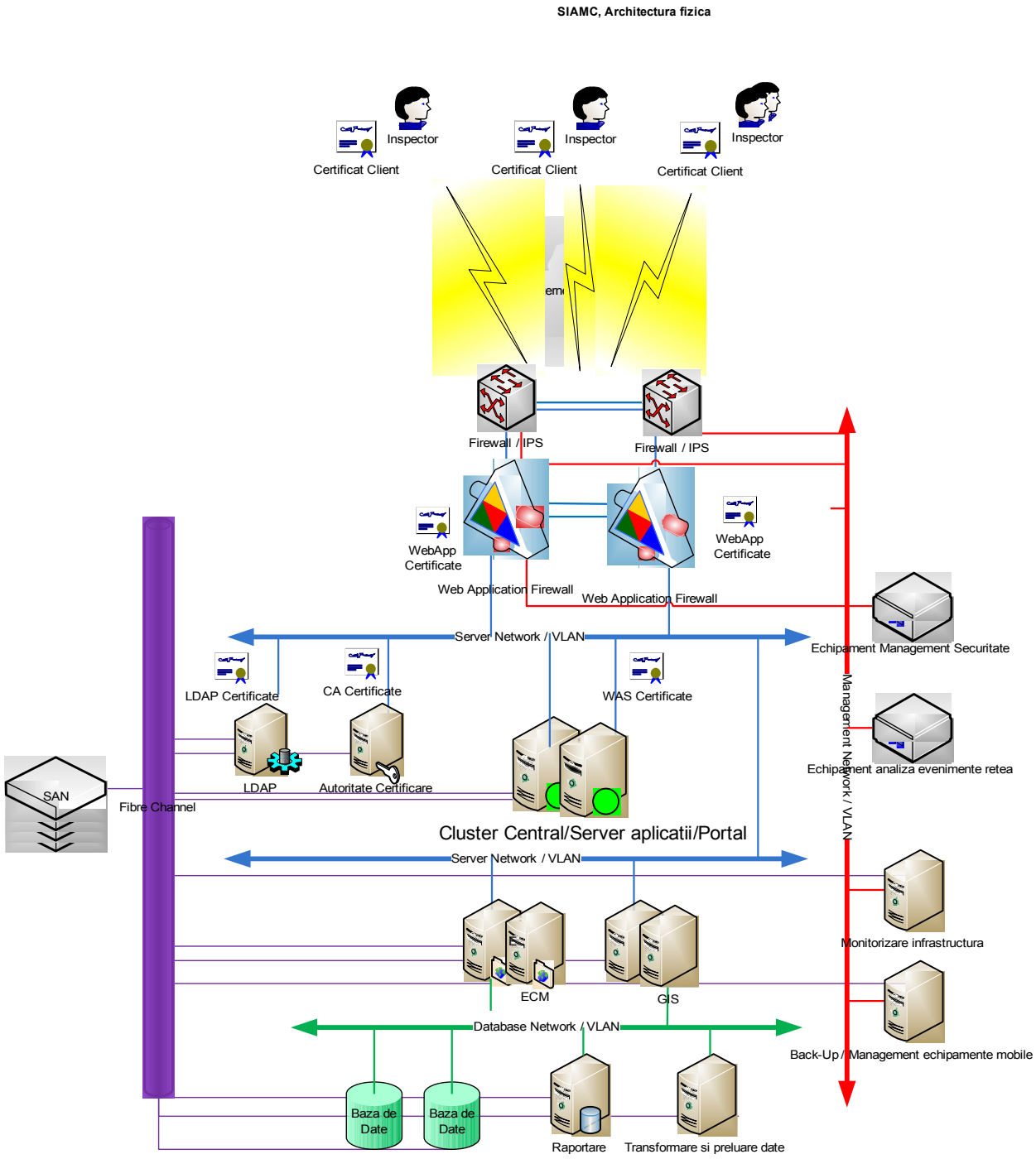
3.5.8. Modul gestiune centralizata accidente de munca

Acest modul permite inregistrarea, evidenta si actualizarea accidentelor de munca individuale si colective. Datele care se vor pastra sunt legate de: informatii de identificare a unitatii unde s-a petrecut accidentul, numele celor accidentati, locul de munca, detalii despre ocupatie, vechime in munca, numarul victimelor, tipul accidentului, gravitatea lui, imprejurarile in care s-a petrecut, cauzele producerii, timpul in care s-a petrecut, consecintele accidentului, descrierea modului in care s-a produs accidentul etc.

3.5.9. Modul transformare si preluare date din REGS, de la ANAF, DEPABD si ONRC

Functionalitatile acestui modul permit accesarea si transpunerea intr-un format utilizabil a informatiilor disponibile preluate de la din sistemul REGES, precum si din sistemele de la ANAF, DPABD si Oficiul National al Registrului Comertului. Toate interogarile efectuate de catre restul de module ale SIAMC care implica informatii referitoare la agentii economici investigati vor fi intermediate de catre acest modul, in vederea transformarii corespunzatoare a informatiilor relevante.

3.6. Arhitectura tehnica



Arhitectura sistemului informatic integrat SIAMC prezentata in diagrama anterioara este orientativa, dar Ofertantul trebuie sa includa cel putin toate componentele solicitate in cadrul Caietului de Sarcini. In oferta tehnica, acesta va include arhitectura conform solutiei propuse.

3.6.1. Cerinte de baza

Arhitectura sistemului integrat SIAMC trebuie sa indeplinesca urmatoarele cerinte de baza:

Accesibil:

Serviciile electronice oferite vor fi furnizate utilizatorilor folosind o interfata grafica simpla, ce va permite accesul nerestrictionat unui numar cit mai mare de utilizatori. Design-ul interfetei grafice va fi realizat in functie de nevoile utilizatorilor pentru a le permite acestora accesul rapid la toate serviciile electronice, formularele si informatiile de interes public. Formularele si structura serviciilor din cadrul portalului va avea o prezentare standard, facilitind astfel claritatea, navigabilitatea si usurinta de folosire. Portalul va oferi posibilitatea de acces personalizat (prin pagini personalizate ale utilizatorilor), facilitate care va usura mult navigarea si inregistrarea diferitelor solicitari.

Accesul utilizatorilor la serviciile electronice nu va fi ingradit in nici un fel, in sensul ca nu va exista o limitare a numarului maxim de utilizatori logati.

Serviciile electronice vor fi disponibile si pe dispozitive de tip infochiosc iar aplicatia va fi astfel personalizata pentru a putea fi accesata intr-un mod facil folosind echipamente mobile.

Aplicatia informatica va fi astfel proiectata incat va eficientiza toate fluxurile interne ale IM si ITM in functie de nevoile cetateanului.

Eficient:

Procedurile vor fi clare si directe, formularele mai usor de completat, datele vor fi mai usor de prelucrat, gradul de responsabilizare si siguranta va creste, iar administratia publica isi va eficientiza activitatea (costurile vor fi scazute, vor fi promovate serviciile cu impact ridicat, va creste productivitatea muncii angajatilor, etc.)

Implementarea proiectului va avea un impact pozitiv direct asupra intregii activitatii a institutiei. Asfel va creste eficienta muncii angajatilor institutiei prin reducerea aglomeratiei de la ghiseu, se va reduce timpul de procesare a informatiilor, se vor reduce costurile de furnizare a informatiilor prin economia de hartie ce se va realiza.

Eficace:

Oferirea alternativei electronice la serviciile clasice, precum si automatizarea activitatilor inspectorilor IM va genera o reducere a timpului de prestare a serviciilor si spori confortul utilizatorilor interni si al cetatenilor, acestia din urma putand beneficia de o interactiune online

directa cu Inspectoratele Teritoriale de Munca si cu Inspectia Muncii, eliminindu-se barierele birocratice.

Inovativ si neutru tehnologic:

Aplicatia este proiectata astfel incat solutiile ce vor fi folosite la implementare sa fie neutre tehnologic pentru a permite dezvoltari continue. Astfel aplicatia informatica este inovativa si poate fi dezvoltata continuu in functie de necesitati, fara restrictii.

Sigur - protejarea confidentialitatii datelor furnizate de utilizatori:

Proiectul propus va respecta prevederile legislatiei in vigoare care asigura confidentialitatea datelor cu caracter personal si cea privind dreptul de informare al cetateanului:

- Legea nr. 506/17.11.2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice completata cu prevederile Legii nr. 677/21.11.2001 privind protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date.
- Legea nr. 52/21.01.2003 privind transparenta decizionala în administratia publica;
- Ordinul Avocatului Poporului nr. 52/18.04.2002 privind aprobarea Cerintelor minime de securitate a prelucrarilor de date cu caracter personal.

Scalabil:

Aplicatia informatica trebuie sa faca fata unui nivel de incarcare continuu crescator, fara a-i fi diminuata performanta. Componentele majore ale arhitecturi de sistem ce se vor supune scalabilitatii vor fi: topologiile si sistemele de retea, serverele de aplicatii, serviciile de infrastructura, componentele de management al infrastructurii si subsistemele responsabile de stocarea datelor.Sistemul nu trebuie sa permita pierderea datelor, in acest sens fiind necesare capabilitati de restaurare in caz de accident si modalitati de prevenire a acestora. Totodata, arhitectura de sistem va avea o componenta de securizare a infrastructurii care sa nu permita accesul neautorizat la date.

Aplicatia electronica ce urmeaza a fi implementata va fi interconectata cu Sistemul Electronic National, conform Legii nr. 161/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei, cu modificari si completari ulterioare, respectind conditiile tehnice in care se poate asigura interconectarea.

3.6.2. Componentele sistemului integrat SIAMC

Din punct de vedere logic, SIAMC va fi dispus pe trei niveluri, respectiv nivelul de platforma de baza, nivelul de logica de business si nivelul de prezentare.

Nivel	Componenta
1. Platforma de baza	
	Hardware
	Sisteme de comunicatii
	Sisteme de operare
	Platforma de monitorizare hardware
	Platforma back-up si restaurare
	Antivirus
2. Nivel logica de business	
	Platforma fluxuri configurata
	Platforma baza de date
	Platforma Raportare si BI configurata
	Server GIS
	Platforma transformare date configurata
	Platforma colaborare configurata
	Platforma certificate digitale
	Modul gestiune sesizari on-line
	Modul control preventiv euristic
	Modul consemnare rezultate control
3. Nivelul de prezentare	
	Platforma Portal

3.6.3. Infrastructura hardware

Comunicarea in cadrul sistemului informatic si de comunicatii se poate realiza intr-un sistem inchis (VPN). Sistemul intern trebuie sa fie protejat de un sistem de firewall-uri care limiteaza traficul prin politici stricte de access, pentru functionarea in conditii de securitate ridicata a aplicatiilor. Serverele de aplicatii vor fi relationate cu serverele de baze de date integrate intr-un sistem de stocare.

3.6.3.1. Cerinte generale echipamente hardware si sistem de comunicatii

In vederea alcatuirii unei solutii si arhitecturi complete de infrastructura (hardware, comunicatii si software de sistem) de nivel “enterprise” este necesara achizitionarea echipamentelor si componentelor corespunzatoare cerintelor aplicatiilor propuse.

Toate echipamentele active trebuie sa functioneze la 230V AC, 50Hz, valori nominale specifice Romaniei.

Solutia trebuie sa asigure suportul necesar tuturor componentelor sistemului la un nivel inalt de performanta si fiabilitate, furnizand in acelasi timp baza pentru dezvoltari ulterioare din punct de vedere software si hardware - scalabilitate. De asemenea, platforma trebuie sa asigure un grad crescut de flexibilitate, astfel incat eventuale noi cerinte ale beneficiarului sa poata fi usor aplicate.

Solutia propusa trebuie sa asigure un mare grad de disponibilitate a aplicatiilor. Acest lucru se obtine prin oferirea de redundanta la nivelul:

- serverelor (prin folosirea de echipamente cu surse redundante si cu capacitati hot-plug, prin folosirea de hard-diskuri interne in configuratie RAID (mirroring recomandat), a ventilatoarelor redundante si alte capabilitati RAS);
- folosirea de arhitecturi de tip cluster pentru componentele sistemului (serverul de aplicatii si serverul de baza de date, dar si serverul de front end – portal). Arhitectura de tip cluster asigura inalta disponibilitate a aplicatiilor ce ruleaza pe nodurile clusterelor si asigura practic disponibilitatea aplicatiilor pentru utilizatorii acestora chiar in cazul in care unul din nodurile (serverele) din cluster nu mai poate deservi serviciile sale acestea fiind preluate de celalalt nod fara un down-time notabil pentru utilizatori pana la repunere in functie a serverului respectiv;
- folosirea de storage centralizat de tip SAN (Storage Area Network) cu capacitati hot-plug pentru unitatile de stocare;
- echipamentele de retea (switch-urile) vor oferi o inalta disponibilitate a comunicatiei in retea locala a Data Center-ului in care sunt interconectate toate serverele ce gazduiesc aplicatiile tuturor subsistemelor.

Sistemul informatic trebuie sa fie capabil sa functioneze utilizand reteaua de comunicatii care prezinta urmatoarele caracteristici tehnice minimale:

- Conexiuni permanente la o capacitate minim garantata si nepartajata de 2 MB/locatie si o capacitate de acces minima garantata in internet pentru portalul public de 8 MB;
- Trafic nelimitat;
- Posibilitatea upgradarii ulterioare de banda fara costuri initiale;
- Timpul de intrerupere nu va fi mai mare de 24 de ore pentru o singura defectiune.

Subsistemul hardware presupune realizarea unui datacenter la nivelul institutiei (compus din echipamentele achizitionate in cadrul proiectului), ce se va integra cu componentele existente.

Echipamente necesare	Cantitate
Sasiu servere lamelare	1
Servere lamelare	14
Echipament de stocare centralizata	1
Infrastructura de gazduire a echipamentelor	1
Infrastructura de alimenatre cu energie electrica protejata cu UPS-uri	1
Firewall	2
Firewall aplicatie	2
Echipament analiza logurilor	1
Managementul echipamentelor	1
Managementul echipamentelor mobile	1
Aer conditionat pentru camera serverelor	1
Terminale mobile	1000

3.6.3.2. Securizarea sistemului de comunicatii

Securizarea sistemului de comunicatii se va baza pe echipamente instalate in cluster (High-Availability) activ-activ, pentru redundanta. Produsele vor fi instalate in mod NAT/Route si vor realiza urmatoarele functionalitati:

- Router (inclusiv BGP, daca este cazul);
- State-full Firewall;
- Gateway Antivirus, cu antispyware (HTTP, FTP, IMAP, POP3, SMTP);
- Intrusion Prevention System (IPS);
- Web Filtering;
- Antispam;
- Traffic Shaping;
- Instant Messenger/Peer-to-Peer Access Control.

Cerintele tehnice detaliate pentru echipamente sunt prezentate in capitolul FIrewall.

Pentru o redundanta completa a conexiunii la Internet, Beneficiarul intentioneaza sa puna la dispozitie conexiune la Internet de la 2 provideri diferiti, astfel incat este nevoie ca SIAMC sa fie pregatit pentru acest scenariu.

3.6.3.3. Sasiu servere lamelare

Sasiu servere lamelare – 1 buc.	
Descriere generala	Sasiu rackmountable, maximum 10U, oferind o densitate mai mare de 1,6 servere/U
Arhitectura	Arhitectura complet redundanta pentru asigurarea unei inalte disponibilitati a sistemului

Caracteristici de inalta disponibilitate	Back-plane de mare viteza si latenta redusa care sa asigure minim patru canale de comunicatie redundante per blade. Tehnologia utilizata pentru conectivitate trebuie sa permita gruparea logica a oricaror doua sau mai multe porturi Ethernet / Fiber Channel, corespunzand oricarui slot pentru servere blade din sasiu, intr-un singur port extern ale carui caracteristici (MAC, WWN) nu se vor schimba atunci cand un server blade este inlocuit.
Capacitate servere	Minim 14 servere
Capacitate module switch	Minim 8 module cu suport pentru Gigabit Ethernet, 10 Gigabit Ethernet, 8Gbps Fibre Channel, InfiniBand QDR si FDR, FcoE, SAS
Echipare module switch	Module switch redundante atat pentru conectarea in LAN cat si pentru conectarea in SAN
Alimentare cu energie electrica	Surse de alimentare redundante in cantitate suficienta pentru alimentarea tuturor serverelor
Management sistem	Module de management centralizat pentru intregul sasiu, redundante, hot-plug. Suport pentru management de la distanta, redirectare interfata grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta pentru fiecare server blade, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer), integrare LDAP (Lightweight Directory Access Protocol). Fiecare modul de management trebuie sa dispuna de 2 x USB, 1 x serial (RS-232), 2 x RJ-45 pentru conectare la LAN/WAN.
Conditii de livrare	Garantie minim 1 an

3.6.3.4. Servere lamelare

Servere lamelare – 14 buc.	
Arhitectura	Server in arhitectura x64 cu minim 2 socket-uri
Procesoare	2 procesoare x64 multicore
Nuclee de procesare	Minim 4 nuclee/procesor
Memorie instalata	32 GB memorie RAM utila dupa configurarea mecanismului de mirroring
Memorie maxima	1TB

Interfete instalate	Interfete redundante atat pentru conectarea in LAN cat si pentru conectarea in SAN cu o latime de banda totala de minim 20 Gbps
Sloturi de expansiune	Minim 2 sloturi interne disponibile (libere) pentru carduri de acces la modulele switch cu interfata PCI-Express 3.0 x8
Stocare interna	Minim 100GB spatiu de stocare util realizat dintr-o matrice RAID 1 sau 10 din unitati tip SSD
Conditii de livrare	Garantie minim 1 an

3.6.3.5. Echipament de stocare centralizata

Echipament de stocare centralizata – 1 buc.	
Descriere generala	Sistem de stocare centralizata cu minim 2 controllere redundante si hot-plug, cu failover automat.
Arhitectura	Arhitectura complet redundanta pentru asigurarea unei inalte disponibilitati a sistemului
Acces hosturi	Porturi de acces redundante pe fiecare controller
Protocoale de acces	FCP, iSCSI, NFS, CIFS, HTTP . Sistemul se va livra cu toate protocoalele activate. Sistemul trebuie sa permita utilizarea simultana a tuturor protocoalelor de acces .
Porturi de acces	4 porturi FC 8Gbps, instalate, SFP-uri incluse 8 porturi Ethernet 1Gbps, instalate, SFP-uri incluse Sistemul trebuie sa ofere suport pentru porturi 10Gbps Ethernet.
Memorie cache instalata	12 GB
Capacitate utila de nivel 1	Minim 3,5TB spatiu util format din discuri SAS cu o viteza de rotatie de cel putin 10.000 rpm
Capacitate utila de nivel 2	Minim 10TB spatiu util format din discuri NL-SAS sau SATA cu o viteza de rotatie de cel putin 7.200 rpm
Protectia datelor pe disc	Sistemul trebuie sa permita implementarea de matrici RAID si a discurilor de tip hot-spare. Echipamentul trebuie sa asigure conectarea catre fiecare unitate HDD prin intermediul a doua cai de access redundante cu fail over automat.
Redundanta sistemului si suportul pentru operatiuni de	Sistemul trebuie sa includa surse de alimentare redundante. Sistemul trebuie sa includa controllere, surse de alimentare

intretinere fara intreruperea serviciilor	si discuri in tehnologie HotSwap – extragerea, completarea sau inlocuirea lor sa poata fi realizata on line. Adaugarea unitatilor de expansiune trebuie sa poata fi realizata online fara intreruperea conexiunilor cu unitatile de expansiune deja instalate.
Conectivitate (hosts)	Numarul minim de host-uri suportate trebuie sa fie de cel putin 256.
Sisteme de operare (host) suportate si certificate	Sistemele de operarea minim certificate trebuie sa fie: Microsoft Windows 2003, 2008, VMware ESX, RedHat Linux, Suse Linux, IBM AIX, HP-UX, SUN Solaris, Mac© OS. Sistemul de stocare trebuie sa fie livrat impreuna cu driverele de multipath si load balancing incluse in configuratia propusa.
Sertare de expansiune	Sertarele de expansiune trebuie sa suporte cel putin urmatoarele tipuri de discuri: SSD, FC, SAS, SATA si discuri cu autocriptare.
Scalabilitate	Configuratia livrata trebuie sa ofere posibilitatea de upgrade a numarului de discuri cu cel putin 50%, fata de numarul discurilor instalate, fara a necesita o achizitie ulterioara de sertare pentru discuri. Sistemul ofertat trebuie sa suporte minim 140 HDD prin adaugare de sertare suplimentare. Sistemul ofertat trebuie sa fie capabil sa scaleze intern, prin inlocuirea controllerelor existente cu controllere superioare, fara migrarea datelor stocate, minim 700 HDD. Sistemul trebuie sa fie capabil sa scaleze extern, prin mecanisme de tip cluster la nivelul controllerelor si consolidarea capacitatii de stocare, minim 6 controllere.
Functionalitati software la nivel de controller	Sistemul trebuie sa permita realizarea copiilor locale instantanee – tip Snapshot Sistemul trebuie sa suporte restaurarea instantanee a copiilor tip snapshot

	Sistemul trebuie suporte realizarea copiilor locale integrale tip Clona Sistemul trebuie sa suporte realizarea de clone locale virtuale ale seturilor de date. Sistemul trebuie sa suporte realizarea copiilor la distanta a seturilor de date, in maniera sincrona si asincrona, atat prin porturi FC cat si prin porturi Ethernet. Sistemul trebuie sa suporte backup si restaurare disk-to-disk pe un echipament secundar din aceeasi gama. Sistemul trebuie sa suporte definirea de volume tip WORM Toate functionalitatile mentionate mai sus trebuie sa fie active (licentiate daca este cazul) pentru intreaga capacitate de stocare.
Functionalitati software de eficientizare a spatiului	Echipamentul trebuie sa permita utilizarea mecanismelor de tip Thin Provisioning sau echivalent: mecanismul trebuie sa permita alocarea catre servere a unor capacitati mai mari decat cele instalate fizic in interiorul sistemului de stocare. Echipamentul trebuie sa permita deduplicarea datelor stocate atat la nivel de bloc cat si la nivel de fisier, in mod transparent pentru serverele host. Ecipamentul trebuie sa suporte compresia datelor stocate, in mod transparent pentru serverele host. Toate functionalitatile mentionate mai sus trebuie sa fie active (licentiate daca este cazul) pentru intreaga capacitate de stocare.
Optimizarea performantei	Echipamentul trebuie sa dispuna de un mecanism de prioritizare a accesului aplicatiilor la volumele de date, cu cel putin 5 nivele de prioritate implementate. Toate functionalitatile mentionate mai sus trebuie sa fie active (licentiate daca este cazul) pentru intreaga capacitate de stocare.

Integrarea serviciilor de copiere pentru back-up la nivel de aplicatii	Echipamentul trebuie sa ofere suport la nivel de controler pentru functionalitati de backup si restaurare prin care sa asigure protectia datelor in maniera consistenta cel putin pentru: MS Windows, Linux, Exchange, SQL Server, SharePoint, Oracle, SAP, VMware si Hyper-V. Operatiunea de backup trebuie sa se realizeze fara oprirea serviciilor la nivel de aplicatie. Toate functionalitatile mentionate mai sus trebuie sa fie active (licentiate daca este cazul) pentru intreaga capacitate de stocare.
Conditii de livrare	Garantie minim 1 an

3.6.3.6. Infrastructura de gazduire a echipamentelor

Infrastructura de gazduire a echipamentelor – 1 buc.	
Rack	19”, minim 25U, inclusiv toate accesoriile necesare cum ar fi panouri pentru acoperirea unitatilor nefolosite
Consola rack Ecran rabatabil cu diagonala de minim 17” cu tastatura si pointing device integrat	Ecran rabatabil cu diagonala de minim 17” cu tastatura si pointing device integrat
Conditii de livrare	Garantie minim 1 an

3.6.3.7. Infrastructura de alimentare cu energie electrica protejata cu UPS-uri

Infrastructura de alimentare cu energie electrica protejata cu UPS-uri – 1 buc.	
UPS-uri	Minim 2 UPS-uri redundante, fiecare capabil sa asigure alimentarea tuturor echipamentelor
Infrastructura de interconectare	PDU-uri si cabluri in cantitatea suficienta pentru conectarea in mod redundant a tuturor echipamentelor la UPS-uri
Conditii de livrare	Garantie minim 1 an

Obs.: UPS-urile ofertate trebuie sa asigure o autonomie de minim 10 minute pentru echipamantele protejate. Ofertantul va include in oferta tehnica calculul consumului energetic al tuturor echipamentelor ofertate pentru a demonstra capacitatea UPS-urilor ofertate de a indeplini cerinta.

3.6.3.8. Firewall

Firewall - 2 buc configuratie in cluster	
Porturi 10/100/1000BaseT	Minim 8 porturi accelerate hardware
Stocare interna	Minim 32 GB
Performanta firewall	Minim 8Gbps pentru orice dimensiune a pachetelor Minim 12 Mpps
Sesiuni	Minim 50000 sesiuni noi pe secunda
Performanta VPN	Minim 4.5 Gbps
Politici firewall	Minim 10000
Numar de tunele VPN	Minim 2000 tunele VPN
Performanta IPS	Minim 1.2 Gbps
Performanta SSL VPN	Minim 200 Mbps
Performanta antivirus	Minim 200 Mbps
Domenii virtuale	Minim 10
Conditii de livrare	Garantie minim 1 an incluzand toate licentele software pentru IPS, VPN, SSL si Antivirus

3.6.3.9. Firewall aplicatie

Firewall Aplicatie (Layer 7) - 2 buc configuratie in configuratie activ/pasiv	
Porturi 10/100/1000BaseT	Minim 4 porturi cu bypass hardware si 2 porturi fara bypass Minim 2 porturi SFP
Stocare interna	Minim 2 TB
Performanta firewall	Minim 500 Mbps
Sesiuni HTTP	Minim 25000 sesiuni noi pe secunda
Protectie si monitorizare	Protectie la nivel aplicatie impotriva vulnerabilitatilor; Prevenirea scurgerii de date; Support pentru o varietate mare de aplicatii; Protectie la expunerea datelor confidentiale pe web; Evaluarea Vulnerabilitatilor; Validarea pachetelor conform RFC HTTP; Antivirus.
Protectie la urmataorele atacuri	Cross Site Scripting; Cookie Tampering / Poisoning; Atacuri prin intermediul carora utilizatorii sunt forttai sa execute actiuni ndeorite in cadrul unei aplicatii web in care este autentificat (CSRF); Injectare cu cod SQL;

	Injectare si executare de comenzi; Incarcare de fisiere malitioase (RFI); Deturnarea sesiunii; Forms Tampering; Hidden Field Manipulation; Outbound Data Leakage; HTTP Request Smuggling; Encoding Attacks; Broken Access Control; Forceful Browsing; Directory Traversal; Site Reconnaissance; XML Parameter Tampering si Intrusion Prevention; Search Engine Hacking; Atac de tip autentificare Brute Force; Access Rate Control; Schema Poisoning; Scanare WSDL; Atac de tip refuz/blocare serviciu (DoS); Recursive Payload; External Entity Attack; Buffer Overflows.
Conditii de livrare	Garantie minim 1 an incluzand maximum de licentiere software

3.6.3.10. Echipament analiza logurilor

Echipament analiza logurilor - 1 buc	
Porturi 10/100/1000BaseT	Minim 4
Stocare interna	Minim 1 TB
Dimensiunea zilnica a logurilor suportata	Minim 5GB/zi
Numarul de sesiuni suportate pe zi	Minim 18M
Durata medie de retinere a	Minim 3 luni

logurilor	
Numarul minim de echipamente suportate	Minim 100
Functionalitati	Corelarea evenimentelor din retea; Rapoarte Grafice; Performanta si capacitate scalabila; Permite stocarea mai multor formate de log; Integrare nativa cu restul echipamentelor de retea; Functionalitate de colector, analizor sau amandoua;
Tipuri de rapoarte	Vizualizarea tipurilor de trafic; Vizualizarea continutului traficului: HTTP, FTP, email, mesagerie instant; Vizualizarea evenimentelor de securitate; Vizualizarea sumarului pentru trafic; Vizualizarea celor mai mari generatori de trafic; Cel putin 400 de rapoarte predefinite.
Conditii de livrare	Garantie minim 1 an

3.6.3.11. Managementul echipamentelor

Managementul echipamentelor - 1 buc	
Porturi 10/100/1000BaseT	Minim 4
Stocare interna	Minim 1 TB
Licenta pentru managementul echipamentelor de retea	Pentru minim 30 de echipamente de retea
Numarul de domenii administrate	Minim 25 de domenii administrate
Posibilitatea de definire a politicilor globale	Solicitat
Alte functionalitati	Baza de date orientata pe obiecte; Management centralizat pentru echipamente de retea; Permite configurarea de politici centralizate; Permite provizionarea de echipamente in mod automat; Administrare de tip role-based; Permite auditarea politicilor si a echipamentelor; Functionalitate Drag and Drop;

	Permite crearea de profile pentru echipamente; Detine APIP XML.
Conditii de livrare	Garantie minim 1 an

3.6.3.12. Managementul echipamentelor mobile

Managementul echipamentelor mobile - 1licenta software	
Functionalitati securitate	Solutia trebuie sa permita managementul centralizat al parolelor pe echipamentele mobile atat prin intermediul componentei LDAP, cat si pentru utilizatorii creati local in componenta de management centralizat al parolelor; Solutia trebuie sa faciliteze criptarea componentei de stocare a echipamentelor mobile prin intermediul politicilor de securitate sau alta metoda echivalenta; printre algoritmii de criptare trebuie sa regaseasca cel putin AES-256; Solutia trebuie sa permita restrictionarea utilizatorilor la anumite aplicatii sau functionalitate ale echipamentelor mobile; Trebuie sa permita definirea de reguli pentru activitatile care incalca politica de securitate sau pentru echipamente compromise, cel putin urmatoarele: • trimiterea unei alerte daca dispozitivul nu a mai comunicat cu consola de management pentru un anumit numar de zile; • daca modificarile la politicile trimise nu au fost aplicate intr-un numar de zile; • daca criptarea datelor de pe dispozitiv a fost dezactivata. Solutia trebuie sa suporte mecanisme de autentificare cu 2 factori; Solutia trebuie sa permita integrarea cu o infrastructura de chei publice existenta; Solutia va trebui sa permita integrarea securizata cu protocoale standard de autentificare cum este LDAP fara a

	deschide porturile de aplicatie LDAP catre exterior; Solutia trebuie sa permita securizarea dispozitivelor prin implementarea unei politici de credentiale de acces, care sa presupuna stabilirea complexitatii, perioadei de activitate si istoricului credentialelor; Solutia trebuie sa ofere protectie impotriva incercarilor de a aflare a credentialelor de acces la dispozitiv prin atacuri de tip brute-force. La detectarea unui astfel de atac, in functie de anumite criterii, solutia trebuie sa ofere functionalitatea de stergere a datelor de pe dispozitiv; Solutia trebuie sa permita integrarea cu o autoritate de certificare intr-o structura PKI existenta; Solutia trebuie sa permita distribuirea de certificate digitale dispozitivelor si utilizatorilor in mod dinamic si automat; Distributia certificatelor trebuie sa se poata personaliza prin stabilirea de grupuri, in functie de dispozitiv sau in functie de utilizator.
Functionalitati de configurare	Trebuie sa permita definirea de profile; Trebuie sa faciliteze aplicarea anumitor politici in functie de localizarea geografica a echipamentelor mobile; Trebuie sa permita definirea de profile active in anumite perioade orare; Trebuie sa permita integrarea cu autoritati de certificare si utilizarea certificatelor digitale; Trebuie sa permita managementul aplicatiilor instalate pe echipamentele mobile (cel putin publicarea aplicatiilor); Publicarea de aplicatii trebuie efectuata in mod nativ fara a fi necesara nicio alta componenta software. Solutia trebuie sa permita publicarea de aplicatii doar pentru anumiti utilizatori sau grupuri in conformite cu directorul LDAP; Trebuie sa permita distributia de continut (documente)

	catre echipamente mobile in mod securizat; Solutia trebuie sa contina sabloane de profile de gestionare a dispozitivelor, dar sa permita si crearea de profile noi, personalizabile; Solutia trebuie sa permita provizionarea dispozitivelor mobile cu configuratii pentru setarea conexiunilor fara fir, a celor de tip VPN si instalarea certificatelor digitale. In cazul conexiunilor fara fir, acestea trebuie sa suporte minim WPA2 Personal si WPA2 Enterprise cu protocoalele PEAP, MS-CHAPv2, TTLS si TLS. In cazul conexiunii VPN trebuie sa suporte cel putin protocoalele PPTP, L2TP, IPSEC si SSL.
Functionalitati de monitorizare	Trebuie sa furnizeze un dashboard: solutia trebuie sa contina functionalitati de tipul tabloului de bord in care sa fie afisate informatii despre dispozitivele gestionate, statutul lor (activ, inactiv, blocat, retras etc.), sistemul de operare, in functie de criterii prestabilite cum ar fi perioada. Trebuie sa permita monitorizarea localizarii echipamentelor mobile; Trebuie sa permita gestiunea alertelor la incalcarea politicilor definite; Trebuie sa furnizeze un motor de reguli pentru a determina conformitatea cu politicile de securitate; Trebuie sa faciliteze raportarea si distributia automata a rapoartelor; Solutia trebuie sa contina functionalitati de inventariere a dispozitivelor inregistrate care sa cuprinda detalii despre fiecare dispozitiv, cat si posibilitatile de a actualiza informatiile, de a retrage dispozitivul din uz si de a-l clasifica in functie de criterii prestabilite sau

	personalizabile; Solutia trebuie sa contina functionalitate de jurnalizare si inregistrare a evenimentelor de sistem, a evenimentelor privind gestionarea dispozitivelor mobile, a evenimentelor legate de certificate digitale.
Functionalitati generale	Trebuie sa permita controlul la distanta asupra echipamentelor mobile prin aplicarea la cerere sau programata de politici; Trebuie sa permita diagnosticarea la distanta a echipamentelor mobile, respectiv a conformitatii cu politicile de securitate; Trebuie sa faciliteze managementul centralizat al echipamentelor mobile, cel putin prin crearea de grupuri si etichete personalizabile. Trebuie sa ofere posibilitatea ca un echipament mobil sa faca parte din mai multe grupuri; Solutia trebuie sa poata fi accesata si gestionata cu usurinta de oriunde prin intermediul unui browser web; Solutia nu trebuie sa fie dependenta de un anume sistem de operare; Solutia trebuie sa poata fi integrata cu usurinta in infrastructura existenta, fara modificari substantiale, atat intr-un mediu fizic, cat si intr-un mediu virtual; Solutia trebuie oferita impreuna cu documentatia tehnica aferenta; Solutia de gestionare a dispozitivelor mobile trebuie sa aiba suport nativ pentru urmatoarele platforme software: Android, iOS , OS X, Windows 8, Symbian, Windows Mobile, Windows Phone, BlackBerry 10; Solutia trebuie sa fie compatibila cu browserele folosite la scara larga cum ar fi Internet Explorer 8 sau mai nou, Firefox 14 sau mai nou, Safari 4 sau mai nou.
Conditii de livrare	Garantie si updateuri minim 1 an

3.6.3.13. Aer conditionat pentru camera serverelor

Aer conditionat pentru camera serverelor	
Capacitate BTU/h	21000
Rece Kcal/h	5000
Rece W/h	6115
Tensiune / Frecventa	220-240V/50 Hz
Corent nominal	11 A
Cantitate aer recirculat	920 m3/h
Nivel zgomot	48 dB
Dezumidificare	2 l/h
Greutate unitate interna	20 kg
Greutate unitate externa	70 g

Obs.: Ofertantul va include in oferta tehnica calculul caldurii degajate de echipamentele oferite. In cazul in care totalitatea echipamentelor instalate in cadrul acestui proiect necesita o capacitatea de racire mai mare de 21.000 BTU/h, ofertantul are obligatia sa includa in oferta unul sau mai multe echipamente pentru generarea aerului conditionat cu o capacitate de racire suficienta pentru a acoperi intreg necesarul de racire.

3.6.3.14. Terminale mobile

Terminale mobile – 1000 buc.	
Procesor	Cu patru nuclee, frecventa minim 1.3 GHz, minim 2MB cache
Memorie RAM	2 GB
HDD	64 GB eMMC
Placa video	Integrata
Placa audio	Integrata, difuzor integrat, microfon integrat
Conectivitate integrata	WLAN 802.11 b/g/n Bluetooth 4.0
Porturi integrate	1 x microUSB 1 x audio combo (casti si microfon)
Sloturi integrate	1 x microSD
Greutate si dimensiuni	Greutate maxim 0,4 kg incluzand bateria
Baterie	Polymer, capacitate cel putin 3000 mAh sau asigurand minim 6 ore de functionare
Sistem de operare	Inclus
Suita programe de birou	Inclus Tip Office
Display	- de tip IPS multi touch, diagonala minim 8 inch - rezolutie minim 1280 x 800 WXGA
Facilitati si metode de introducere a datelor	Suport pentru stylus
Alte facilitati	- minim 2 x webcam integrate: una frontala cu cel putin 2MP

	rezolutie si una pe spate cu cel putin 5MP rezolutie - suport pentru recunoastere faciala - protectie magnetica detasabila si stilou pentru sarcini de productivitate in timpul deplasarii incluse

3.6.4. Cerinte sisteme software de baza

Aceasta componenta va asigura o baza solida pentru toate celelalte module ale sistemului. Principalele functionalitati ale acestui subsistem sunt

- Asigurarea unui suport software robust si fiabil
- Asigurarea unui suport de stocare a informatiilor robust si scalabil pentru a permite stocarea unui numar foarte mare de informatii acumulate
- Asigurarea unei arhitecturi deschise la integrarea cu alte institutii.

3.6.4.1. Sisteme de operare

Sistemul de operare pentru servere trebuie sa asigure cel putin urmatoarele:

- Functionalitati privind Sistemele de fisiere;
- Functionalitati de Management al accesului;
- Functionalitati de Tiparire;
- Functionalitati de Stocare;
- Suport pentru integrarea cu servicii de Directory – Server de LDAP;
- Functionalitati privind Retele si comunicatii;
- Functionalitati privind Securitatea;
- Functionalitati privind Administrare remote;
- Suport pentru optimizarea fluxului de lucru al administratorului pentru gasirea rapida a obiectelor din director;
- Asistenta eficienta in gasirea obiectelor in directoare mari;
- Impact redus asupra serviciilor director in retea;
- Suport pentru implementare serviciu de director in virtualizare;
- Suport pentru clonarea serverelor cu rolul de serviciu de director;

- Capacitate flexibila de interogare pentru gasirea obiectelor in director, bazata pe atributele acestora;
- Serviciul de director pentru administrarea identitatilor trebuie sa reduca complexitatea administrarii directoarelor disparate, sa scada complexitatea asigurarii redundantei si sa creasca calitatea si accesibilitatea prin federalizarea mediului de director;
- Sa permita folosirea structurii de director, constand din servicii de director pentru administrarea identitatilor si servicii de meta-director in scopul imbunatatirii administrarii;
- Serviciile de director pentru administrarea identitatilor trebuie sa suporte RFC 1823;
- Monitorizarea, operatiunile si restaurarea directorului pentru administrarea identitatilor trebuie sa poata fi delegate;
- Serviciile de director pentru administrarea identitatilor trebuie sa poata suporta replicarea continutului;
- Serviciul de director trebuie sa prezinte posibilitatea de modificare a topologiei infrastructurii, configuratiei si procedurilor operationale printr-un proces de administrarea a schimbarii, iar modificarile sa poata fi delegate;
- Structura de director trebuie sa poata fi administrata direct de un utilizator sau de aplicatie;
- Trebuie sa ofere posibilitatea modificarii accesului serviciului de director si a procedurilor de administrare;
- Serviciul de director de management al identitatilor trebuie sa aiba un singur root;
- Spatiul de nume al serviciului de director pentru administrarea identitatilor trebuie sa poata fi partitionat intr-un mod care sa reflecte sau nu structura organizationala a organizatiei;

- Conventia de nume a organizatiei trebuie sa identifice unic persoanele folosind un identificator numeric unic ca valoare pentru atributul Relative Distinguished Name;
- Serviciul de director trebuie sa permita adaugarea sau modificarea definitiilor claselor de obiecte si a topologiei spatiului de nume;
- Serviciul de director trebuie sa permita definirea politicilor de securitate;
- Serviciul de director trebuie sa ofere posibilitate de acces anonim, acces cu autentificare simpla si mecanisme puternice de autentificare prin LDAP;
- Trebuie sa ofere posibilitati de audit al accesului la serviciul de director si al modificarilor aduse serviciului de director;
- Serviciul de director trebuie sa ofere abilitatea de a stoca certificate si CRL-uri;
- Trebuie sa asigure integrare cu serviciul de DNS;
- Trebuie sa ofere posibilitatea de a efectua legaturi multiple prin Lightweight Directory Access Protocol pe o conexiune, in scopul autentificarii utilizatorilor;
- Trebuie sa ofere posibilitatea de a dezactiva comprimarea traficului de replicare intre controlerele de domeniu care se afla in situri diferite;
- Trebuie sa permita administratorului eliminarea restrictiilor RDN - Relative Distinguished Name incompatibile cu standardul de director X.500;
- Trebuie sa permita memorarea si reproducerea zonelor DNS memorate in partitia de aplicatie a serviciului director;
- Trebuie sa permita mutarea elementelor interactive din faza configurarii in faza ulterioara instalarii, eliminand interactiunea administratorului la instalarea sistemului de operare;
- Trebuie sa ofere o interfata unica pentru configurarea si monitorizarea serverului, cu programe de tip expert pentru optimizarea sarcinilor comune de administrare a serverului;

- Trebuie sa ofere un shell optional cu linie de comanda si limbaj de script care sa ajute administratorii sa automatizeze sarcinile de rutina de administrare a sistemului pe mai multe servere;

- Trebuie sa ofere instrumente de diagnosticare puternice, care sa ofere vizibilitate permanenta asupra mediului serverului, fizic si virtual, pentru a identifica si rezolva rapid problemele care apar;

- Trebuie sa permita instalari minimale, in care sunt instalate numai rolurile si caracteristicile de care e nevoie, minimizand nevoile de intretinere si reducand zonele de atac de pe server;

- Trebuie sa ofere suport pentru Internet Protocol versiunea 6 (IPv6), iar nodurile de clustere de la locatii dispersate geografic sa nu mai trebuiasca sa se gaseasca intr-o subretea cu acelasi IP sau sa fie configurate cu retele locale virtuale (VLAN) complicate;

- Trebuie sa ofere suport pentru tehnologie Load Balancing;

- Trebuie sa integreze tehnologii de backup care sa simplifice restaurarea datelor sau a sistemului de operare;

- Trebuie sa permita virtualizarea rolurilor de server sub forma de masini virtuale (VM) separate care ruleaza pe aceeasi masina fizica, fara a fi necesara achizitia de software de la terti;

- Trebuie sa ofere replicarea masinilor virtuale catre gazde situate in locatii la distanta; capabilitatea de replicare sa poata fi oferita intre gazde care sunt membri ai unui cluster sau gazde independente;

- Trebuie sa ofere replicare masinilor virtuale si datelor de pe un echipament de stocare pe celalalt;

- Trebuie sa ofere suport pentru arhitecturi de tip NUMA in interiorul masinilor virtuale;

- Trebuie sa se poata implementa mai multe sisteme de operare – Windows, Linux si altele – in paralel pe un singur server;

- Trebuie sa contina un design modular si optiuni de instalare ce permit numai instalarea caracteristicilor strict necesare, reducand zonele de atac si simplificand administrarea actualizarilor;
- Trebuie sa ofere administrarea delegata a aplicatiilor si a site-urilor pentru control personalizat asupra diferitelor componente ale serverului Web;
- Trebuie sa ofere suport pentru rularea aplicatiilor PHP;
- Trebuie sa ofere suport pentru protocol HTML 5 si WebSocket;
- Trebuie sa ofere un depozit central pentru stocarea certificatelor digitale folosite pentru protectia site-urilor web;
- Trebuie sa ofere administrare la distanta pentru mai multe servere web dintr-o singura consola;
- Trebuie sa ofere posibilitatea de a gazdui servicii web in regim partajat de tip „multi-tenant" pentru mai multe site-uri web in regim de izolare;
- Trebuie sa ofere posibilitatea de a masura consumul de resurse al serverelor web partajate;
- Trebuie sa ofere posibilitatea de a limita consumul de resurse de procesor, memorie sau latime de banda consumate de serverul web;
- Trebuie sa ofere un mecanism ce asigura ca reteaua si sistemele nu sunt compromise de calculatoare virusate, izoland si/sau depanand calculatoarele care nu se conformeaza politicilor de securitate stabilite de administrator;
- Trebuie sa ofere un mecanism de protectie impotriva aplicatiilor periculoase;
- Trebuie sa ofere flexibilitate criptografica crescuta, suportand algoritmi de criptare standard si definiti de utilizator, permitand crearea, stocarea si preluarea mai facila a cheilor criptografice;
- Trebuie sa contina un modul pentru monitorizarea starii autoritatilor de certificare (CA);

- Trebuie sa contina un serviciu pentru prevenirea scurgerilor de informatii confidentiale din interiorul organizatiei catre exterior prin intermediul fisierelor;

- Trebuie sa ofere sistem de clasificare a informatiilor pentru informatii partajate cu configurarea automata a politicilor de acces prin politici de grup aplicate prin intermediul serviciului director.

Sistemul de operare pentru terminalele mobile trebuie sa asigure cel putin urmatoarele:

- Interfata de lucru moderna, intuitiva care sa ofere facilitati si suport pentru tablete cu ecran tactil;
- Posibilitatea de a lucra concomitent in 2 aplicatii pe acelasi ecran;
- Cautarea obiectelor electronice (fisiere, documente, email-uri, programe etc.) folosind un motor de cautare contextual;
- Posibilitatea de a utiliza si interfata grafica de tip desktop pentru a rula aplicatii mai vechi;
- Interfata de lucru cu utilizatorul si in limba romana;
- Aplicatii de genul client de posta, calendar, fotografii, contacte, mesagerie cat si facilitati de a lucra cu public cloud integrate in produs;
- Posibilitate de a instala aplicatii in mod traditional cat si din magazin online de aplicatii;
- Browser de web integrat care sa suporte HTML5, CSS3, EcmaScript5 si care sa poata fi utilizat in mod traditional (cu tastatura si mouse) cat si in mod tactil;
- Centru de accesibilitate pentru persoanele cu deficiente vizuale, motorii sau auditive, care sa permita:
    - Ajustarea elementelor vizuale, cum ar fi dezactivarea animatiilor, sau prelungirea timpului in care o caseta de dialog sta deschisa, pentru a permite citirea ei;
    - Alegerea unor scheme de culori cu contrast ridicat, si navigarea intre aceste scheme de contrast ridicat si contrast scazut prin combinatii de chei;
    - Marirea dimensiunii textului si a pictogramelor;
    - Activarea unei lupe virtuale pe ecran, pentru a mari anumite elemente vizuale;
    - Utilizarea unei tastaturi vizuale pe ecran, accesibila prin mouse sau alte dispozitive, cum ar fi joystick;

    - Configurarea timpului in care o tasta poate fi tinuta apasata pentru ca sistemul sa accepte o tasta, pentru a se evita repetarea tastelor cand se apasa o tasta, sau pentru a se evita efectul apasarii accidentale a unei taste;
    - Utilizarea alternativelor textuale sau vizuale pentru sunet;
- Instalare simplificata prin intermediul imaginilor de sistem de operare ce pot fi instalate de la distanta, centralizat;
- Sistem de administrare local ce poate fi controlat prin politici, care sa permita controlul granular al setarilor echipamentului, incluzand aici setari de acces utilizatori, de gestiune fisiere, aplicatii, securitate, drivere;
- Controlul accesului contului de utilizator la resurse critice ale dispozitivului, chiar daca acesta este administrator local;
- Posibilitatea de a restrictiona utilizarea anumitor aplicatii prin politici centralizate, chiar si cand utilizatorul este administrator local;
- Facilitati de a aproba sau bloca rularea unei aplicatii pe mai multe criterii (producator, versiune etc.) prin intermediu politicilor de retea;
- Facilitati care sa permita stocarea intr-o zona tampon temporara a fisierelor preluate de la sediul central peste linii de retea care au caracteristici scazute (latime de banda mica, latenta mare etc) pentru optimizarea lucrului in retea;
- Facilitatea de a instala sistemul de operare impreuna cu aplicatii pe un dispozitiv de stocare extern (memory stick, hard drive extern) pentru a fi utilizat ulterior de pe un echipament care prezinta facilitatea de boot de pe USB;
- Posibilitatea restaurari sistemului la caracteristicile initiale fara reinstalare;
- Aplicatie de protectie impotriva atacurilor cu malware si/sau spyware, care sa fie actualizata permanent;
- Sistem de criptare a fisierelor, in functie de contul utilizatorului, astfel incat acesta sa poata cripta/decripta fisiere/directoare fara a fi nevoit a utiliza parola sa la fiecare criptare/decriptare;
- Firewall integrat in sistemul de operare, configurabil atat prin politici locale, cat si prin politici globale care se aplica centralizat unor retele de comunicatii;

- Centru de securitate local prin care pot fi controlate setarile cheie de securitate ale sistemului de operare – anitivirus, firewall, antimalware, update-uri;
- Mod protejat de functionare al browser-ului, prin care acesta, chiar si cand utilizatorul este administrator local, nu poate utiliza aplicatii sau controale externe care functioneaza peste browser, care sa strice buna functionare a sistemului de operare si al echipamentului;
- Sistem de protejate impotriva atacurilor de phishing, integrat in browser;
- Posibilitatea de a configura toate politicile de securitate de la distanta, centralizat;
- Acces la distanta securizat, prin conexiuni de tip VPN cu reconectare automata;
- Acces la distanta securizat prin conexiune de tip acces direct care permite aplicare de politici de retea si utilizarea echipamentului in conditii similare cu accesul local in retea.
- Criptare disk si dispozitive amovibile;
- Sa permita metode de autentificare sigure bazate pe ceritificate digitale sau dispozitive biometrice;
- Sa ofere aplicatie pentru depistarea automata a problemelor pe echipament;
- Sa ofere aplicatie pentru rularea de aplicatii incompatibile cu sistemul de operare prin virtualizare locala;
- Sistem de urmarire a integritatii secventei de bootare pentru a preveni infectarea sistemului de operare;
- Fecilitati de autentificare clasice (parola, smartcard, fingerprint) cat si sistem de autentificare tactila pe baza unor elemente de identificare dintr-o poza;
- Sistemul de operare trebuie sa fie permanent actualiza, sa isi poata cauta singur actualizarile de la producator sau prin intermediul unui sistem de actualizare centralizat;
- Centru de gestiune a copiilor back-up si restaurarea acestora. Copiile back-up trebuie sa se poata face pe CD, DVD, hard-disk extern sau retea;
- Posibilitatea de a mentine versiuni multiple ale fisierelor/directoarelor, intr-un mod automat (astfel incat daca utilizatorul sterge sau modifica accidental un fisier sau director, sa poata recupera din mai multe versiuni anterioare);
- Sistem de monitorizare a eventualelor probleme de functionare, ce permite identificarea automata a unor eventuale solutii atat de la producator, cat si de la terte parti;

- Sistem de monitorizare si audit al evenimentelor de pe echipament, care sa inregistreze:
    - Activitatile de logon/logoff ale utilizatorilor;
    - Evenimentele generate de aplicatii;
    - Evenimentele inregistrate de browser;
    - Evenimentele hardware;
    - Evenimentele inregistrate de serviciile critice ale sistemului de operare;
- Sistemul de monitorizare si audit trebuie sa permita ca in functie de anumite evenimente, sa se declanseze actiuni automatizate (de exemplu in cazul caderii unui anumit serviciu pe un echipament, sa se trimita un e-mail catre adminsitrator);
- Posibilitatea de monitorizare si audit in timp real, cu reprezentare grafica, a activitatilor procesorului, hard-disk-ului, memoriei si transferuri de date;
- Posibilitatea sistemului de operare de a se auto-optimiza in functie de configuratia hardware disponibila (de exemplu sa poata opri functionarea unor facilitati ce ar putea incetini functionarea echipamentului, cum ar fi unele facilitati grafice);
- Posibilitatea sistemului de operare de a recomanda utilizatorului/administratorului, in functie de scenarii cunoscute, anumite setari pe care care acesta le poate face pentru a optimiza functionarea echipamentului;
- Aplicatie de curatire a hard-discului ce permite identificarea si eliminarea unor fisiere/directoare ce nu sunt folosite sau sunt temporare;
- Posibilitatea de a utiliza sistemul de operare cu minim 1.000 de dispozitive hardware;
- Suport pentru un sistem de fisiere optimizat pentru discuri flash;
- Suport pentru SSTP (Secure Socket Tunneling Protocol);
- Suport pentru tastatura in limba romana standardizata (SR 13392:2004) si caractere vizuale romanesti standardizate (ce au codurile Unicode 0218/0219 si 021A/021B).

Vor fi furnizate licente pentru toate echipamentele de procesare livrate in cadrul proiectului, respectiv pentru toate masinile virtuale create, in cazul in care solutia propusa de catre Ofertant se bazeaza pe o arhitectura virtualizata.

De asemenea, toate terminalele mobile vor fi echipate cu sistem de operare care sa respecte cerintele minimale exprimate anterior.

Licentierea pentru sistemele de operare trebuie sa asigure accesarea sistemului de catre 1.000 de utilizatori interni si numar nelimitat de utilizatori externi.

3.6.4.2. Software pentru platforma de baza de date

Pentru bazele de date se solicita o solutie robusta si scalabila capabila sa asigure disponibilitatea sistemului. Sistemul de baze de date trebuie sa indeplineasca urmatoarele obiective :

a. Schimb usor de date, fiabilitate si robustete
b. Acces la date prin protocoale standardizate (ODBC, XML, SOAP)
c. Administrare si dezvoltare simplificata

Functionalitatile generale pe care trebuie sa le indeplineasca sistemul de baze de date sunt:

- Serverul de baza de date terbuie sa permita folosirea a peste 64Gb memorie;
- Trebuie sa ofere suport pentru servere cu mai multe procesoare;
- Serverul trebuie sa permita folosirea a minim 12 core-uri;
- Trebuie sa ofere suport pentru transferul datelor din baza de date din si in alte baze de date prin protocoale standard (ODBC, XML, TXT) pentru a putea permite integrarea la nivel de date a altor sisteme externe;
- Functionalitati de administrare grafica a sistemului de gestiune a bazelor de date;
- Suport pentru mecanisme de control si blocare la nivel de tabela, fara escaladare, pentru a permite accesul concurent si manipularea datelor;
- Suport pentru suspendarea operatiilor consumatoare de resurse;
- Facilitati pentru gestionarea automata a memoriei (self-tuning);
- Suport pentru rularea mai multor instante de server de baze de date pe acelasi echipament
- Suport pentru interogare in format XML;
- Suport pentru stocare date in format XML si comunicare cu aplicatii in format XML;
- Suport pentru limbaje de tip SQL;
- Mecanism de securitate bazat pe utilizatori si roluri, integrat in sistemul LDAP;
- Facilitati pentru diagnosticarea problemelor: urmarirea executiei, expertiza, analiza, prognoza;
- Facilitati pentru monitorizarea tranzactiilor;
- Facilitati pentru monitorizarea, configurarea si optimizarea performantelor;

- Criptarea transparenta a datelor, a fisierelor de date si a fisierelor jurnal fara sa fie necesara modificarea aplicatiei. Functionalitatile de criptare sunt necesare pentru indeplinirea cerintelor si respectarea reglementarilor generale cu privire la confidentialitatea datelor. Criptarea trebuie sa ofere inclusiv instrumente de cautare in datele criptate utilizand sisteme de regasire intr-un interval sau cautarea partiala, fara modificarea aplicatiilor existente;
- Auditarea operatiilor trebuie sa includa informatii despre momentul in care au fost citite datele, in plus fata de orice modificare a datelor;
- Posibilitatea de a filtra evenimentele auditate; posibilitatea de a customiza operatia de audit in functie de evenimentele din baza de date;
- Posibilitatea adaugarii online a resurselor de memorie la masinile fizice care gazduiesc bazele de date, pentru scalarea la cerere a acestora;
- Facilitati de optimizare si depanare a performantei server-ului de baze de date, pentru a furniza administratorilor o perspectiva interactiva cu privire la performanta;
- Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de server prin captarea, filtrarea si reglarea evenimentelor generate de procesele de server;
- Evenimentele trebuie sa poata fi captate si exportate in diferite formate de iesire pentru corelarea cu aplicatiile sistemului de operare si ale bazelor de date, permitand astfel o monitorizare completa a sistemului;
- Comprimarea rapida a backup-urilor bazelor de date;
- Posibilitatea definirii limitelor si prioritatilor resurselor pentru diferite sarcini (workloads), si obtinerea unei performante consecvente in executarea acestora.
- Modul de alocare a resurselor fizice ale server-ului trebuie sa poata fi controlat de catre administratorul de sistem.
- Duplicarea datelor prin tehnologii de tip data „database mirroring”;
- Suport pentru replicarea datelor;
- Facilitati de partitionare a tabelelor pentru a asigura suport pentru baze de date foarte mari;

- Facilitati de indexare in paralel a datelor si suport pentru indecsi multipli pentru obiectele stocate;
- Facilitati pentru view-uri indexabile pentru a mari viteza de acces a interogarilor on-line;
- Suport pentru functionare in regim clustering;
- Suport pentru indexare on-line;
- Facilitati de administrare a aplicatiei din programe cu interfata grafica prietenoasa fara a fi nevoie de a utiliza scripturi de acces;
- Facilitati de optimizare a bazei de date si de tuning a arhitecturii;
- Suport nativ pentru acces la interogari prin servicii web;
- Suport pentru interogarea bazei de date in standardul xQuery 1.0.;
- Facilitati de rulare proceduri automate de back-up, arhivare, recuperare a unor versiuni mai vechi a bazei de date;
- Facilitati pentru proceduri de administrare si configurare, prin intermediul interfetelor grafice;
- Facilitati de operare a modificarilor in setul de date prin intermediul unor instante intermediare (transaction log);
- Facilitati pentru anularea tranzactiilor in ordine inversa (rollback);
- Facilitati pentru asigurarea integritatii datelor in timpul utilizarii prin solutii echivalente; Posibilitatea nativa de modelare a structurilor de date de tip arbore: metode incorporate pentru crearea si operarea pe noduri ierarhice;
- Posibilitatea stocarii datelor binare mari, precum documente si imagini, ca parte integranta a bazei de date, pastrand in acelasi timp consecventa tranzactionala;
- Cautare complexa la nivel de text, folosind indecsi specializati; efectuarea rapida a cautarilor in acest tip de date;
- Managementul performant al coloanelor cu valori rare: modalitati eficiente pentru administrarea spatiilor necompletate dintr-o baza de date relationala, astfel incat valorile de tip NULL sa nu consume spatiu fizic;
- Suport pentru definirea datelor de tip spatial pentru consumul, extinderea si utilizarea informatiilor in aplicatii activate din punct de vedere spatial. Datele de tip spatial trebuie sa corespunda standardelor din domeniu, precum Open Geospatial Consortium (OGC);

- Trebuie sa asigure gestionare facila a obiectelor bazelor de date:
    - Instrumente de dezvoltare a obiectelor din baza de date: solutia trebuie sa ofere unelte de dezvoltare pentru modulele ETL (Extract, Transform, Load), pentru design-ul bazelor de date atat relationale cat si multidimensionale, pentru design-ul rapoartelor;
    - Unelte pentru administrarea bazelor de date si a proceselor uzuale care se executa asupra bazelor de date precum si al rapoartelor;
    - Posibilitatea de definire si gestionare a obiectelor bazei de date (tabele, indecsi, proceduri stocate, triggere) direct din instrumentele folosite de dezvoltatori pentru scrierea aplicatiilor;
    - Posibilitatea de a oferi compresia datelor folosind suport UCS-2 Unicode;
    - Loc central care ofera posibilitatea administrarii entitatilor de date si ierarhiilor din multiple baze de date cu posibilitatea versionarii;
- Trebuie sa ofere capabilitati de disponibilitate ridicata si mentenanta:
    - Posibilitatea efectuarii backup-ului in multiple fisiere simultan pentru a putea efectua operatia pe discuri diferite in paralel;
    - Posibilitatea de a crea, modifica, sterge index-ul concurent cu activitatile utilizatorilor;
    - Posibilitatea de a crea un snapshot al bazei de date;
    - Modificarea schemei online;
    - Arhitectectura propusa de ofertant trebuie sa includa o baza de date in configuratie de inalta disponibilitate;

De asemenea, sunt necesare instrumente de modelare si editare date pentru 2 utilizatori care trebuie sa asigure urmatoarele:

- editor SQL inteligent cu functie de completarea automata a frazelor prin sugestii in functie de context;
- posibiliatea organizarii activitatilor in ”proiecte” pentru o administrare facila;
- posibilitatea explorarii mai multor baze de date simultan si compararea datelor din acestea intr-o singura interfata unitara;

- posibilitatea editarii tabelelor bazelor de date intr-o fereastra interactiva in care se pot edita parametrii de interogare sau executie, valida sau calcula diverse valori etc.;
- posibilitate elaborarii rapide de grafice pe baza datelor interogate (minim line chart, 2D/3D Pie/Bar chart, indicatoare de tip ”ceas”);
- posibilitatea elaborarii de grafice avansate folosind filtre, date agregate sau efectuand diverse calcule;
- posibilitatea reformatarilor interogarilor SQL in functie de nevoie sau de utilizator;
- posibilitatea proiectarii structurii bazelor de date: vizualizarea si editarea in mod grafic a structurii bazelor de date;
- posibilitatea compararii datelor din doua tabele si reuniunea acestora intr-una singura;
- posibilitatea compararii datelor din doua baze de date si reuniunea acestora intr-una singura;
- posibilitatea conversiei structurii de baze de date tipica unui vendor la formatul altui vendor in mod facil, interactiv din interfata grafica;
- suport pentru modele XML stocate in bazele de date;
- suport pentru view-uri si proceduri stocate;
- suport pentru import si export date, formatele suportate pentru import fiind minim: CSV, XML si pentru export minim: CSV, XML, HTML sau de tip Excel (sau echivalent);
- suport 32/64 bit.

Platforma de baze de date se va licentia atfel incat sa asigure rularea pe minim 6 nuclee de procesare active, 1.000 de utilizatori interni si numar nelimitat de utilizatori externi ai sistemului.

3.6.4.3. Software pentru platforma portal si colaborare

Portalul va trebui sa prezinte urmatoarele caracteristici:

- Interfata web standardizata, simpla si intuitiva;
- Interfata cu utilizatorii bogata in functionalitati, care sa ofere un nivel ridicat de accesibilitate
- Grad ridicat de securitate a sistemului, care sa garanteze confidentialitatea si securitatea datelor utilizatorilor pentru accesul neautorizat atat din afara, cat si din interiorul sistemului;

- Servicii si extensii ale portalului modulare, care sa permita dezvoltarea ulterioara de noi functionalitati;
- Arhitectura orientata pe servicii, astfel incat toate serviciile implementate pentru gestionarea continutului in portal (publicare, cautare, versionare, etc.), sa poata fi reutilizate si incluse in alte aplicatii;
- Administrarea si dezvoltarea portalului se va putea realiza facil, utilizand doar un browser web;
- Sa ofere acces catre toate resursele prezente in cadrul portalului printr-o singura autentificare, la deschiderea sesiunii

Se doreste un sistem cunoscut in domeniul solutiilor de portal-uri enterprise ce foloseste cele mai noi tehnologii .net, Java sau echivalent si Web 2.0. Sistemul trebuie sa fie construit pornind de la nevoile utilizatorului final, interfata sa oferind functionalitati intuitive, dinamice si rapide care conduc la o performanta remarcabila. De asemenea, arhitectura trebuie sa fie bazata pe tehnologii deschise si facilitatile de integrare deja prezente, ce permit o extensibilitate facila a sistemului, indiferent de modalitatea aleasa pentru acest lucru. Astfel, vor putea fi folosite toate serverele de aplicatii majore, baze de date, sisteme de operare, limbaje de programare diverse.

Componenta trebuie sa ofere urmatoarele functionalitati:

- Managementul continutului web – platforma trebuie sa ofere toate uneltele si functionalitatile necesare pentru managementul continutului web si sa permita crearea de pagini web personalizate: editor de text WYSIWYG, separarea continutului de layout, continut reutilizabil, CSS, sabloane pentru crearea paginilor web, generare dinamica de taxonomii web, site map, Search Engine Optimization (SEO), motor de cautare etc.;
- Facilitati de colaborare - componenta de colaborare trebuie sa ofere uneltele necesare pentru a sprijini interactiunea utilizatorilor: email, mesagerie instant de tip YM, wiki, blog, forum de discutii, calendar, anunturi si alerte, RSS etc.;
- Solutia trebuie sa fie astfel construita incat sa ofere suport pentru instalarea de servere multiple pe o singura masina fizica. In fapt trebuie sa suporte clusterizare multi-nivel pentru orice combinatie de niveluri posibila (prezentare, serviciu, logica de business si baza de date) prin implementarea celor mai noi tehnologii in domeniu:
    - Advanced Caching;
    - Page Caching;

- Load Balancing;
- Session Replication;
- Distributed Cache;
- Static Content Export.

- Solutia propusa de ofertant trebuie sa aiba configuratie de inalta disponibilitate pentru platforma portal si colaborare.

Solutia trebuie sa fie dezvoltata folosind o strategie de tip SOA si sa ofere suport pentru standardul WSRP 1.0 si 2.0 ce permite o integrare usoara a portletilor remote, aplicatiilor si continutului.

Solutia trebuie sa ofere posibilitatea de import al continutului de la diferite alte surse de date (alte aplicatii similare, sisteme de fisiere, baze de date, pagini web, servicii web, etc.);

Solutia trebuie sa ofere functionalitati de continut personalizat si facilitati de personalizare avansate functie de context.

Solutia trebuie sa fie complet web-based astfel incat absolut toate operatiunile, inclusiv administrarea si definirea layout-ului si a resurselor Portal sa se faca din browser-ul web.

Solutia trebuie sa fie construita in intregime pe o infrastructura de securitate care sa ofere mecanisme de control al accesului granularizat la nivel de utilizator, grup si rol si care sa garanteze confidentialitatea, autenticitatea si integritatea informatiilor din portal.

Solutia trebuie sa permita un singur punct de acces la toate modulele.

Arhitectura solutiei trebuie sa permita o scalabilitate sporita, performanta sporita, inalta disponibilitate si simplitate pentru deservirea unui numar mare de utilizatori.

Solutia trebuie sa ofere suport pentru instalarea pe diverse servere de aplicatii, trebuie sa ofere suport toate serverele de aplicatii majore din piata, cu capabilitati de clustering, balansare si failover.

Solutia trebuie sa permite functionalitatea dynamic virtual hosting care permite ca dupa setarea unui site web, intranet sau portal, ca pe aceeasi masina fizica sa se poata seta si alte site-uri sau portal-uri, fiecare cu propria adresa URL unica, si cu alte functionalitati si interfata cu utilizatorul.

Solutia trebuie sa ofere un mecanism de tip asistent (wizard) pentru crearea automata a site-urilor pe baza de sabloane.

Solutia trebuie sa suporte functionalitatea de drag and drop dinamic, permitand utilizatorilor sa adauge module si functionalitati in paginile portalului fara a fi necesara scrierea de cod sau reproiectarea modulelor existente.

Functionalitati predefinite ale platformei portal

Solutia trebuie sa ofere o functionalitate standard care sa permita comunitatilor de utilizatori sa isi creeze si asocieze propriile personalizari si sabloane de layout-uri in conformitate cu nevoile acestora. Fiecare comunitate, indiferent ca se refera la o echipa sau un departament, poate avea propriul spatiu de lucru securizat echipat cu o serie de functionalitati si cu un set de unelte ce permite personalizarea layout-ului dupa dorinta.

Solutia trebuie sa ofere facilitati incorporate de management al documentelor si continutului care sa permita stocarea fisierelor in orice format electronic. Principalele functionalitati oferite sunt:

- Depozit de documente compatibil cu standardul JSR-170 sau echivalent;
- Check in / check out;
- Versionare;
- Fluxuri de lucru;
- Posibilitatea adaugarii de tag-uri dinamice;
- Afisare fara a permite copierea;
- Cautare simpla si complexa multi-nivel bazata pe motorul de cautare Lucene sau echivalent;
- Import de fisiere multiple;
- Conversia formatelor de fisiere Microsoft Office, PDF, TXT si HTML (import si export);
- Suport pentru standardul WebDAV;
- Galerie de imagini.

Solutia trebuie sa ofere facilitati incorporate de managementul continutului web; crearea de continut web si unelte de publicare pe portal

- editor de text WYSIWYG si editor web;
- separarea continutului de layout;
- continut reutilizabil;
- suport pentru CSS;

- sabloane pentru crearea paginilor web;
- generare dinamica de taxonomii web;
- motor de cautare bazat pe tehnologia Lucene sau echivalent;
- versionarea continutului web;
- posibilitatea de adaugare de metadate etc.;

Solutia trebuie sa ofere un editor de tip WYSIWYG care permite dezvoltarea continutului intr-o maniera structurata si care ofera o multitudine de facilitati pentru adaugarea de elemente si articole atat in modul design cat si in format HTML.

Editorul de tip WYSIWYG trebuie sa permita publicarea, editarea, arhivarea continutului, categoriilor si paginilor fara a fi necesare cunostinte de programare sau HTML. Uneltele de tip WYSIWYG contin posibilitati de formatare ale textului similare cu cele din suita Office si permit adaugarea de elemente de tip text, tabele, imagini, audio, video, animatii flash, link-uri etc.

Solutia trebuie sa ofere facilitati de colaborare - componenta de colaborare trebuie sa ofere uneltele necesare pentru a sprijini interactiunea utilizatorilor: email, mesagerie instant de tip YM, wiki, blog, forum de discutii, calendar, anunturi si alerte, RSS, etc

Solutia trebuie sa ofere autorizare granularizata, bazata pe roluri. Pentru a asigura cerinta ca anumite grupuri de utilizatori sa controleze accesul la informatiile din cadrul site-ului, administratorii portalului pot asocia utilizatori individuali sau grupuri de utilizatori cu roluri diferite care ofera niveluri diferite de drepturi de acces si editare in conformitate cu uneltele, aplicatiile, fisierele, continutul publicat si comunitatile pe care este necesar sa le foloseasca. Utilizatorii vor accesa numai continutul din portal pentru care li s-au definit drepturi de acces, restul informatiilor fiind ascunse.

Solutia trebuie sa foloseasca standarde de securitate recunoscute in industrie, precum si tehnologii de criptare ce include algoritmi avansati cum ar fi DES, MD5 si RSA.

Infrastructura de securitate a platformei trebuie sa cuprinda autentificare prin componente externe (pluggable authentication), verificare email, permisiuni cu granularitate fina, autentificare prin LDAP si managementul sesiunilor.

Administrarea utilizatorilor, grupurilor si profilurilor se face dintr-o noua interfata web complet redesenata care ofera o uzabilitate sporita bazata pe principiul configurare single-click.

Solutia va contine un Panou de Control din care se realizeaza managementul centralizat al utilizatorilor, rolurilor, comunitatilor si drepturilor de acces.

Administratorii portalului pot asocia utilizatori individuali sau grupuri de utilizatori cu roluri diferite care ofera niveluri diferite de drepturi de acces si editare in conformitate cu uneltele, aplicatiile, fisierele, continutul publicat si comunitatile pe care este necesar sa le foloseasca. Utilizatorii vor accesa numai continutul din portal pentru care li s-au definit drepturi de acces, restul informatiilor fiind ascunse. In acest sens sunt oferite unelte care permit:

- Crearea unui numar nelimitat de utilizatori;
- Gruparea utilizatorilor functie de profilul acestora (se pot crea taxonomii de utilizatori);
- Definirea si gestiunea drepturilor de acces la informatii ale utilizatorilor si grupurilor de utilizatori;
- Fiecare utilizator are un profil pe care il poate gestiona prin editarea datelor stocate in profil;
- Posibilitatea de inregistrare a unui utilizator nou pe site;
- Unelte de recuperare a parolei.

Solutia trebuie sa se poata baza pe mecanismele de autentificare implementate in cadrul organizatiei. Astfel, platforma portal trebuie sa faciliteze alinierea la politicile si procedurile de securitate ale organizatiei. Aceasta functionalitate permite beneficiarului sa gestioneze utilizatorii si grupurile acestora intr-un singur punct si elimina nevoia de a intretine simultan mai multe parole.

Interfata portalului trebuie separata din punct de vedere logic de codul aplicatiei astfel incat orice actualizare sa pastreze toate particularizarile efectuate anterior interfetei.

Solutia trebuie sa permita particularizarea interfetei pentru fiecare rol sau pentru fiecare sablon de lucru.

Solutia trebuie sa ofere o locatie centralizata in care este stocat, agregat si gestionat tot continutul portalului. Fiecare comunitate parte trebuie sa aiba acces la propriile librarii de documente si imagini pentru a oferi securitatea necesara. Aceste librarii vor avea directoare personalizate care actioneaza ca directoare web-based partajate catre toti membrii comunitatii si sunt organizate intr-o structura ierarhica usor de folosit si de administrat. Modulele dedicate vor oferi instrumentele necesare care sa permita vizualizarea, crearea, convertirea si editarea de

documente, tabele de calcul si fisiere de tip prezentare direct din portal, fara instrumente aditionale.

Solutia trebuie sa ofere unelte flexibile si componente out-of-the-box care sa permita crearea, personalizarea, administrarea si integrarea mai multor site-uri web, folosind o interfata cu utilizatorul extrem de usor de folosit si configurat precum si intuitiva. Sarcini consumatoare de timp cum ar fi design-ul layout-ului paginilor, adaugarea de continut si de functionalitati, modificarea temelor si a interfetelor se vor putea face din doar 2-3 click-uri. Utilizatorii vor avea profile separate: pot fi administratori, utilizatori normali sau editori, continutul paginilor si layout-ul fiind stabilit de acestia, nu de catre dezvoltatori. Solutia trebuie sa ofere suport pentru site-uri personale, care pot fi facute publice prin intermediul unui URL prietenos sau pot fi tinute private. Accesul la acestea si la continutul din portal in general trebuie sa se faca diferentiat in functie de profilul utilizatorului, iar administrarea sa se faca usor folosind uneltele si aplicatiile predefinite puse la dispozitie.

Solutia trebuie sa ofere functionalitatea dynamic virtual hosting care sa permita ca dupa setarea unui site web, intranet sau portal, ca pe aceeasi masina fizica sa se poata implementa rapid si alte site-uri sau portal-uri, fiecare cu propria adresa URL unica, si cu alte functionalitati, grupuri de utilizatori si elemente grafice de interfata cu utilizatorul diferite.

Solutia trebuie sa contina un modul ce permite utilizatorilor cu drepturi de editare sa lucreze in timp real fara a afecta continutul deja existent si sa previzualizeze modificarile efectuate. Acest lucru trebuie sa se poata face atat la nivel de pagina cat si la nivelul intregului portal. Daca nu se doreste publicarea imediata a continutului editat, trebuie sa existe posibilitatea de a seta periodicitatea publicarii la o data prespecificata, iar portalul va afisa automat la data stabilita ceea ce se doreste a fi publicat in locatia selectata anterior. De asemenea, trebuie sa existe posibilitatea de a reveni la versiunile mai vechi ale continutului daca este necesar.

Aprobarea continutului trebuie sa se faca direct de catre editor sau prin intermediul unui flux de aprobare in mai multe etape, mai multi autori fiind responsabili de sectiunile de care s-au ocupat.

Solutia trebuie sa contina o interfata de administrare (Panou de Control.) Aceasta trbuie sa ofere o administrare centralizata pentru administratorii portalului, dar si pentru administratorii de continut si editorii portalului. Panoul de Control trebuie sa aiba o interfata unificata si simplu de utilizat pentru toate activitatile de administrare: administrarea continutului, portalului, utilizatorilor, serverului.

Solutia trebuie sa ofere o functionalitate standard prin care sa stocheze informatii despre continutul publicat. Trebuie stocata data la care a fost publicat continutul, informatii despre valabilitatea acestuia si data la care trebuie arhivat.

Solutia trebuie sa ofere un motor de sabloane web-based care sa permita editarea rapida a sabloanelor prin intermediul unei interfete facile, ce permite operatiuni de tip drag and drop, redimensionare, minimizare, maximizare, modificarea aspectului si alte configurari ce permit realizarea rapida a unui design in functie de preferinte. Pe baza template-urilor standard oferite sau pe baza celor create de utilizatorii cu drepturi de administrare trebuie sa se poata genera automat pagini HTML optimizate pentru motoarele de cautare.

Solutia trebuie sa ofere posibilitatea de a arhiva configuratiile, permitand revenirea la o varianta de configurare anterioara.

Solutia trebuie sa ofere o functionalitate care sa permita extragerea de continut din mai multe surse de date, inclusiv direct din baza de date.

Solutia trebuie sa ofere portleti de navigare ce permit structuri de navigare arborescenta si ajuta utilizatorii sa ajunga la informatiile necesare mult mai usor. Portletii de navigare trebuie sa fie de mai multe tipuri: navigare bazata pe categorii si taxonomii, breadcrumb, harta site, navigare categorii, navigare meniuri, navigare tag-uri etc. Acestia trebuie sa poata fi usor personalizati si adaugati in pagini astfel incat sa se poata oferi mai multe variante de acces la continut si la documente.

Solutia trebuie sa permita utilizatorilor cu drepturi de editare sa lucreze in timp real fara a afecta continutul deja existent si sa previzualizeze modificarile efectuate. Acest lucru trebuie sa se poata face atat la nivel de pagina cat si la nivelul intregului portal. Daca nu se doreste publicarea imediata a continutului editat, trebuie sa existe posibilitatea de seta periodicitatea publicarii la o data prespecificata, iar aplicatia va afisa automat la data stabilita ceea ce se doreste publicat in locatia selectata anterior. Trebuie sa existe posibilitatea de a reveni la versiunile mai vechi ale continutului daca este necesar.

Continutul site-urilor trebuie sa fie complet separat de partea de design existand concepte diferite pentru libraria de sabloane grafice, layout-ul paginilor si continutul propriu-zis al acestora. Administratorul trebuie sa aiba posibilitatea de a genera o pagina pe baza unui layout dar elementele din acea pagina sa poata fi modifica in mod facil ulterior, personalizandu-se astfel un site intreg sau numai paginile necesare, pentru acest lucru nefiind necesare cunostinte tehnice.

Platforma va oferi uneltele necesare pentru aceste operatiuni out-of-the-box intr-o maniera prietenoasa si usor de folosit si invatat.

Solutia trebuie sa permita crearea mai multor administratori si posibilitatea de a oferi drepturi de acces personalizate utilizatorilor. Pentru a se asigura controlul accesului va fi implementat un sistem granularizat de autorizare bazat pe roluri. Administratorii vor avea posibilitatea de a asocia drepturi de acces diferentiate pentru utilizatori individuali sau grupuri de utilizatori, pe mai multe niveluri pentru comunitati specifice, fisiere, aplicatii si uneltele puse la dispozitie.

Un grup special de utilizatori este acela al editorilor de continut care creeaza continut pe pagini si carora li se pot acorda drepturi de a aproba si publica acest continut pe site.

Solutia trebuie sa monitorizeze si sa impiedice orice incercare de acces la o functionalitate sau document / informatie din sistem, daca utilizatorul nu are drepturi suficiente; mai mult, in general utilizatorul nici nu va avea afisate acele optiuni / documente / servicii la care nu i-a fost acordat acces in mod explicit printr-un mecanismul de profile si drepturi utilizator.

Platforma portal si colaborare se va licentia atfel incat sa asigure rularea pe minim 24 nuclee de procesare active, 1.000 de utilizatori interni si numar nelimitat de utilizatori externi ai sistemului.

3.6.4.4. Software pentru platforma GIS

Serverul GIS trebuie sa indeplineasca urmatoarele cerinte in vederea posibilitatii administrarii datelor spatiale centralizat si dezvoltarii de aplicatii web cu suport GIS:

- Serverul GIS trebuie fie o solutie GIS scalabila, bazata pe platforma server, ce poate fi instalata pe un singur server pentru a deservi un numar restrans de utilizatori sau poate fi instalata distribuit pe mai multe servere pentru a asigura suport aplicatiilor beneficiarului;
- Sa permita crearea, administrarea, si distribuirea de servicii WebGIS pentru a putea fi utilizate ca suport cartografic atat in aplicatiile WEB, desktop, cat si pentru aplicatiile mobile;
- Sa permita controlul asupra continutului geografic printr-o administrare centralizata a datelor spatiale, inclusiv a imaginilor raster;
- Sa permita transcalculul de coordonate “on-the-fly” din sistemul in care sunt stocate datele in cel in care sunt afisate;
- Sa permita utilizarea datelor vector si datelor raster cu diverse rezolutii;
- Sa ofere posibilitatea de particularizare, integrare si comunicare tinand seama de standardele internationale specifice informatiei geospatiale si asigurarea

interoperabilitatii Web;

- Sa fie conform cu standardele OGC (Open Geospatial Consortium) (WMS, WFS, WCS, WPS);
- Sa ofere suport pentru integrare cu aplicatiile software desktop GIS, fara a fi nevoie de conversia datelor GIS;
- Sa ofere suport pentru diseminarea informatiilor geospatiale si distribuirea capabilitatilor de cartografiere diferitelor tipuri de aplicatii client, aplicatii web de tip lightweight, aplicatii de tip browser si aplicatii desktop GIS;
- Sa fie prevazuta cu instrumente ce permit publicarea de algoritmi, calcule si procese geospatiale;
- Sa ofere acces la functionalitatile GIS folosind o aplicatie tip browser si posibilitatea publicarii de servicii Web;
- Sa permita editarea datelor spatiale atat pentru serviciile WEBGIS (folosind standarde de interoperabilitate web deschise, exemple putand fi REST cat si SOAP);
- Sa permita utilizarea urmatoarelor operatii de editare (folosind standarde de interoperabilitate web deschise, exemple putand fi REST cat si SOAP): Creare entitati noi, modificare geometrie si atribute etc.;
- Sa ofere functii de integrare a datelor provenite din diferite surse, de pe Internet sau surse locale;
- Sa permita conectarea la urmatoarele sisteme relationate de baze de date: Microsoft SQL Server, MySQL, Oracle, H2, PostGIS;
- Sa fie prevazut cu instrumente care sa permita accesarea urmatoarelor formate raster: GeoTIFF, GTOPO30, ArcGrid, MrSID, ECW, JPEG2000;
- Sa permita crearea de chache-uri pentru serviciile web-gis publicate;
- Sa permita utilizarea mai multor formaturi de imagini ex, jpeg, png in cadrul cache-ului;
- Sa permita gruparea serviciilor de harta cache-uite astfel incat sa fie optimizata stocarea si accesarea acestora;
- Sa permita crearea de “cache”-uri pentru serviciile WebGIS;
- Sa fie prevazut cu instrumente de “anti-aliased”;
- Sa ofere functionalitati dedicate si instrumente specific gestionarii securizarii datelor si

serviciilor WebGIS si sa asigure definirea utilizatorilor, a rolurilor si drepturilor de utilizare a datelor si serviciilor WebGIS dezvoltate. Modelul de securitate trebuie sa permita limitarea accesului utilizatorilor neautorizati la datele si serviciilor WebGIS;

- Sa permita combinarea de servicii web de harta multiple intr-o singura aplicatie web dezvoltata proprie;
- Sa permita mentinerea informatiei temporale prezente in datele spatiale publicate prin intermediul serverului de gis si executarea de interogari asupra informatiei temporale;
- Sa permita prin serviciile webgis publicate, accesarea atasamentelor existente in baza de date pentru fiecare obiect spatial (atasamentele pot fi fisiere de tip text, imagine s.a. si pot fi salvate mai multe fisiere pentru fiecare obiect spatial);
- Sa ofere capabilitati de publicare pe Internet precum: randare de imagini, extragere si descarcare de date, etc.;
- Sa permita descarcarea serviciilor WFS in format Shapefile, Excel, DXF;Sa fie prevazut cu instrumente ce permit conformitatea cu cerintele de vizualizare cerute de directive INSPIRE;
- Sa fie prevazut cu instrumente ce permit filtrarea informatiei geospatiale;
- Sa permita descarcarea datelor geospatiale pentru a putea fi vizualizata in aplicatii, cel putin GoogleEarth.

Aplicatia WebGIS trebuie sa indeplineasca urmatoarele cerinte specifice:

- Sa permita afisarea informatiei geospatiale in format raster si vector pe harta;
- Sa permita afisarea mai multor harti tematice simultan;
- Sa permit afisarea pe harta a altor surse de informatii geospatiale cum ar fi: Google, OpenStreet Map, Bing etc.;
- Sa permita afisarea altor servicii de harta de tipul WMS, WFS, TMS;
- Sa ofere operatii specifice de operare a hartilor: zoom-in, zoom-out, pan, zoom to full extent, zoom extent anterior, zoom extent urmator;
- Sa afiseze scara de expunere a hartii;
- Sa furnizeze un mecanism de selectare flexibil;
- Sa afiseze coordonatele geografice in momentul deplasarii pe harta;
- Sa permita masurarea de arii pentru poligoane si masurarea de lungimi pentru linii;

- Sa permita printarea hartii direct din pagina WEB;
- Sa fie prevazuta cu mecanisme de activare/dezactivare a straturilor astfel incat sa fie posibila vizualizarea si interactiunea cu un singur strat sau cu un subset de straturi;
- Afisarea straturilor pe harta sa fie insotite si de legenda;
- Sa permita afisarea simultana a detaliilor alfanumerice si a reprezentarii geografice;
- Sa permita afisarea tabelara a informatiilor pentru maximizarea informatiei vizualizate la un moment dat;
- Sa permita afisarea paginata pentru a permite o navigare facila atunci cand listele de entitati devin foarte lungi;
- Sa fie prevazuta cu instrumente ce permit interogari complexe asupra atributelor alfanumerice asociate entitatilor grafice;
- Sa permita exportul in format tabelar a interogarilor efectuate asupra atributelor alfanumerice ce insotesc entitatile vectoriale;
- Sa fie prevazuta cu instrumente ce permit filtrari spatiale complexe;
- Sa fie prevazuta cu mecanisme ce permit actualizarea hartii cum ar fi: adaugare, modificare, stergere entitati vectoriale, reactualizare atribute alfanumerice asociate entitatilor vectoriale;
- Sa fie prevazuta cu instrumente de geocoding;
- Sa fie prevazuta cu instrumente de reverse geocoding;
- Sa permita publicarea hartilor prin incorporarea acestora intr-o pagina web;
- Sa permita realizarea de grafuri cu rute optime.

Aplicatia software Desktop GIS trebuie sa indeplineasca minim urmatoarele cerinte:

- Sa ofere posibilitatea de a vizualiza si suprapune vectori si informatii raster in diferite formate si proiectii;
- Sa ofere posibilitatea de creare, editare si export date spatiale in formate standard;
- Sa dispuna de instrumente de editare, culegere, intretinere, integrare, analiza, cartografiere si vizualizare a datelor geospatiale in cat mai multe formate diferite;
- Sa includa instrumente si proceduri de analiza si geoprocesare oferind astfel evaluarea, interpretarea, compararea si intelegerea cat mai corecta a procesului decizional folosind hartile si informatia geospatiala;

- Sa permita automatizarea si modelarea proceselor de analiza a datelor geospatiale;
- Aplicatia Desktop GIS trebuie sa ruleze in mai multe siteme de operare, ex: Windows, Mac OS, Linux etc.;
- Sa permita personalizarea interfetei utilizator prin adaugarea sau eliminarea barelor de instrumente;
- Sa aiba in componenta o aplicatie standard pentru managementul datelor si metadatelor prin care acestea se pot vizualiza si previzualiza in interioarul aplicatiei;
- Sa permita efectuarea de analize spatiale (exemplu: operatii algebrice pe harti, analiza terenului);
- Sa permita rularea pe procesoare cu 64bit;
- Sa fie extensibila – posibilitatea adaugarii functionalitatilor geospatiale specifice serviciilor si proceselor de lucru;
- Sa asigure instrumente pentru incarcarea obiectelor spatiale din formate OGC in baza de date geospatiala;
- Sa suporte sistem de coordonate globale, nationale si locale in special proiectia nationala Stereografic 1970;
- Sa permita transcalulul de coordonate ”on the fly” din sistemul de coordonate in care sunt datele catre cel in care sunt afisate;
- Sa permita conectarea la urmatoarele siteme relationate de baze de date:
    a. Micorsoft SQL Server;
    b. Oracle Spatial;
    c. PostGIS;
    d. MySQL;
    e. SQLite.
- Solutia propusa de ofertant pentru platforma GIS trebuie sa fie in configuratie de inalta disponibilitate;
- Posibilitatea de creare de harti si explorare interactiva a datelor spatiale intr-o interfata grafica prietenoasa;
- Sa fie prevazuta cu instrumente de analiza topologica pentru seturile de date spatiale;
- Sistemul trebuie sa fie prevazut cu instrumente de cartografiere complexa, inclusiv

legende, reprezentarea corecta a diferitelor sisteme de coordonate, scalare corecta, redarea corecta a hartii in concordanta cu proiectia selectata;

- Aplicatia trebuie sa fie prevazuta cu instrumente ce permit redarea la scara reala la diferite formate (A4, A3, A2, A1, A0, etc.) a hartilor;
- Sa fie prevazuta cu instrumente avansate pentru simbolizarea entitatilor vectoriale si raster cum ar fi: transparenta, culoare, dimensiune etc.;
- Sa permita simbolizarea entitatilor geospatiale pe baza de reguli particulare;
- Sa permita etichetarea avansata a elementelor vectoriale geospatiale prin functii de tipul: amplasare, rotire, dimensionare, prioritizare etc.;
- Sa dispuna de functii de geoprocesare de tipul: Buffer, **Union, Intersect**, Merge, Clip, Dissolve, Eliminate etc.;
- Se dispuna de functii de editare de tipul:
    - Separarea unui obiect spatial de tip linie sau polygon in doua parti;
    - Adaugarea unui poligon la un poligon existent fara trasarea laturii comune;
    - Modificarea formei unui obiect spatial existent.
- Sa dispuna de functii de generalizare a obiectelor geospatiale;
- Sa fie prevazuta cu functii de geocodare;
- Sa fie prevazuta cu functii de geocodare inversa;
- Sa fie prevazuta cu functionalitati care sa permita relationari definite intre straturile tematice si tabelele de date independente (Join);
- Sa permita efectuarea de operatii de cautare si interogare asupra tabelelor independente sau straturilor tematice si extragerea informatiei in baza regulilor stabilite intre acestea;
- Sa permita descarcarea sau incarcarea de atasamente pentru obiectele spatiale existente in baza de date;
- Sa permita vizualizarea imaginilor asociate obiectelor spatiale existente in baza de date (ex: imaginea unei vane etc);
- Sa permita editarea serviciilor webgis prin mentinerea regulilor de integritate a datelor spatiale la nivelul aplicatiei desktop;
- Definirea de reguli prin care datele sunt clasificate in tipuri si reguli prin care se stabilesc

tabele de lookup pentru informatiile non-spatiale, de exemplu prin join-uri si view-uri;

- Sa permita accesarea serviciilor web de genul: Google Maps, Open Street Map, Yahoo Map, Bing;
- Sa permita incarcarea mai multor tipuri de date vectoriale geospatiale in cadrul aplicatiei. Exemplu SHP, DXF, DGN, CSV, GeoJSON, MIF, TAB etc.;
- Sa permita incarcarea mai multor tipuri de date raster geospatiale in cadrul aplicatiei. Exemplu: GeoTIFF, JPEG2000, JPEG, ECW, MrSID, ASC, GRD etc.

Platforma GIS se va licentia atfel incat sa asigure rularea pe minim 8 nuclee de procesare active, 1.000 de utilizatori interni (cu drepturi de scriere) si numar nelimitat de utilizatori externi (cu drept de acces de tip read-only). De asemenea, se vor oferi instrumente de tip desktop pentru 5 utilizatori.

Platforma GIS va include si o componenta de harta. In acest sens, baza de date geospatiala trebuie sa contina minim urmatoarele seturi de date vectoriale si cu informatie alfanumerica aferenta:

- Harta Judetelor;
- Harta UAT;
- Harta Localitati;
- Furnizorul va trebui sa realizeze harta locatiilor angajatorilor din municipiul Bucuresti (sediul social si puncte de lucru), urmand ca pentru celelalte localitati informatia geospatiala din harta sa fie generata de catre angajatii Beneficiarului pe masura efectuarii de controale pe teren.

Harta Judetelor trebuie sa contina informatia vectoriala si alfanumerica aferenta tuturor judetelor tarii, respectiv 41 de judete si municipiul Bucuresti. Campurile cu date alfanumerice aferente obeictelor vectoriale trebuie sa contina minim urmatoarele informatii:

a. Nume Judet;
b. Resedinta Judet;
c. Cod Judet (Prescurtare denumire judet, Ex: Alba – AB, Brasov – BV etc.);
d. Observatii.

Geometria stratului va fi de tip poligon iar informatia alfanumerica trebuie sa fie scrisa cu diacritice.

Harta Unitatilor Administrativ Teritoriale trebuie sa contina informatia vectoriala si alfanumerica aferenta tuturor unitatilor administrative teritoriale din Romania. Campurile cu datele alfanumerice aferente obiectelor vectoriale trebuie sa contina minim urmatoarele informatii:

a. Nume UAT;
b. Nume Judet;
c. Cod Judet (Prescurtare denumire judet, Ex: Alba – AB, Brasov – BV etc.);
d. Tip UAT;
e. Siruta UAT;
f. Siruta Resedinta;
g. Resedinta;
h. Observatii.

Geometria stratului va fi de tip poligon iar informatia alfanumerica trebuie sa fie scrisa cu diacritice.

Harta Localitatilor trebuie sa contina informatia vectoriala si alfanumerica aferenta tuturor Localitatilor din Romania. Campurile cu datele alfanumerice aferente obiectelor vectoriale trebuie sa contina minim urmatoarele informatii:

a. Nume Localitate;
b. Nume UAT;
c. Nume Judet;
d. Cod Judet (Prescurtare denumire judet, Ex: Alba – AB, Brasov – BV etc.);
e. Tip UAT;
f. Siruta;
g. Siruta UAT;
h. Resedinta;
i. Observatii;

Geometria stratului va fi de tip poligon iar informatia alfanumerica trebuie sa fie scrisa cu diacritice.

Harta Angajatorilor din Municipiul Bucuresti trebuie sa contina informatia vectoriala si alfanumerica aferenta Angajatorilor din Municipiul Bucuresti. Campurile cu datele alfanumerice aferente obiectelor vectoriale trebuie sa contina minim urmatoarele informatii:

a. Nume Localitate;

b. Nume UAT;
c. Nume Judet;
d. Cod Judet (Prescurtare denumire judet, Ex: Alba – AB, Brasov – BV etc.);
e. Tip UAT;
f. Siruta;
g. Siruta UAT;
h. Resedinta;
i. Denumire Angajator;
j. Adresa Sediu Social;
k. Adresa Punct de Lucru;
l. CUI;
m. Obiectul principal de activitate al Angajatorului;
n. Contact;
o. Observatii.

Similar hartii aferente municipiului Bucuresti, realizata de catre Prestator, se va include informatia geospatiala de catre angajatii Beneficiarului pe masura efectuarii de controale pe teren folosind functionalitatile sistemului dezvoltat de catre Furnizor.

Geometria stratului va fi de tip punct iar informatia alfanumerica trebuie sa fie scrisa cu diacritice.

Straturile din baza de date trebuie sa fie realizate corect topologic prin respectarea regulilor de completitudine a datelor vectoriale geospatiale si a relatiilor dintre ele.

Ofertantul trebuie sa descrie in cadrul Propunerii Tehnice procesele prin care realizeaza urmatoarele etape de productie pentru indeplinirea cerintelor de la acest capitol:

- Geocodare informatiilor alfanumerice;
- Publicarea serviciilor cu informatie spatiala.

3.6.4.5. Software pentru platforma antivirus

Solutia antivirus va asigura protectia tuturor echipamentelor de procesare livrate in cadrul proiectului. Antivirusul trebuie sa indeplineasca urmatoarele cerinte:

- Actualizare automata si programabila prin internet sau de pe servere de update locale la interval de timp programate (minim 1 ora) sau la cerere;
- Scanare in timp real a fisierelor ce trec prin server, atat la deschiderea acestora, cat si la

inchidere; posibilitatea scanarii la cerere si a serverului pe care este instalat;

- Cu ajutorul unei baze de date complete cu semnaturi de spyware si a euristicii de detectie a acestui tip de programe, produsul va trebui sa ofere protectie anti-spyware si sa permita prevenirea furtului de date confidentiale;
- Solutia trebuie sa detecteze si sa protejeze impotriva virusilor, virusilor de tip file infector, virusilor de boot, virusilor polimorfici, virusilor de macro, scripturilor malitioase, cailor troieni, viermilor, 'bots', 'backdoors';
- Solutia trebuie sa detecteze si protejeze impotriva aplicatiilor de tip adware si spyware si a atacurilor 'phishing';
- Solutia trebuie sa ofere protectie impotriva amenintarilor necunoscute prin livrarea de semnaturi dinamice oferite gratuit de producatorul sistemului antivirus printr-un serviciu integrat in clientul de antivirus si livrare acestor semnaturi dinamice din Internet;
- Solutia trebuie sa permita controlul resurselor de procesor ocupate de clientul antivirus prin setarea unei limite intre 10-90%;
- Administrarea trebuie sa poata fi facuta centralizat din cadrul consolei de management globale sau independent;
- Posibilitatea scanarii la alegere doar a fisierelor avand extensiile specificate de administrator precum si optiunea de scanare numai a fisierelor de o dimensiune mai mica decat o limita stabilita de administrator;
- Posibilitate de scanare a fisierelor deja existente pe server;
- Solutia trebuie sa ofere controlul sistemului firewall din sistemul de operare;
- Auto-submit pentru fisierele suspecte catre laboratorul de analiza al producatorului;
- Posibilitati de actiuni multiple la detectia unui virus (disinfect, delete, mutare in carantina);
- Protectia in timp real antivirus si antispyware trebuie sa fie asigurata prin intermediul tehnologiei de tip "mini-filter";
- Clientii antivirus trebuie sa permita monitorizarea activa a registrilor;
- Clientii antivirus trebuie sa permita definirea unor liste de excludere de la scanare a anumitor directoare, discuri, fisiere dorite sau extensii si fisere accesate de o lista de procese date;
- Informatiile colectate de la clienti si folosite pentru raportare trebuie sa poata fi stocate

intr-o baza de date relationala (SGBD);

- Actualizarea antivirus trebuie sa poata fi facuta automat la un interval de minim 1 ora, on demand precum si fortat de catre producatorul antivirusului in momentul aparitiei unei amenintari virale astfel incit sa nu existe brese de timp intre aparitia semnaturilor de virusi aparute pe site-ul producatorului si momentul actualizarii serverului de mail;
- Protectie antivirus, antispyware si antirootkit superioara pentru fluxul de fisiere;
- Solutia trebuie sa permita extragerea informatiilor din baza de data relationala (SGBD) pentru rapoarte complexe statice si dinamice cu privire la nivelul securitatii: statusul deployment-ului, sumar al amenintarilor si vulnerabilitatilor si starea statiilor administrate;
- Protectie euristica proactiva impotriva pericolelor informatice pe durata "ferestrei de vulnerabilitate";
- Scanare optimizata, pentru accesarea mai rapida a fisierelor;
- Scanare pe mai multe fire de executie pentru reducerea timpului necesar acestui proces;
- Scanare la acces si la cerere pentru protectia completa a serverului de fisiere;
- Compatibilitate cu consola de administrare centralizata, care reduce eforturile de administrare;
- Compatibilitate cu arhitectura pe 64 de biti;
- Scanare si marcare fisiere "protejate la scriere" (read only files) o singura data in cursul aceleiasi sesiuni si sa nu repete scanarea decat la lansare unei noi sesiuni, in cazul unei actualizari sau a unei infectii in sistem;
- Sa permita accesarea foarte rapida a fisierelor, datorita functionalitatii sale avansate de scanare pe mai multe fire de executie (multithread scanning);
- Sa ofere o optiune configurabila de programare a scanarilor antivirus la cerere si a actualizarilor;
- Sa lanseze notificari legate de efectuarea scanarilor si a actualizarilor prin intermediul modulului sau eficient de Alerte;
- Update inclus pentru o perioada de minim 1 an.

Licentierea solutiei va acoperi toate echipamente de procesare ofertate.

3.6.4.6. Software pentru platforma fluxuri control si preventie

In vederea asigurarii posibilitatii de derulare a proceselor specifice de control, monitorizare si preventie, va fi necesara existenta urmatoarelor capabilitati tehnice ale acestui modul:

- Modulul trebuie sa se integreze cu portalul astfel incat care sa permita accesul atat din interior cat si din exterior la zone diferite de informatie si documente – ca atare modulul trebuie sa fie dezvoltat in concordanta cu standardele si protocoale tehnologice internationale, precum JSR168, HTML, XHTML, XML, XSL, WSDL, SOAP, LDAP;
- Sa inregistreze, scaneze si sa stocheze in format electronic orice document intrat in institutie impreuna cu orice alte atribute conexe care sa ajute la o rapida organizare si ordonare, dupa tip, data, expeditor, destinatar persoana sau compartiment caruia ii este adresat explicit sau automat prin fluxul informational definit pentru respectivul tip de document;
- Sa permita definirea de fluxuri de lucru folosind un designer grafic web based;
- Pentru fluxurile de lucru definite sa se poata crea formulare care sa poata fi completate de-a lungul activitatilor care sunt indeplinite de participantii la flux;
- Formularele trebuie sa poata fi create utilizand un designer grafic web based, integrat in solutie;
- Sistemul trebuie sa aiba integrat un generator de documente in format Word. Acest generator trebuie sa permita adaugarea de sabloane de documente in format Word si posibilitatea de creare documente Word pe baza sabloanelor si metadatelor introduse. Metadatele vor fi adaugate in campurile definite in fisier si vor fi asociate in functie de tipul de document asociat cu sablonul. Generatorul de documente trebuie sa fie disponibil din interfata web;
- Modulul trebuie sa aiba facilitatea de a prezenta un raport cu documentele aflate curent in lucru la un utilizator, starea acestora si timpul afectat rezolvarii lor, precum si o lista cu documente cu termen de rezolvare depasit;
- Sa permita regasirea rapida a documentului prin metode de cautare moderne, dupa oricare dintre atributele asociate acestuia;
- Criteriile de cautare vor fi: dupa metadate, comentarii, versiune, adnotari si continut;
- Sistemul trebuie sa ofere posibilitatea de a reutiliza indecsii de cautare, de a filtra

rezultatele cautarilor daca numarul de documente este prea mare, precum si de a sorta rezultatele cautarilor;

- Sa permita stocarea tuturor documentelor interne in format electronic intr-un depozit accesabil on-line si cu o structura ce asigura evidentierea versiunilor intermediare de lucru, impreuna cu atributele lor, astfel incat sa se poata gasi repede informatia necesara;
- Solutia trebuie sa permita atat vizualizarea documentelor in fereastra de lucru cat si posibilitatea de a vizualiza informatiile asociate acestuia (atributele documentului), precum si informatii referitoare la versiunile intermediare de lucru;
- Sa permita lucrul pe comisii de specialitate de la distanta prin prezentarea electronica a documentelor si preluarea propunerilor si observatiilor facute;
- Sa prezinte documentele in format electronic spre consultare, in conformitate cu rolurile si drepturile asociate utilizatorilor;
- Interfata sa se afiseze in functie de drepturile de acces si rolurile asociate utilizatorilor;
- Sistemul trebuie sa ofere posibilitatea stocarii documentelor intr-un spatiu centralizat si organizat, indiferent de tipul documentului;
- Trebuie sa fie integrat cu suita Microsoft Office si Open Office;
- Sistemul trebuie sa ofere posibilitatea de asociere pe fiecare document in parte a unor informatii auxiliare despre data crearii, autor, cuvinte cheie, tipul documentului si descriere pe fiecare versiune in parte;
- Modulul trebuie sa dispuna de un modul de tip „enterprise search” care sa permita cautarea atat in depozitul propriu cat si pe siturile interne ale institutiei sau in exterior si organizarea rezultatelor astfel incat sa permita regasirea dupa cuvinte cheie si ordonarea raspunsurilor in functie de relevanta rezultatelor;
- Modulul trebuie sa permita pastrarea de profile de cautare si definirea de cautari personalizate. Sistemul de cautare trebuie sa detina facilitati de rafinare a rezultatelor afisate;
- Sistemul de cautare trebuie sa ofere urmatoarele functionalitati Componente de cautare oferite utilizatorilor:
    a. Auto-completare (afisarea unei liste de cuvinte care incep cu caracterele deja introduse);
    b. Auto- corectie (corectarea automata a termenilor de cautare);

c. Cautare booleana folosind operatori logici de tip AND, OR, excludere termen, fraza exacta, interval de cautare, ignorare majuscule;
d. Activare indecsi document ca filtre de cautare;
e. Cautare in campuri suplimentare predefinite;
f. Cautare in tezaur;
g. Evidentierea termenilor cautati;
h. Cautare inflexata (sistemul va folosi automat toate inflexiunile termenilor cautati ex. „a scrie” => „scriu”;
i. Posiblitatea cautarii cu wildcard-uri (caractere tip „*” care inlocuiesc portiuni);
j. Cautare utilizand game de valori;
k. Atunci cand se efectueaza cautarea dupa un cuvant, alte cuvinte cheie similare pot sa aduca rezultate relevante. Utilizand cautarea dupa sinonime, motorul de cautare trebuie sa poata sugera termeni de cautare pentru utilizator. De exemplu, daca se efectueaza o cautare dupa cuvantul „polita”, motorul de cautare poate sugera alternative ca „intelegere” sau “contract”;
l. Motorul de cautare trebuie sa ofere informatii legate logic de cererea de cautare. De exemplu, lista de rezultate returnata de o cautare a cuvantului „petitie” sa contina si termenii „petent” sau „rezolutie”, acesti termeni fiind derivati din context;

- Pentru fiecare document in parte se doreste ca sistemul sa stocheze versiunile ce sunt create la fiecare modificare facuta de catre utilizatorii care au drept de modificare. Acest lucru este necesar pentru a se putea urmari trasabilitatea pe fiecare document in parte;
- Sistemul trebuie sa fie document centric, permitand tuturor utilizatorilor cu drepturi sa intervina asupra unui document electronic, in functie de regulile prestabilite;
- Sistemul trebuie sa fie capabil sa atentioneze automat utilizatorii, prin notificarea pe e-mail, asupra necesitatii interventiei asupra unui document si sa actualizeze automat stadiul documentului;
- Pentru imbunatatirea comunicatiei si a mecanismului de transmitere a informatii lor este necesara integrarea Modulului de gestiune a documentelor si a fluxurilor de lucru cu sisteme de e-mail printr-un sistem de notificari la cerere;
- Sistemul trebuie sa permita transmiterea informatiilor despre activitatea ce trebuie

realizata de catre un utilizator prin mesaje e-mail astfel incat acesta sa primeasca aceste informatii chiar daca nu este conectat in permanenta la sistemul;

- Modulul trebuie sa dispuna de functionalitatea de expunere a depozitului de documente si a activitatilor de workflow in format RSS;
- Sistemul trebuie sa puna automat la dispozitia utilizatorului responsabil de prelucrare, documentele necesare in vederea operarii lor;
- Continutul documentelor trebuie sa poata fi incarcat in baza de date, pentru a asigura controlul accesului la documente, dar totodata sa se ofere si posibilitatea incarcarii numai a unei referinte la un document electronic sau in format hartie;
- Sistemul trebuie sa ofere facilitati de management de inregistrari (Records Management) conform ISO15489 si Moreq2. Aceste functionalitati trebuie sa fie accesibile din interfata de baza si nu dintr-o interfata separata;
- Sistemul trebuie sa permita introducerea metadatelor unui document fara obligativitatea introducerii continutului. De exemplu, daca nu exista posibilitatea de scanare a documentelor, atunci se pot introduce doar metadatele asociate, care sa identifice documentul si locatia in care se afla, pentru a avea o referinta electronica a acestuia. In acest caz prin intermediul fluxurilor de documente sunt transmise doar referintele, urmand ca documentele in format hartie sa fie transmise pe caile uzuale.
- Sistemul trebuie sa poata defini si utiliza exact structura organizatorica a organizatiei;
- Accesul trebuie sa se faca in mod controlat si sigur prin definirea de utilizatori, grupuri de utilizatori si drepturi de acces la diferite functionalitati si documente sau dosare. Pentru a putea obtine informatii din sistem, un utilizator va trebui sa se autentifice la conectare. Dupa inchiderea sesiunii (prin actiunea explicita a utilizatorilor sau prin inchiderea aplicatiei client), sistemul nu va permite refolosirea sesiunii incheiate (de exemplu: Prin functionalitatea de „Back” a navigatoarelor Web);
- Un utilizator poate apartine de unul sau mai multe grupuri de securitate;
- Fiecare utilizator va avea acces doar la documentele si informatiile la care i-a fost permis explicit accesul;
- Pentru fiecare din functionalitatile Modulului, utilizatorul cu drept de administrare va defini drepturile de acces pentru utilizatori, acestia putand avea sau nu drept de vizualizare asupra functionalitatilor;

- De asemenea, drepturile de acces trebuie specificate si la nivel de folder, dosar sau document. Trebuie sa se permita mostenirea drepturilor de acces in structura ierarhica a spatiului de stocare a documentelor;
- Sistemul trebuie sa permita accesarea tuturor functionalitatilor sale, in functie de drepturile de acces ale utilizatorilor, prin realizarea unei singure actiuni de autentificare. Nu se doreste ca aceasta accesare sa se faca prin deschiderea mai multor module separate ci sa fie prezentata o interfata unica;
- Sistemul trebuie sa contina suport pentru mecanisme de autentificare cel putin bazate pe standardul LDAP, pentru a permite conectarea utilizatorilor folosind mecanismele de conectare in domeniu;
- Sistemul trebuie sa permita criptarea documentelor pe 128 biti si utilizarea de chei de criptare;
- Sistemul trebuie sa permita transmiterea documentelor pe fax, email, imprimanta direct din interfata acestuia;
- Sistemul trebuie sa ofere posibilitatea utilizatorilor de a se conecta folosind un client smartphone non-web (Windows, Java, iPhone);
- Avand in vedere necesitatile de mobilitate si variatatea echipamentelor folosite in institutie sistemul trebuie sa ofere cel putin urmatoarele optiuni de client/administrare:
- Sistemul trebuie sa permita pornirea de fluxuri ad-hoc de tip informare/distribuire sau de tip avizare/aprobare cu selectarea utilizatorilor sau grupurilor de utilizatori care vor fi implicati. De asemenea, trebuie sa permita salvarea acestor fluxuri ad-hoc pentru refolosirea ulterioara;
- Sistemul trebuie sa permita nativ integrarea cu LDAP pentru autentificarea si managementul centralizat al utilizatorilor;
- Modulul va permite scanarea direct din cadrul solutiei, fara necesitatea apelarii unei aplicatii externe. Sistemul va fi compatibil cu driverele TWAIN si ISIS, sa permita realizarea de profiluri de scanare, configurarea unor facilitati precum: stabilirea nivelului de alb din pagina, rezolutie, calitatea imaginii, setarea formatului imaginii si al compresiei acesteia, dimensiunea paginii scanate, sa permita setarea scanarii duplex sau simplex;
- Sistemul trebuie sa permita utilizarea de separatori de documente pentru oferirea

posibilitatii de automatizare a separarii documentelor scanate in loturi din cadrul unor procese de lucru;

- Facilitatile de administrare vor fi permise inclusiv din interfata Web;
- Sistemul trebuie sa permita oferirea de drepturi multiple de acces in cadrul solutiei, adaugare de noi utilizatori, mostenirea de drepturi, gruparea utilizatorilor in grupuri, asocierea de administratori de grupuri de utilizatori;
- Necesitatile de securitate la nivelul institutiei impun o granularitate crescuta a drepturilor utilizatorilor asupra anumitor actiuni. In acest sens s-au identificat urmatoarele permisiuni speciale:
    m. *Editare document*: utilizatorul poate crea si edita documente;
    n. *Modificare parametri stare document*: utilizatorul poate schimba statusul unui obiect (sa nu fie controlat din punct de vedere al versiunii, sa fie controlat din punct de vedere al versiunii, read-only);
    o. *Administrare flux de lucru*: utilizatorul are posibilitatea de a crea si administra fluxurile de lucru;
    p. *Lansare fluxuri de lucru*: utilizatorul poate initializa fluxuri de lucru;
    q. *Editare formulare cuvinte cheie*: etilizatorul poate crea, edita si modifica formulare de indexare cu cuvinte cheie;
    r. *Editare data de expirare*: utilizatorul poate edita si seta data expirarii documentelor;
    s. *Administrare cale de indosariere*: utilizatorul poate modifica setarile caii de stocare a documentelor in meniul;
    t. *Stergere versiuni*: utilizatorul poate sterge versiunile unui document ce are optiunea de control a versiunilor activata;
    u. *Autor pentru versiuni limitate*: permite crearea si editarea unui numar limitat de documente;
- Sistemul va oferi posibilitatea de setare de drepturi de access pentru utilizatori si grupuri de utilizatori, cu granularitate pana la nivel de document si camp de indexare asociat documentului;
- Sistemul va detine facilitatea de realizare de preview al unui document prin transformarea documentului in sine, in format TIFF sau PDF spre exemplu;

- Sistemul va detine optiuni de imbunatatire a calitatii imaginii precum si optiuni multiple de vizualizare a acestor imagini: zoom pe zone, incadrari pe orizontala sau verticala, fullscreen, rotire imagine, vizualizare serii de imagine in forma Thumbnail cu preview;
- Sistemul va prezenta facilitati de recunoastere OCR, BCR;
- Sistemul trebuie sa permita adaugarea de adnotari de tip imagine (stamp) la un document (de exemplu pentru marcare ca draft a unui document);
- Sistemul trebuie sa permita adaugarea de adnotari asupra documentului. Adnotarile sa poata fi publice sau private;
- Sistemul trebuie sa permita notificari automate ca e-mail sau task;
- Sistemul trebuie sa permita extinderea functionalitatilor direct din cadrul interfetei de lucru de catre utilizator, printr-o zona de scripting, pentru a automatiza anumite activitati;
- Sistemul trebuie sa permita integrarea cu cel putin urmatoarele tipuri de aplicatii: ERP, CRM, CAD;
- Sistemul trebuie sa permita folosirea sistemelor profesionala de stocare: benzi magnetice, blueray-uri, storage-uri;
- Sistemul trebuie sa includa un modul specializat de registratura;
- Sistemul va oferi posibilitatea de tiparire a registrelor de documente;
- Sistemul trebuie sa permita realizarea unui nomenclator de documente si a unor forme de indexare;
- Sistemul trebuie sa permita definirea de template-uri de documente;
- Interfata utilizator va fi multilingva, utilizatorul avand posibilitatea de a realiza selectie in momentul autentificarii;
- Sistemul trebuie sa ofere o interfata de tip API, care sa ofere suport pentru dezvoltarea/integrarea cu alte sisteme folosind limbajele de programare Java si .NET;
- Sistemul trebuie sa detina un mecanism avansat de Audit, care sa furnizeze rapoarte la nivel general si individual;
- Sistemul trebuie sa ofere un mecanism ce permite inghetarea documentelor;
- Sistemul trebuie sa permita mutarea de documente in aria de lucru a altui utilizator;
- Sistemul va detine facilitati de restaurare a elementelor sterse;
- Sistemul va prezinta facilitati de replicare intre client si server si server-server;

- Sistemul trebuie sa permita adaugarea de “voice notes” ca atasament la documentul respectiv (de exemplu o inregistrare vocala care sa stabileasca instructiuni cu privire la acel document);
- Sistemul va putea permite definirea si utilizarea taxonomiilor;
- Sistemul va permite afisarea documentelor grupate in foldere virtuale in functie de metadatele asociate. Ex. documentele referitoare la un anumit angajator vor putea fi afisate ca apartinand unui folder cu numele acelui angajator chiar daca in sistem ele sunt stocate diferit;
- Sistemul trebuie sa ofere functionalitati native de semnatura digitala.

Platforma de fluxuri control si preventie se va licentia astfel incat sa asigure rularea pe minim 6 nuclee de procesare active, 1.000 de utilizatori interni (cu drepturi de scriere) si numar nelimitat de utilizatori externi (cu drept de acces de tip read-only).

3.6.4.7. Software pentru platforma de Raportare si Business Intelligence

Platforma de raportare si BI trebuie sa asigure urmatoarele:

- Suport de servicii de transformare a datelor pentru a putea permite importuri din surse de date neomogene;
- Serverul de analiza si raportare trebuie sa permita folosirea a peste 64Gb memorie;
- Index secundar la nivel de coloane care sa comprime si sa stocheze datele in memorie pentru access rapid la datele din depozit;
- Posibilitatea de a procesa sute de milioane de linii in mai putin de o secunda pentru access rapid la rapoarte;
- Afisarea rapoartelor intr-un mod interactiv, astfel incat utilizatorii sa poata urmari evolutia in timp a anumitor evenimente, sa poata efectua filtrari asupra datelor prezentate;
- Facilitati de analiza a datelor, data mining (OLAP);
- Functionalitati native de extragere a datelor din diferite surse de date, realizarea de filtrari, agregari si diferite alte transformari asupra datelor si in final stocarea datelor in data warehouse (ETL);
- Stocarea datelor in cuburi multidimensionale pentru interogarii si construire de rapoarte relevante;

- Posibilitati de raportare din surse de date precum Oracle Database, Microsoft SQL Server, SAP NetWeaver BI, Hyperion, Teradata;
- Posibilitati de raportare cu moduri multiple de vizualizari: harti, sparklines si indicatori:
    - Harti: Posibilitatea de creare de rapoarte folosind componente de tip wizard care permit vizualizarea datelor sub forma unui model geografic care poate prelua datele dintr-o galerie de harti pe baza de interogari SQL sau dintr-un fisier stocat in sisteme tip GIS. Elementele dintr-o harta pot fi poligoane (pentru reprezentare de arii), linii (pentru reprezentarea de rute si drumuri) si puncte (reprezentand locatii diverse). Se pot adauga date aditionale de afisare sau atentionari interactive folosind harti online;
    - Sparklines: Posibilitate de creare rapoarte folosind tabele si matrici pentru a afisa date agregate;
    - Indicatori: Posibilitatea de vizualizarea a datelor intr-un mod rapid folosind metode grafice (icoane).
- Instrumente de data mining;
- Capabilitate de raportare “ad hoc” cu ajutorul careia utilizatorii sa poata edita propriile rapoarte pe baza unui model (template), fara sa detina cunostinte de baze de date sau despre structura acestora. Serviciile de raportare trebuie sa fie incluse in solutie, fara add-on-uri suplimentare;
- Facilitati de interogare a datelor disparate in momentul solicitarii rapoartelor;
- Extragerea si editarea dinamica a rapoartelor utilizand instrumente familiare de tip Office si interfete intuitive care includ harti, sparklines si indicatori;
- Sa permita exportarea rapoartelor in Excel, fisiere CSV, o alta baza de date, fisiere XML;
- Sa permita exportul in documente tip PDF, TIFF;
- Posibilitati de colaborare cu ajutorul instrumentelor de analiza de tip pivot;
- Posibilitatea abonarii la alerte in cazul unor evenimente din baza de date.

Platforma de raportare si BI se va licentia atfel incat sa asigure rularea pe minim 6 nuclee de procesare active, 1.000 de utilizatori interni si numar nelimitat de utilizatori externi ai sistemului.

3.6.4.8. Software pentru platforma de transformare si preluare date

Modulul transformare si preluare date ANAF si RC va fi implementat cu ajutotul unei platforme dedicate care trebuie sa prezinte urmatoarele caracteristici tehnice minime

Transformare

Aceasta componenta va avea doua module, unul ce se va putea instala pe statiile administratorilor sistemului si unul de tip server pentru executia si stocarea sabloanelor de integrare.

Modulul desktop pentru minim 5 utilizatori:

- Solutia trebuie sa dispuna de o librarie de sabloane cu filtre si functii ce pot fi aplicate pentru procesarea datelor;
- Solutia trebuie sa suporte integrari de date din fisiere multiple cu posibilitatea de a selecta sursele sau destinatiile in mod dinamic la rulare;
- Solutia trebuie sa permita reutilizarea modelelor de integrare pentru orice fel de continut
- Solutia trebuie sa permita manipularea datelor preluate prin aplicarea de filtre, inserare de functii, constante sau alti operatori asfle incat datele sa fie utilizabile de sistemul destinatie;
- Solutia trebuie sa permita transformari complexe de date in care datele de iesire dintr-o integrare sau transpunere sa devina date de intrare pentru alt proces;
- Solutia trebuie sa permita sortarea datelor de intrare sau de iesire dupa caz;

Cerinte specifice privind modelarea si crearea de servicii de date bazate pe XML:

- Solutia trebuie sa permita maparea grafica a datelor in format XML;
- Solutia trebuie sa permita transformarea de date XML;
- Solutia trebuie sa permita crearea de mapari complexe XML in care datele de iesire ale unei mapari devin date de intrare pentru alte mapari;
- Solutia trebuie sa permita crearea de mapari pe baza unor surse de date provenite din baze de date;
- Solutia trebuie sa permita crearea de mapari din baza de date catre date XML;
- Solutia trebuie sa permita construirea de servicii web pornind de la surse de date;

- Solutia trebuie sa permita conectarea la servicii web bazate pe WSDL 1.1 or 2.0 si integrarii functionalitatilor direct in maparile XML destinatie;
- Solutia trebuie sa permita generarea automata de cod intr-un limbaj de tip enterprise pentru crearea de mapari;
- Solutia trebuie sa permita folosirea de semnaturi digitale XML.

Modulul tip server:

Modulul de tip server va fi componenta principala de orchestrare si automatizare a proceselor de integrare. Acest modul este motorul de executie al modelelor generate de modulul de tip desktop. Modulul server trebuie sa ofere minim urmatoarele functionalitati:

- Management avansat al tranzactiilor:
    - Trebuie sa ofere o interfata grafica Web pentru administrare si monitorizare a tranzactiilor;
    - Trebuie sa suporte configurare programabila folosind "triggeri" pentru rularea job-urilor;
    - Trebuie sa suporte configurarea mai multor triggeri pentru acelasi job;
    - Trebuie sa permita rularea mai multor triggeri simultan;
    - Trebuie sa permita functii de tip "precaching" al datelor pentru tranzactiile consumatoare de resurse sau timp;
    - Trebuie sa ofere posibiliatea generarii de log-uri pentru toate job-urile executate;
    - Trebuie sa permita configurarea unor containere pentru stocarea maparilor, profilelor si datelor stocate pentru fiecare utilizator;
    - Trebuie sa suporte configuratii de tip "multi-tenant" intr-o singura instanta pentru a permite folosirea de mai multe departamente sau utilizatori a solutiei;
    - Trebuie sa permita configurarea de alerte e-mail pentru toti pasii de executie;
    - Trebuie sa permita rularea fluxurilor din interfata grafica sau direct din consola (CLI);
- Management si executie centralizata a modelelor de integrare
    - Trebuie sa ofere capabilitati de preprocesare ale maparilor de date pentru optimizarea vitezei de executie dar si a utilizarii memoriei serverului;

- Trebuie sa permita importul de fisiere generate de administratori in modulul desktop;
- Sisteme de operare suportate: Windows, Linux, MacOS X;

Preluare

Solutia trebuie sa ofere un mecanism/serviciu pentru transmitere de mesaje la nivel de aplicatie cu urmatoarele caracteristici:

- Trebuie sa includa posibilitatea stocarii mesajelor intern;
- Trebuie sa permita afisarea unor informatii de procesare precum numarul de mesaje procesate, starea serviciului, mesaje de eroare daca exista;
- Trebuie sa permita conectarea la serverele de aplicatie si accesul la datele interne;
- Caracteristicile cerute ale componentei:
  - Transfer al mesajelor folosind protocoale sigure (reliable);
  - Transformarea mesajelor intre diferite formate;
  - Orchestrarea mesajelor si procesare asincrona;
  - SDK si API pentru dezvoltare personalizata;
  - Prelucrarea mesajelor in secventa si livrarea acestora in cadru de tranzactie;
  - Publicarea mesajelor sub forma de servicii web;
  - Arhitectura de tip inregistrare / publicare;
  - Baza de date si log detasabil cu posibilitate de extragere a informatiilor in medii externe;
  - Posibilitate de sincronizare de la sursa de timp NTP sau optiune de atasare sursa de timp GPS;
- Protocoalele suportate trebuie sa dea posibilitatea de a se transmite si prelua date prin diverse protocoale precum FTP/SFTP, protocoale de cozi de mesaje, HTTP, FILE, POP3, SMTP, REST, SOAP etc.;
- Formatele de mesaje suportate XML, CSV, dar si alte standarde de mesaje precum UN/EDIFACT si EDI (X12), XBRL, ebXML, OOXML, HL7 2.2-2.6, 3.0, AIS (Automatic Identification System);
- Trebuie sa suporte mai multe sisteme de baze de date precum Microsoft SQL Server, DB2, Oracle etc.;

- Securitatea trebuie asigurata prin:
    - Criptarea mesajelor transmise folosind certificate digitale;
    - Stocarea criptata a mesajelor;
    - Comunicatii pe canale SSL;
    - Posibilitate de administrare de la distanta, pe un canal securizat;

Platforma de transformare poate fi oferita ca un appliance de transformare dedicat sau ca masina/masini virtuale care vor rula pe o resursa hardware dedicata si diferita de echipamentele de calcul prezentate la capitolul *Infrastructura hardware*.

3.6.4.9. Platforma de certificate digitale

Solutia trebuie sa ofere un grad sporit de securitate prin integrarea comunicatiilor autentificate prin certificatele digitale cu autorizarea dispozitivelor prin folosirea de tokenuri OTP.

Solutia pentru managementul autentificarii multi-factor trebuie sa includa certificate digitale calificate si tokenuri OTP pentru toti cei 1.000 de utilizatori de terminale mobile.

Solutia trebuie sa asigure indeplinirea urmatoarelor cerinte:

- Solutia trebuie sa beneficieze de functionalitate integrata de autoritate de certificare (CA) pentru emitere si revocare de certificate digitale;
- Solutia trebuie sa ofere suport pentru metoda de autentificare challenge-response;
- Certificate digitale emise de catre autoritatea de certificare trebuie sa prezinte un grad ridicat de securitate astfel incat:
    - Sa suporte cel putin functiile SHA-256, SHA-384, SHA-512;
    - Lungimea cheii sa fie de cel putin 2048, 3072 sau 4096 biti.
- Solutia trebuie sa contina mecanism implementat de prevenire a atacurilor de tip “brute force”;
- Solutia trebuie sa ofere functionalitate de autentificare prin mecanismul “OTP – One-Time Password”. Aceasta metoda se bazeaza pe ideea ca parola folosita la autentificare este valabila pe perioada acelei sesiuni de lucru;
- Solutia trebuie sa ofere metode de generare a parolei OTP atat de tipul “Event based”, cat si de tipul “Time based”;
- Tokenurile OTP trebuie sa ofere suport pentru standardele DES si 3DES;
- Solutia trebuie sa asigure conformite cu standardul SAML v2;

- Solutia trebuie sa suporte cel putin functiile de criptare 3DES, AES, RSA, familiile ECC si SHA-2;
- Solutia trebuie sa ofere functionalitate de detectare a amenintarilor, astfel incat sa poata detecta accesul de la computere folosite in scop malitios sau compromise in acest sens, detecta credentialele compromise si bloca conturile de utilizator compromise;
- Solutia trebuie sa ofere functionalitati de integrare cu protocoale de autentificare standard cum sunt LDAP si RADIUS;
- Solutia trebuie sa ofere suport pentru protocolul SCEP (Simple Certificate Enrollment Protocol);
- Solutia trebuie sa permita integrarea autoritatii de certificare intr-o structura PKI existenta;
- Autoritatea de certificare trebuie sa poata oferi certificate digitale atat pentru dispozitive, cat si pentru utilizatori;
- Autoritatea de certificare trebuie sa ofere functionalitate de subiect dinamic in certificatele digitale astfel in permita alocarea automata a certificatelor catre utilizatori si dispozitive;
- Autoritatea de certificare va trebui sa ofere suport pentru subiecte alternative in cadrul certificatelor digitale;
- Autoritatea de certificare trebuie sa permita genera certificate digitale atat pentru semnatura electronica, cat si pentru criptarea informatiilor;
- Solutia trebuie sa ofere posibilitate de autentificare OTP cu echipamente si protocoale de autentificare multiple, astfel incat sa suporte urmatoarele tehnologii:
    - EMV CAP/DPA si Smartcard X.509;
    - Soft Token pe cele mai raspandite platforme de pe piata (cel putin iOS, Android si Java Blackberry);
    - Out of Band prin SMS sau E-mail.
- Tokenurile trebuie :
    - Sa fie de dimeniuni reduse, astfel incat sa poata fi atasate la suportul de chei;
    - Sa detina un display de cel putin 8 caractere;

    - Sa detina un singur buton pentru usurinta in folosire, iar la apasare acesta va trebui sa genereze un nou cod OTP;
    - Sa prezinte posibilitati de personalizare grafica astfel incat sa fie usor de distins.
- Sistemul de autentificare OTP trebuie sa fie disponibil pentru diverse sisteme de operare:
    - Unix (de exemplu) IBM AIX;
    - Linux (de exemplu Red Hat Enterprise Linux sau SUSE Enterprise Linux);
    - Altele (de exemplu Windows sau Solaris - SPARC).
- Solutia trebuie sa asigure gestionarea echipamentelor de autentificare si anume initializarea acestora, inrolarea, monitorizarea starii, sincronizarea blocarea si deblocarea;
- Solutia trebuie sa asigure managementul conturilor utilizator si anume inrolare, asignarea echipamentului de autentificare, tiparirea codului pin initial, monitorizarea starii / blocare;
- Solutia trebuie sa asigure managementul conturilor de administrator prin desemnarea de roluri si drepturi de acces;
- Solutia trebuie sa ofere suport pentru echipamente HSM;
- Solutia trebuie sa contina modul de de statistici si raportare;
- Solutia trebuie sa asigure auditarea tuturor operatiunilor efectuate in cadrul sistemului de autentificare;
- Solutia trebuie sa ofere suport pentru protocolul de monitorizare SNMP v3;
- Solutia trebuie sa respecte standardele ISO 7810, ISO 14443, OATH, RoHS;
- Solutia trebuie sa poata fi accesata si gestionata cu usurinta de oriunde prin intermediul unui browser web;
- Solutia nu trebuie sa fie dependenta de un anume sistem de operare;
- Solutia trebuie sa poata fi integrata cu usurinta in infrastructura existenta, fara modificari substantiale, atat intr-un mediu fizic, cat si intr-un mediu virtual;
- Solutia trebuie sa includa toate componentele software si licentele necesare pentru a functiona in mod corespunzator;
- Solutia trebuie sa contina doar componentele software necesare pentru a functiona in mod corespunzator si trebuie sa fie securizata atat la nivelul sistemului de operare, cat si al aplicatiei in sine;

- Solutia trebuie oferita impreuna cu documentatia tehnica aferenta;
- Trebuie oferita garantie si updateuri pentru minim 1 an;
- Pentru tokenuri garantia functionare a bateriei trebuie sa fie de minim 4 ani.

3.6.4.10. Platforma monitorizare infrastructura HW

Solutia de monitorizare trebuie sa ofere monitorizarea serverelor Windows, Linux sau Unix precum si a dispozitivelor de retea si alertare in cazul aparitiei unei erori, probleme de performanta, intrerupere in functionare la nivel de aplicatie, serviciu de aplicatie, server, dispozitive de retea (switch, routere, imprimante etc); oferirea unei explicatii pentru apartitia acelei erori; oferirea unei recomandari de solutionare a erorii aparute; posibilitatea de a lansa automat actiuni de remediere in cazul aparitiei unei erori; posibilitatea de a arhiva centralizat jurnalele de securitate ce contin istoricul accesului utilizatorilor la servere;
Solutia de monitorizare trebuie sa asigure indeplinirea urmatoarelor cerinte:

- Sa poata administra evenimentele sistemului de operare, ale serviciului director, ale serverului de aplicatii, printr-un jurnal de evenimente la nivel de organizatie care colecteaza si raporteaza problemele si informatiile generate referitoare la sistemele si aplicatiile din reteaua organizatiei;
- Sa permita monitorizarea switch-urilor, routerelor, imprimantelor si altor echipamente prin SNMP cu suport pentru SNMP v1,v2 sau v3; monitorizare virtual local area networks (VLAN) si grupuri Hot Standby Router Protocol (HSRP);
- Sa permita monitorizarea sistemelor Linux/Unix cu suport pentru RedHat Enterprise Server, centOS, Suse Linux Enterprise Server, IBM AIX, HP UX;
- Sa permita monitorizarea proactiva si generarea de mesaje de avertizare prin capacitatile distribuite care urmaresc si monitorizeaza informatiile si trimit problemele la telefoane mobile, prin e-mail sau prin alte medii externe; aceste avertizari sa poata lansa task-uri automate care sa duca la rezolvarea problemelor;
- Sa efectueze raportarea si analiza tendintelor, necesare pentru urmarirea problemelor in timp si generarea rapoartelor detaliate despre starea de functionare generala a mediului administrat; aceste rapoarte trebuie sa poata fi accesate local sau sa poata fi publicate pe site-uri Web pentru accesul facil la informatiile de administrare ale sistemelor;
- Sa permita exportul rapoartelor in formate uzuale precum pdf, doc etc.;

- Sa permita monitorizarea unei infrastructuri ce contine mii de statii client, servere si aplicatii;
- Sa permita monitorizarea aplicatiilor distribuite pe mai multe servere;
- Sa ofere posibilitatea de a defini in mod grafic componentele unui serviciu;
- Sa permita monitorizarea si raportarea evenimentelor, urmarirea nivelului de sanatate al sistemului;
- Sa permita monitorizarea statiilor de lucru la nivelul sistemului de operare;
- Sa permita monitorizarea fara agent (agentless) prin capturarea erorilor de aplicatii;
- Sa permita crearea unor rapoarte si alerte pentru administratori privind problemele cu impact asupra sistemelor si utilizatorilor;
- Sa includa cele mai bune practici pentru descoperirea, monitorizarea, depanarea si rezolvarea problemelor pentru o componenta specifica (sistem de operare, aplicatie);
- Implicit, serverul trebuie sa refuze conexiuni de la agenti instalati manual;
- Comunicatia dintre serverul de management si agenti trebuie sa fie autentificata si criptata;
- Administratorii trebuie sa poata avea nivele de securitate diferite si accesa separat consola de administrare;
- Monitorizeaza si raporteaza evenimentele, permite urmarirea nivelului de sanatate al sistemului precum si oferirea unui dashboard centralizat ce ofera informatiile critice despre resursele IT “business critical”;
- Integrare cu servicii director astfel incat prin introducerea unui nou echipament intr-un Organizational Unit (OU) el sa fie automat detectat iar agentul de monitorizare automat instalat si configurat sa comunice cu serverul de monitorizare;
- Posibilitatea de a colecta jurnalele de securitate din sistemele de operare Windows/Linux/Unix si stocarea lor intr-o baza de date separata;
- Posibilitatea de a colecta jurnale de securitate bazate pe standardul Syslog;
- Produsul trebuie sa fie livrat impreuna cu baza de date necesara functionarii corecte;
- Solutia trebuie sa permita crearea de diagrame care sa figureze aplicatiile si serviciile prin actiuni simple de tip drag and drop;

- Solutia trebuie sa permita vizualizarea simultanta atat a starii curente a serviciilor critice, cat si a indicatorilor de performanta asociati serviciilor precum: disponibilitate, timp de raspuns etc.;
- Solutia trebuie sa permita vizualizarea topologiei retelei si porturile la care sunt conectate echipamentele;
- Solutia trebuie sa permita nu numai identificarea problemei ci si localizarea acesteia prin intermediul diagramelor de tip harta ale centrului de date si ale rack-urilor gazduite in centrul de date;
- Solutia trebuie sa asigure tablouri de bord interactive pentru diversele roluri din organizatie, inclusiv factori decizionali si manageri si posibilitatea de vizualizare atat a imaginii de ansamblu, cat si navigarea in adancime pentru vizualizarea detaliilor problemei;
- Solutia trebuie sa permita definirea de harti geografice statice pentru localizarea echipamentelor, precum si harti geografice interactive cu functionalitati cel putin de tip zoom;
- Solutia trebuie sa permita vizualizarea starii chiar si de pe dispozitive mobile;
- Solutia trebuie sa permita prioritizarea incidentelor de rezolvat;
- Solutia trebuie sa includa tablouri de bord de depanare in timp real;
- Solutia se va licentia pentru toate echipamentele sistemului din centrul de date conform solutiei propuse.

3.6.4.11. Platforma backup si restaurare

Solutia de backup trebuie sa fie o aplicatie software dedicata pentru realizarea operatiunilor de backup, licentiata si configurata corespunzator pentru toate echipamentele din cadrul caietului de sarcini.

Serverul de back-up trebuie sa prezinte urmatoarele functionalitati minime:

- Serverul de backup va trebui sa execute backup-ul bazei de date;
- Sa se furnizeze toate licentele necesare pentru asigurarea backup-ului pe banda sau disc al serverelor de aplicatie si baze de date din solutie;
- Sa ofere agent dedicat pentru baza de date folosita in solutie;
- Sa permita instalare si backup-ul in configuratii de tip cluster;

- Solutia tehnica are ca obiectiv realizarea si securizarea comunicatiei intre cele 3 zone: LAN users, Corporate LAN si Internet;
- Trebuie sa ofere posibilitatea de a efectua back-up la nivel de date, server, sistem de operare si masini virtuale la un interval minim de 15 minute, fara intreruperea accesului utilizatorilor la acestea;
- Posibilitatea de a efectua back-up disk-to-disk si disk-to-tape;
- Posibilitatea de a efectua usor restaurarea datelor in caz de dezastru;
- Trebuie sa permita restaurarea serverelor dintr-o singura operatie, fara a fi necesara reinstalarea sistemului de operare, aplicatiei si datelor succesiv;
- Solutia sa permita backup pentru minim utlimele doua versiuni majore ale sistemului de operare ofertat;
- Solutia trebuie sa permita back-up pentru minim ultimele versiuni ale platformei de baza de date ofertata cu restaurare in locatia originala fara a fi necesare cunostinte avansate de SQL pentru operator; la sfarsitul operatiunii baza de date va fi montata si disponibilia; solutia trebuie sa ofere si restaurare in locatie alternativa pe acelasi server fara a perturba utilizatorii bazei de date in lucru;
- Posibilitatea de a efectua usor restaurarea datelor in caz de dezastru; solutia sa permita restaurarea serverelor dintr-o singura operatie – bare metal restore, fara a fi necesara reinstalarea sistemului de operare, aplicatiei si datelor succesiv;
- Solutia sa ofere posibilitate de a face backup pentru clienti protejati de firewall in retele de tip LAN sau wireless;
- Solutia sa ofere posibilitate de a face backup pentru client accesibili prin VPN cu suport pentru urmatoarele tipuri de protocol VPN Point-to-Point Tunneling Protocol (PPTP), Secure Socket Tunneling Protocol, (SSTP), Layer 2 Tunneling Protocol (L2TP);
- Solutia strebuie sa permita protectia clientilor conectati in retea sau offline;
- Trebuie sa ofere rapoarte locale si consolidate asupra intregului mediu de backup cat si a operatiunilor de backup;
- Solutia trebuie sa ofere o consola centralizata pentru managementul dintr-o singura consola a mai multor servere de backup;
- Produsul trebuie sa fie livrat impreuna cu baza de date necesare functionarii sale corecte;

- Sistemul se va licentia pentru toate serverele/componentele conform solutiei propuse.

3.7. Managementul utilizatorilor si accesul la sistem

In cadrul sistemului integrat SIAMC trebuie sa fie disponibile mecanisme si interfete de administrare si configurare a tuturor claselor si instantelor de entitati asociate rolurilor, grupurilor si profilelor de utilizatori, prin intermediul utilizarii componentei de administrare. Astfel, SIAMC va permite autentificarea tuturor utilizatorilor in conjuctie cu nivelurile de securitate prezente la toate nivelele arhitecturale.

Administratorii reprezinta o categorie aparte de utilizatori, ce acceseaza zona de management a sistemului, si vor avea configurate roluri si profile corespunzatoare astfel incat sa aiba acces la toate datele si modulele aplicatiei. Ei vor fi prevazuti si cu drepturi in subsistemul de administrare, pentru a avea acces in vederea monitorizarii, intretinerii si configurarii sistemului. In contextul controlului accesului, doar administratorii au dreptul de a specifica roluri pentru utilizatori si drepturi de acces ale acestora.

Utilizatorilor li se vor acorda permisiuni in mod individual sau pe grup. Apartenenta la un grup va acorda tuturor utilizatorilor din grupul respectiv drepturi echivalente. Un utilizator poate apartine simultan la unul sau mai multe grupuri. Drepturile vor putea fi mostenite. De asemenea, sistemul va permite notiunea de subgrup, care reprezinta posibilitatea ca un grup sa fie membru intr-un alt grup. Administrarea conturilor de utilizator se va face respectand urmatoarele cerinte:

- Sistemul asigneaza fiecarui cont de utilizator unui identificator unic;
- Sistemul va oferi reguli configurabile pentru crearea identificatorilor unici;
- Sistemul va include capabilitatea de a exporta/importa utilizatori;
- Sistemul ofera posibilitatea de a aproba in mod automat orice solicitare printr-un set de reguli si politici.

Sistemul va oferi capabilitatea de a vizualiza o solicitare de cont care a fost trimisa si datele asociate cu acea solicitare.

3.8. Securitatea sistemului

Sistemul informatic trebuie protejat impotriva incercarilor deliberate sau accidentale de acces neautorizat la datele pe care acestea le inmagazineaza. Sistemul trebuie sa permita urmatoarele facilitati:

- Ierarhizarea in grupuri a utilizatorilor finali;

- Autentificarea in sistem printr-un mecanism de tip „Single Sign-On”, permitind accesul utilizatorului in toate modulele pentru care dispune de drepturile necesare dupa introducerea numelui de utilizator si a parolei o singura data in cadrul unei sesiuni de lucru;
- Impiedicarea accesului utilizatorilor finali de a se conecta la sistem daca acesta este in stare de eroare;
- Asigurarea securitatii tuturor interfetelor sistemului informatic, prevenind accesul utilizatorilor neautorizati la sistem;
- Raportarea pe baze periodice a detaliilor privitoare la accesul in sistem al utilizatorilor;
- Sa poata fi definite drepturi de acces (vizualizare/ actualizare) la informatie pentru utilizatori/ roluri/ grupuri;
- Pentru fiecare rol, in functie de specificul activitatii acestuia, se vor stabili componentele sistemului informatic care trebuie sa acopere activitatea curenta. Se va realiza asocierea intre salariatul care lucreaza si utilizatorul declarat in cadrul aplicatiei, caruia i s-a acordat un set de drepturi de acces la informatiile din baza de date. Toate tranzactiile efectuate de utilizatori vor fi inregistrate in fisiere speciale;
- Se vor furniza functionalitati de administrare care sa permita oferirea sau revocarea drepturilor de acces, accesul la informatii pe baza de parole.
- Drepturile de acces se vor acorda diferentiat in functie de: modul, operatie, grad de securizare a informatiei, nivel organizational;
- Furnizorul sistemului informatic integrat trebuie sa asiste clientul in realizarea unei politici de securitate a organizatiei;
- Sistemul nu va permite accesul la datele din baza de date decit prin intermediul functiilor incluse in sistemul standard integrat;
- Sistemul va permite administrarea drepturilor pentru grupuri de utilizatori la nivel de module, functii si operatii;
- Sistemul va permite lucrul in paralel cu toate aplicatiile si a mai multor utilizatori simultan in aceeasi aplicatie, chiar in acelasi ecran;
- Sistemul va gestiona si va rezolva probleme de acces concurent la resurse, alegind politica in functie de specificul aplicatiei. Sistemele si bazele de date nu vor permite generarea de inconsistente in date din cauza accesului concurent.

3.9. Confidentialitatea datelor

Accesul la date se va face doar prin intermediul serviciilor oferite de sistemul SIAMC, pe baza drepturilor avute in sistem, accesul direct la datele din bazele de date nefiind permis. De asemenea, accesul va fi reglementat prin politicile de securitate, aferente fiecarui utilizator. Implementarea acestora va trebui sa asigure dezideratele de securitate ale reprezentantilor Inspectiei Muncii si Inspectoratelor Teritoriale de Munca, dar si prevederile legale in ceea ce priveste libertatea cetatenilor si dreptul la viata libera, si procesarea informatiilor cu caracter personal.

4. IMPLEMENTAREA PROIECTULUI

4.1. Management de proiect

Activitatea de management de proiect trebuie sa se desfasoare conform unui cadru (framework) de management de proiect recunoscut international de catre organisme profesionale specifice de Project Management.

Ofertantul trebuie sa prezinte in cadrul propunerii tehnice descrierea detaliata a metodologiei proprii de management de proiect pe care o va utiliza in cadrul proiectului.

Ofertantul trebuie sa prezinte in cadrul propunerii tehnice planul de proiect pentru prestarea serviciilor pe toata durata contractului. Planul de proiect trebuie sa contina toate activitatile precum si etapele/subetapele determinante de realizare a activitatilor, dependentele dintre activitati, jaloanele de proiect (milestones), rezultatele activitatilor si alocarea resurselor in vederea prestarii serviciilor ofertate astfel incat sa fie atinse obiectivele proiectului. Ofertantul trebuie sa propuna planul de proiect cat mai detaliat posibil si sa raspunda cerintelor de etapizare si inscriere in termenele de realizare ale proiectului. In perioada de initiere a proiectului, ulterior semnarii contractului, planul de proiect poate fi modificat doar cu aprobarea Beneficiarului.

Implementarea intregului sistem trebuie sa acopere urmatoarele:

- 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, prestatorul 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.

4.2. 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, Prestatorul 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.

Propunerea tehnica trebuie sa cuprinda urmatoarele:

- Metodologia detaliata pentru derularea activitatilor de analiza in cadrul propriei organizatii;
- Descrierea instrumentelor utilizate in vederea colectarii si evidenta cerintelor, asigurarii trasabilitatii cerintelor pornind de la obiectivele proiectului pana la specificatiile tehnice pentru demonstrarea acoperirii integrale a tematicii proiectului, modelarii proceselor si activitatilor in conformitate cu standarde de modelare si reprezentare recunoscute (UML sau echivalent);
- Prezentarea detaliata a livrabilelor aferente prestarii activitatilor de analiza, care sa includa:
    - Formularul/formularele aferente fiecarui livrabil;
    - Descrierea informatiilor continute de catre fiecare livrabil;
    - Modul de interpretare al continutului fiecarui livrabil.

Analiza se va efectua dupa caz la sediul Beneficiarului sau la Prestator si va avea ca finalitate un pachet de specificatii functionale agreat de comun acord cu acesta.

Serviciile de analiza vor acoperi cel putin urmatoarele aspecte:

- Analiza contextului existent;
- Intelegerea structurii organizatorice a Beneficiarului;
- Analiza situatiei din momentul de fata din cadrul institutiei Beneficiarului prin sedinte de analiza, chestionare etc. Se vor identifica procesele operationale (la nivelul organizatiei) care vor fi impactate prin implementarea solutiei proiectului;
- Identificarea nevoilor si neajunsurilor din cadrul sistemului existent pe care institutia doreste sa le rezolve prin realizarea acestui proiect. Prin aceasta se va avea in vedere intelegerea in detaliu a obiectivelor generale si specifice ale proiectului;
- Definirea cerintelor informationale pentru noul sistem ca urmare a analizei sistemului existent. Se va contura astfel, imaginea viitorului sistem informational prin stabilirea proceselor operationale care sa precizeze parcipantii, momentul interventiei acestora, locatia sau contextul, modalitatea de interventie si informatia procesata. Pentru prezentarea proceselor operationale se vor utiliza instrumente de modelare a proceselor si activitatilor in conformitate cu standarde de modelare si reprezentare recunoscute (UML sau echivalent);

- Stabilirea actorilor de business care vor interactiona in viitorul sistem;
- Se vor evidentia activitatile care urmeaza a fi automatizate daca este cazul, astfel incat sa se identifice clar functiile viitorului sistem informatic si modul in care acesta va ajuta la indeplinirea obiectivelor proiectului.

La realizarea imaginii viitorului sistem, se vor avea in vedere sistemele informatice existente, daca este cazul, care vor conlucra la indeplinirea obiectivelor proiectului, indiferent daca acestea sunt interne sau externe organizatiei Beneficiarului. Se vor avea in vedere volumul si frecventa interactiunilor de integrare intre sisteme.

4.3. 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, Prestatorul va trebui sa execute activitati de proiectare care sa asigure premizele unei implementari eficiente.

Proiectarea sistemului dorit, care va contine detalierea la nivel tehnic a cerintelor si specificatiilor rezultate din activitatea de analiza pentru toate nivelurile si componentele sistemului care va fi realizat:

- Arhitectura de sistem – va prezenta cel putin urmatoarele niveluri: hardware, comunicatii, componente software instalate (sisteme de operare, produse COTS), arhitectura logica cuprinzand descrierea componentelor de sistem, a celor dezvoltate sau personalizate si caracteristicile functionale si non-functionale ale acestora;
- Scenarii (cazuri) de utilizare – din care sa reiasa modul de utilizare a sistemului informatic din perspectiva utilizatorului final, modul in care utilizatorii interactioneaza cu sistemul, in corespondenta directa cu activitatile mentionate in cadrul proceselor operationale ale acestor utilizatori. Scenariile de utilizare trebuie sa cuprinda si interactiunile cu sistemele externe, astfel incat sa fie evidentiat exact modul in care este fructificata o integrare la nivel de sistem informatic. De asemenea, scenariile de utilizare vor fi insotite de o lista a actorilor sistemului si maparea acestora cu actorii de business. Pentru prezentarea cazurilor de utilizare se vor folosi instrumente in conformitate cu standarde de modelare si reprezentare recunoscute (UML sau echivalent);
- Modelul de securitate – la nivel logic (organizarea pe roluri, grupuri, drepturi, pozitia in structura organizatorica etc.) si la nivel fizic (servere, comunicatii, aplicatii etc.);

- Integrarile la nivel de componenta software – pentru fiecare interactiune se va specifica sistemul sursa/destinatie, modalitatea de implementare, canal de comunicare, setul si structura de date transferate, reguli specifice de validare etc.;

Rapoarte ce vor fi realizate in cadrul sistemului – vor fi descrise rapoartele, care sunt informatiile continute, care sunt criteriile de filtrare daca este cazul si tipul de livrare al acestora (timp real, la cererea utilizatorului sau automatizate la un anumit moment de timp programat apriori).

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 Prestatorul 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 solutia 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).

4.4. Dezvoltare, configurare si testare interna

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.

4.5. Implementare (deployment)

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.

4.6. Instruire

Pentru a se asigura o functionare corecta a sistemului, serviciile de instruire vor fi orientate catre urmatoarele categorii de personal:

- administratori de sistem si de baze de date – instruire de specialitate (administrare sistem si baze de date, generare rapoarte etc.);
- utilizatori cheie;
- utilizatori finali – instruire generala aplicatie.

Instruirea administratorilor are in vedere dobandirea cunostintelor necesare, dar fara a se limta la:

a) administrarii utilizatorilor si permisiunilor asociate acestora in cadrul aplicatiei;
b) verificarii realizarii back-upului aplicatiei;
c) consultarii jurnalelor de auditare a accesului si operatiunilor desfasurate in cadrul sistemului.

Instruirea utilizatorilor cheie va avea in vedere familiarizarea cunostintelor mentionate mai jos, dar fara a se limita la:

a) adaugarea/modificarea/stergerea datelor in cadrul sistemului;
b) gestionarea nomenclatoarelor;
c) consultarea rapoartelor specifice;
d) generarea de rapoarte dinamice, altele decat cele predefinite si construite de catre furnizor.

Instruirea utilizatorilor finali are in vedere, dar fara a se limita la:

a) dobandirea cunostintelor necesare utilizarii aplicatiei;
b) consultarea rapoartelor asupra carora au primit drept de acces din partea adminstratorilor de sistem.

Sesiunile de instruire se vor desfasura in limba romana.

Scolarizarea va contine urmatoarele etape si va avea urmatorul cuprins:

Nr.	Descriere	Nr persoane instruite	Nr zile/persoana
1	Scolarizarea administratorilor de sistem si de baze de date	5	12

Nr.	Descriere	Nr persoane instruite	Nr zile/persoana
2	Scolarizarea utilizatorilor cheie	100	6
3	Scolarizarea utilizatorilor sistem	Se va desfasura in serii de maxim 25 cursanti; in total, vor fi 500 de persoane instruite	2

Prezenta la curs

Prezenta la curs va fi evidentiata prin intermediul condicilor de prezenta completate si semnate in fiecare din zilele in care cursantii participa la sesiunile de instruire.

Instructori

Personalul implicat in procesul de scolarizare va fi dupa cum urmeaza:

Nr.	Denumire	Descrierea responsabilitatii
1	Lector	Sustine cursurile Efectueaza certificarea
2	Asistent	Asigura asistenta cursantilor

Atat lectorul cat si asistentul vor fi pregatiti si pusi la dispozitie de catre furnizor.

Materiale folosite

Nr.	Descriere	Suport	
		Imprimat	Alt suport
1	Suport Curs		☐ Suport electronic
2	Prezentare Curs		Power Point Presentation
3	Fisa de prezenta	☐	
4	Chestionar de evaluare	☐	
5	Fisa de examinare	☐	

Evaluarea cursului

Dupa finalizarea fiecarei sesiuni / modul de instruire, participantii vor completa un formular de feedback cu privire la instruirea furnizata in care vor trebui sa evalueze de la “Excelent” la “Foarte Slab” prin marcarea unui “X” in casuta corespunzatoare calificativului ales pentru fiecare dintre urmatoarele aspecte:

1. Evaluarea sesiunii de instruire;
2. Evaluarea instructorului;
3. Evaluarea materialelor de curs folosite.

De asemenea, cursantii vor putea completa comentarii/observatii in cazul in care:

- sunt aspecte din cadrul prezentarilor care ar trebui tratate mai detaliat;

- sunt in cadrul prezentarilor aspecte tratate prea detaliat;
- sunt elemente care ar necesita detalierea intr-o instruire suplimentara dedicata;
- sunt aspecte care ar trebui imbunatatite in organizarea instruirii, materialele de instruire, modalitatea de prezentare a instructorului.

Certificarea utilizatorilor

In vederea certificarii cursantilor, acestia vor fi testati asupra cunostintelor dobandite in cadrul cursului. Testele vor contine atat probe practice, cat si intrebari teoretice. Intrebarile si probele vor fi dimensionate in functie de nivelul de cunostinte pe care fiecare categorie de utilizatori (administratori, utilizatori cheie, utilizatori finali) trebuie sa le detina. Fiecarui utilizator testat si care a facut dovada insusirii cunostintelor, i se va acorda cate o certificare care ii va conferi dreptul de a utiliza sistemul.

Rapoartele de scolarizare

Instruirile vor fi documentate in rapoartele de scolarizare care vor marca incheierea etapei de scolarizare si care vor contine urmatoarele informatii:

1. Lista cursantilor care au participat la sesiunea de instruire;
2. Materialele utilizate in cadrul procesului de scolarizare;
3. Analiza rezultatelor cursului:
    a. Gradul de indeplinire a obiectivelor
    b. Impresia generala a instructorului
    c. Probleme aparute pe timpul scolarizarii
    d. Propuneri de imbunatatire a scolarizarii
4. Evaluarea Cursului (conform Chestionarelor de Evaluare)
    a. Rezultatele evaluarii instruirii
    b. Evaluarea Trainer-ului
    c. Evaluarea Materialelor de Curs.

Documentatia asociata aplicatiei

Documentatia va fi realizata in limba romana.

Furnizorul va prezenta in oferta tehnica lista documentatiilor pe care le va pune la dispozitia beneficiarului, pentru exploatarea si utilizarea sistemului. Toate documentele vor fi in limba romana.

Documente pentru utilizatori

Furnizorul va livra doua copii pe hartie si versiunea electronica a Manualului de utilizare complet, pentru sistem. Acest document va avea urmatoarele caracteristici:

- va cuprinde toate modulele si functiile care pot fi accesate de utilizatori;
- formatul electronic va fi Adobe PDF si Microsoft Word Document;
- va fi revizuit ori de cate ori se lanseaza o versiune noua sau o actualizare punctuala a sistemului si va fi furnizat beneficiarului, fara costuri suplimentare;
- va fi redactat in conformitate cu modulele sistemului, procesele si serviciile acoperite.

Va fi livrata o documentatie de tip Intrebari Frecvente (FAQ), care va cuprinde cele mai importante probleme intampinate de utilizatori, intrebari si solutiile respective. Documentul FAQ va fi accesibil prin Web si va putea fi editat de utilizatori. Drepturile de editare ale utilizatorilor vor fi controlate printr-un mecanism de control al accesului.

Documente pentru administratori

Totodata, vor fi livrate doua copii pe hartie si versiunea electronica a Manualului de administrare. Acest document va avea urmatoarele caracteristici:

- va cuprinde toate operatiunile si functiile de administrare a sistemului;
- formatul electronic sa fie Adobe PDF si Microsoft Word Document;
- va fi revizuit ori de cate ori se lanseaza o versiune noua sau o actualizare punctuala a sistemului si va fi furnizat beneficiarului, fara costuri suplimentare;
- acest manual va cuprinde toate aspectele ciclului de viata al aplicatiei, precum: instalarea, administrarea zilnica, instalarea upgrade-urilor si dezinstalarea / reinstalarea.
- interventii in cazuri de forta majora

Vor fi furnizate copii electronice ale Manualelor de administrare (sau ale documentelor echivalente) pentru toate componentele arhitecturii sistemului (cum ar fi baza de date, e-mail, subsistemul de stocare etc.).

Documente tehnice

Specificatiile tehnice si functionale detaliate si complete ale aplicatiei furnizate vor fi urmatoarele:

- Specificatii detaliate si complete pentru interfetele de interconectare ale sistemului – interoperabilitatea si expunerea de servicii web, care va include cel putin urmatoarele elemente:
    - functiile (intrare, iesire, parametri);

- tipurile de date utilizate;
- contextul de securitate;
- conceptele utilizate.

- Documentatia cu structurile bazelor de date implementate, schema relationala a tabelelor si a legaturilor dintre ele, a celorlalte obiecte din bazele de date, inclusiv modalitatea de acces total la bazele de date.
- Documentatia completa pentru crearea copiilor de rezerva si pentru recuperare. Documentul va include instructiuni pas cu pas pentru procedurile de creare a copiilor de rezerva si de restaurare, necesare pentru asigurarea functionarii corecte a intregii arhitecturi a sistemului.

Pe durata perioadei de scolarizare vor exista o serie de resurse materiale ce vor fi utilizate. Acestea vor fi asigurate de beneficiar:

- Sala pentru desfasurarea cursurilor (in locatia in care se implementeaza proiectul);
- 25 de calculatoare conectate la aplicatia informatica furnizata.

Costurile de deplasare, cazare, diurne si transport pentru cursanti vor fi asigurate de catre Beneficiar.

4.7. Testarea si testele de acceptanta

Ofertantul trebuie sa descrie modalitatea in care va realiza testarea sistemului si testele de acceptanta specifice. Ofertantul trebuie sa prezinte metodologia de testare dupa care se vor realiza activitatile de testare in timpul desfasurarii proiectului. Ofertantul trebuie sa prezinte instrumentele de testare folosite.

Beneficiarul (cu asistenta Prestatorului) va rula toate scenariile pentru testele de acceptanta ale intregului sistem sau componenta livrata. Testele de acceptanta se vor derula in conformitate cu Planul de Teste realizat de Prestator si agreat de Beneficiar, plan ce va fi in concordanta cu intregul ciclu de realizare al proiectului: etape de testare distribuite pe iteratii, seturi de functionalitati sau alte tipuri de teste.

Planul de testare pentru acceptanta va cuprinde toate testele necesare pentru a demonstra acoperirea in intregime a cerintelor din prezentul caiet de sarcini. Astfel, se va avea in vedere faptul ca sistemul functioneaza corect din punct de vedere al respectarii cerintelor, consistentei datelor, al constrangerilor de timp, al validarilor de date si al gestiunii erorilor, inclusiv pentru

functionalitatile existente care au fost extinse sau modificate. Criteriul de succes – sistemul trece toate testele definite in planul de testare agreat impreuna cu Beneficiarul.

O prima varianta a planului de testare va fi prezentata odata cu oferta. Planul detaliat de testare, insotit de scenariile de testare, va fi realizat de catre Prestator si aprobat de Beneficiar inainte de fiecare etapa de testare agreata prin planul de proiect.

Prestatorul va realiza testarea securitatii infrastructurii IT si de comunicatii:

Obiectivele care trebuiesc indeplinite in urma prestarii serviciilor sunt:

a) Evaluarea securitatii fizice;
b) Evaluarea sistemului din punct de vedere al securitatii informatice;
c) Evaluarea protectiei datelor cu caracter personal;
d) Identificarea vulnerabilitatilor specifice sistemului prin teste specifice de penetrare din exteriorul retelei avand in vedere designul, implementarea, utilizarea, mentenanta si dezvoltarea acestuia.

Ofertantul trebuie sa mentioneze metodologiile si tehnicile utilizate in evaluarea vulnerabilitatilor (ca de ex. National Institute of Standards and Technology – NIST, Open Source Security Testing Methodology – OSSTM, Open Information Systems Security Group - OISSG, Information Systems Audit and Control Association – ISACA etc.).

Etape obligatorii pentru desfasurarea serviciilor de evaluare: Pre-evaluare; Evaluare propriu-zisa; Post-evaluare; Urmarire implementare, recomandari.

- **Pre-evaluare**: Reprezinta faza premergatoare actiunii de evaluare propriu-zisa a securitatii informatice; este necesara pentru determinarea specificatiilor precise si a regulilor de desfasurare a evaluarii.
- **Evaluare**: Reprezinta etapa de evaluare a amenintarilor informatice si a vulnerabilitatilor. Trebuie sa contina cel putin urmatoarele activitati:
    - Identificarea si evaluarea riscurilor care pot afecta sistemul;
    - Evaluarea si testarea controlului accesului in sistem;
    - Verificarea si evaluarea fizica a mediului informational;
    - Verificarea si evaluarea securitatii fizice, a procedurilor si a modului de aplicare;
    - Verificarea si evaluarea modalitatii de administrare a sistemului;
    - Testarea integritatii datelor.

Utilizand informatiile descoperite in evaluarea vulnerabilitatilor, trebuie sa se construiasca arbori de atac (attack trees) si trebuie implementate actiunile din aceste structuri.

Aceasta etapa trebuie incheiata cu elaborarea de catre Prestator a unui raport de test. Ofertantul trebuie sa prezinte modul in care va face testarea securitatii infrastructurii IT si de comunicatii cu respectarea cerintelor de mai sus.

- **Post-Evaluare**: Reprezinta etapa de analiza a rezultatelor descoperite in etapa precedenta. Aceste rezultate trebuie sa fie detaliate de catre Prestator intr-un raport care trebuie sa includa recomandari pentru remedierea vulnerabilitatilor descoperite, diminuarii riscurilor identificate etc., in concordanta cu raportul de test din etapa precedenta.
- **Urmarire implementare si recomandari**: Reprezinta etapa de verificare a efectelor concrete privind remedierea vulnerabilitatilor si diminuarea riscurilor. Aceasta etapa trebuie sa aiba loc dupa ce Beneficiarul implementeaza recomandarile/masurile mentionate in raportul de test si in cel realizat de catre Prestator in etapa precedenta.

Livrabile: Prestatorul trebuie sa livreze atat rapoartele din fiecare etapa descrisa, cat si un raport final care trebuie sa contina informatii detaliate despre sistemul testat, vulnerabilitatile identificate, descrierea detaliata a acestora, nivelul de risc calculat dupa metodologia agreata cu Beneficiarul si recomandari de remediere.

In urma etapei Post-Evaluare se va livra un raport suplimentar in care se va mentiona gradul de reducere / inlaturare a riscurilor identificate.

4.8. Asistenta tehnica si suport

Furnizorul va asigura asistenta tehnica si suport pe tot parcursul dezvoltarii si pe timpul perioadei de garantie. Pe aceeasi perioada va asigura serviciile de actualizare si corectie. Asistenta va fi disponibila in toate zilele calendaristice, fara intrerupere (24x7) printr-un sistem de inregistrare a problemelor prin web si prin telefon, utilizand linii de apel dedicate fiecarei categorii de utilizatori.

Solutionarea problemelor (reactia initiala a furnizorului) va incepe dupa raportarea erorii, conform urmatorului tabel de gravitate:

Nivel de gravitate	**Descriere**	**Reactie initiala a Furnizorului (ore)**	**Timp de solutionare a problemei (ore)**

1	Eroare de sistem critica, sistemul nu este functional.	1	8
2	Unele functii sau componente ale sistemului nu sunt functionale.	1	24
3	Unele functii sunt limitate, dar operationale.	1	72
4	Probleme minore, sistemul este operational.	4	72

In cazul in care sunt disponibile componente de upgrade pentru software (corectii, actualizari si versiuni noi) pentru sistem, furnizorul va mentiona in mod explicit daca actualizarile respective sunt compatibile cu aplicatia. Se considera ca upgrade-urile de software ale sistemului fac parte din garantie si trebuie sa satisfaca cerintele legate de garantie. Aceste declaratii vor fi furnizate in termen de 2 saptamani dupa ce responsabilul cu asistenta tehnica formuleaza interogarea pentru corectii si de 4 saptamani pentru versiunile de upgrade (majore si minore, cunoscute si ca „actualizari punctuale").

In cazul echipamentelor, serviciile de garantie includ constatarea defectiunii si remedierea ei in termenele stabilite in procedura de garantie. Remedierea se va face la sediul/sediile beneficiarului, iar in cazul unor defecte mai grave echipamentele vor fi transportate de catre furnizor la sediul acestuia. In urma remedierii, furnizorul va reinstala echipamentele la sediul / sediile beneficiarului. In cazul defectiunilor majore ale echipamentelor care necesita o durata de depanare mai mare de timp, furnizorul va asigura echipament echivalent pentru desfasurarea in continuare a activitatii beneficiarului, respectand cerintele de disponibilitate a sistemului.

In perioada de garantie, service-ul echipamentelor va fi asigurat de furnizor prin unitati de service, persoane juridice autorizate.

In cazul componentelor software, serviciile de garantie includ constatarea defectelor si remedierea lor in termenele stabilite in procedura de garantie. Remedierea defectelor se va realiza cu respectarea termenelor privind severitatea lor.

Pe toata perioada de garantie, furnizorul va asigura asistenta tehnica de specialitate pe mai multe directii: preluarea incidentelor, asigurarea bunei exploatari prin furnizarea informatiilor necesare utilizatorilor finali ai aplicatiei, asistenta pentru instalarea si configurarea la nivel local a aplicatiilor acolo unde este cazul.

Serviciile de garantie oferite includ, de asemenea:

- Inregistrarea incidentelor raportate de catre utilizatorii sistemului, precum si transmiterea confirmarii solutionarii incidentului semnalat, in urma rezolvarii acestuia; este vorba atat despre incidentele care apar la nivelul aplicatiilor, cat si despre incidentele care afecteaza bazele de date ale sistemului;
- Rezolvarea incidentelor datorate lipsei cunostintelor de utilizare a modulelor / aplicatiilor din cadrul sistemului. Se va realiza o analiza preliminara a incidentelor si solutionarea pe loc a tipurilor de incidente care nu necesita escaladare;
- Transmiterea de rapoarte privind rezolvarea incidentelor la cererea beneficiarului;
- Informarea utilizatorilor cu privire la actualizarile aplicatiei.

Inregistrarea si urmarirea evenimentelor se va face folosind o aplicatie software corespunzatoare. Aceasta trebuie sa indeplineasca urmatoarele cerinte:

- Inregistrarea solicitarilor si alocarea unui identificator unic fiecarei solicitari;
- Posibilitatea de definire a unor categorii de solicitari si de incadrare a solicitarilor in aceste categorii;
- Posibilitatea de inregistrare a datelor de identificare ale solicitantului – include atribuirea incidentului unei persoane care raporteaza in aplicatia software de inregistrare si urmarire a evenimentelor, persoana care solutioneaza incidentul (de la orice nivel), persoana care a raportat un incident;
- Posibilitatea de inregistrare a descrierii problemei si de atasare a unor documente suplimentare. Aplicatia software permite atasarea oricaror tipuri de fisiere (doc, xls, jpg, xml etc.) precum si postarea directa a unor capturi de ecran din aplicatii;
- Posibilitatea de alocare a unui criteriu de urgenta. Aplicatia software permite clasificarea incidentelor in functie de tipul stabilit in SLA (Service Level Agreement), putand sa emita notificari pe mail privind alocarea incidentelor catre persoanele implicate in incident;
- Posibilitatea de alocare a unor coduri de incident care sa indice cauza probabila a incidentului. Aplicatia software aloca coduri unice fiecarui incident, fie ca el este unul cunoscut sau unul nou. Permite de asemenea si gruparea pe module a incidentelor;
- Posibilitatea de modificare a acestui cod de incident, in cazul in care cauza reala a acestuia nu a fost cea intuita la inceput. Aplicatia software permite modificarea oricarei stari a incidentului odata ce inregistrarea a fost validata;

- Disponibilitatea unei baze de date cu personalul de suport caruia i se pot aloca spre rezolvare incidentele. Aplicatia software contine implicit datele de contact ale persoanelor care pot fi considerate alocabile sau care pot aloca un incident;
- Inregistrarea automata a datei si a orei primirii unei solicitari de asistenta;
- Posibilitatea de definire a criteriilor de calitate si performanta (SLA) pentru rezolvarea diferitelor categorii de solicitari de asistenta;
- Posibilitatea de atentionare automata in momentul depasirii unor praguri temporale de rezolvare a diferitelor categorii de solicitari de asistenta;
- 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;
- Posibilitatea de escaladare a cererilor de suport;
- 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 pentru care nu s-au respectat criteriile din SLA;
- Permite in orice moment accesul direct la baza de date a personalului autorizat pentru verificarea modului de tratare a incidentelor si pentru rularea de rapoarte de performanta a serviciilor de garantie oferite. Accesul se va face numai pentru citire si nu va fi conditionat in niciun fel de operatorii sau administratorii serviciului.

5. LIVRAREA SI RECEPTIA LIVRABILELOR

Ofertantul va livra echipamentele, va realiza instalarea si configurarea acestora, precum si instalarea si configurarea sistemelor de operare, a software-ului de baza si a pachetelor de aplicatii.

Termenele de livrare si receptie a echipamentelor vor respecta perioadele/termenele prezentate in Diagrama Gantt prezentata de ofertant si acceptata de beneficiar.

Receptia intregului sistem va fi efectuata de catre reprezentantii beneficiarului si se va face dupa instalarea, configurarea si verificarea functionarii tuturor componentelor sistemului la parametrii minimali solicitati in Caietul de Sarcini.

6. DURATA DE EXECUTIE A PROIECTULUI

Durata de implementare a proiectului este de 7 luni.

7. GARANTIE

Pe o perioada de cinci ani de la acceptarea sistemului (dupa etapa de implementare), va fi asigurata garantia pentru componentele software ale sistemului dezvoltate in cadrul proiectului, cat si pentru cele provenite de la terti cu care furnizorul are incheiat un subcontract.

Pentru echipamentele hardware de calcul si stocare se va asigura o garantie de 3 ani din momentul in care va fi semnata acceptanta pentru acestea de catre beneficiar. Pentru echipamentele de comunicatii se va asigura o garantie de 1 an din momentul in care va fi semnata acceptanta pentru acestea de catre beneficiar.

Serviciile de intretinere corectiva vor fi compuse din:

- rezolvarea bug-urilor care nu au fost identificate in timpul implementarii si care apar in faza de productie;
- intretinerea si buna functionare a sistemului furnizat in parametrii agreati (functional, performanta, disponibilitate, integritatea datelor);
- instalarea de noi versiuni ale aplicatiilor in urma efectuarii corectiilor;
- actualizarea manualelor de utilizare si a altor documente rezultate in urma efectuarii corectiilor;
- toate incidentele vor fi gestionate prin intermediul aplicatiei software de gestionare a tichetelor.

8. MENTENANTA SI SUSTENABILITATE

Pe o perioada de cinci ani de la acceptarea sistemului (dupa etapa de implementare), va fi asigurata mentenanta pentru componentele software ale sistemului dezvoltate in cadrul proiectului cat si pentru cele provenite de la terti cu care furnizorul are incheiat un subcontract.
In acest scop, se vor achizitiona separat servicii de intretinere evolutiva pentru acest proiect.
Serviciile de intretinere evolutiva sunt similare serviciilor care vor fi prestate in perioada de implementare a proiectului, vor lua in considerare adaptarea sistemului la eventualele modificari legislative si de proces si vor consta in:

- Analiza (inclusiv Analiza proceselor);
- Proiectare;
- Dezvoltare, configurare si testare interna;
- Implementare (deployment);
- Testarea si testele de acceptanta;
- Punere in productie;
- Asigurarea si controlul calitatii pe durata contractului.

Componentele software vor fi verificate periodic de catre furnizor, utilizand functiuni disponibile ale sistemului de operare. La finalizarea verificarilor se va furniza un raport continand rezultatele verificarii si actiunile recomandate pentru a imbunatati disponibilitatea sistemului. Furnizorul va adopta o atitudine pro-activa in derularea activitatilor de garantie a sistemului informatic. In acest sens, furnizorul va desfasura urmatoarele activitati:

- Oferirea de asistenta in administrarea implementarii schimbarilor, ajutand la minimizarea riscurilor aferente si la evitarea intreruperilor potentiale ale activitatii;
- Evaluarea mediului informatic folosind instrumente specifice de diagnosticare, cel putin o data pe an. O serie de teste de diagnosticare vor fi efectuate pentru compararea mediului informatic al beneficiarului cu metodele acceptate de administrare a sistemelor informatice. In urma verificarilor, se va furniza un raport care detaliaza rezultatele obtinute, evidentiaza elementele care necesita rezolvare sau investigatii si recomanda actiunile ce trebuie urmate;

- Anual, furnizorul va realiza o evaluare a nivelului de disponibilitate al echipamentului de stocare a datelor. Evaluarea include o analiza detaliata a mediului fizic, configuratia echipamentului si versiunile sale de firmware si software. Dupa terminarea evaluarii, va furniza beneficiarului un raport si un rezumat de prezentare a rezultatelor si a recomandarilor pentru imbunatatirea disponibilitatii sistemului.
- Pentru software si firmware, furnizorul va monitoriza toate actualizarile pe masura ce apar. Daca se identifica o problema critica aplicabila mediului aflat in garantie, furnizorul va notifica beneficiarul si va analiza situatia impreuna cu acesta.

Pe masura aparitiei de actualizari pentru produsele software aflate in garantie, ultimele revizii software si documentatia aferenta vor fi puse la dispozitia beneficiarului in cel mai scurt timp.

9. PREZENTAREA PROPUNERII TEHNICE

Toate cerintele din prezentul caiet de sarcini, sunt minime si obligatorii, iar nerespectarea uneia dintre cerinte va duce automat la declararea ofertei ca fiind neconforma.

Pentru toate cerintele expuse in prezentul caiet de sarcini ofertantul trebuie sa raspunda explicit, precizand modalitatea in care solutia propusa ofera functionalitatea solicitata insotite de referinte la documentatia producatorului sau capturi de ecran elocvente la functionalitatea ceruta care sa demonstreze indeplinirea cerintei. Raspunsurile simple de tipul „Solutia raspunde la cerinta" sau simpla conversie a cerintei in raspuns nu sunt acceptate si se va considera ca oferta nu raspunde cerintelor minime obligatorii.

Nu vor fi acceptate oferte partiale ci doar oferte complete, care satisfac toate cerintele prezentei documentatii.

Propunerea tehnica se va prezenta si redacta in limba romana, astfel incat sa fie posibila maparea cu usurinta a corespondentei cu specificatiile minime din Caietul de sarcini.

Propunerea tehnica trebuie sa includa o sectiune cu arhitectura sistemului propus. In aceasta sectiune ofertantul va cuprinde arhitectura detaliata a sistemului propus (software si hardware, dispunerea produselor COTS si a modulelor software personalizate pe masinile virtuale, daca este cazul, si pe echipamentele hardware, descrierea componentelor propuse). Atat arhitectura software cat si arhitectura hardware va trebui sa cuprinda toate produsele propuse de ofertant, in caz contrar oferta va fi declarata neconforma. Totodata ofertantul va trebui sa detalieze si lista licentelor propuse in oferta tehnica, specificand in clar numele licentei de la producator, editia, producatorul, cantitatea si unitatile de licentiere specifice producatorului (de exemplu „User" sau „Processor Core") precum si corelarea acestora cu cerintele caietului de sarcini. Lista licentelor trebuie sa cuprinda toate licentele propuse de ofertant, in caz contrar oferta va fi declarata neconforma.

In functie de solutia propusa, daca platforma este formata din mai multe sub-componente atunci fiecare sub-componenta trebuie licentiata astfel incat sa permita rularea pe minimul de nuclee de procesare solicitate in cadrul fiecarui capitol si pentru numarul de utilizatori precizat.

Tot in cadrul acestei sectiuni ofertantul va trebui sa prezinte lista echipamentelor hardware specificand in clar identificatorul unic producator (part-number) asociat fiecarui echipament, numarul de echipamente ofertate pentru fiecare tip de echipament, configuratia acestora, precum

si corelarea acestora cu cerintele din caietul de sarcini. Nu se accepta echipamente scoase din fabricatie (End of life – EOL). Se accepta livrarea doar de echipamente noi.

Propunerea tehnica trebuie sa includa o sectiune cu comentariu punct cu punct la cerintele caietului de sarcini. Aceasta sectiune va cuprinde un comentariu, articol cu articol privind toate specificatiile continute in caietul de sarcini, prin intermediul carora ofertantul va demonstra corespondenta propunerii tehnice cu prevederile caietului de sarcini. Nu este acceptata o simpla confirmare a indeplinirii cerintei fara o detaliere a modului de indeplinire. Este important ca in cazul in care, in raspunsul punct cu punct, se face referire la alte documente, sa se indice in clar referinta, identificand precis locul din document care demonstreaza indeplinirea cerintei.

Toate documentele referite care sunt parte a ofertei vor fi nominalizate individual in cuprinsul ofertei precizand numarul paginii la care poate fi regasit.

Ofertantul va include specificatiile tehnice ale tuturor produselor software/echipamentelor hardware, consumabilelor de proces si, dupa caz, ale instalatiilor/utilajelor tehnice prevazute in oferta, sub forma de fise tehnice din care sa rezulte indeplinirea cerintelor functionale precizate in caietul de sarcini, respectiv documentele oficiale care provin de la producatori si/sau rapoartele de incercari/testari emise de laboratoare de incercare sau organisme de certificare si inspectie, din cadrul carora sa rezulte modul de indeplinire a parametrilor solicitati, precum si conditiile de vanzare, garantie si punere in functiune a acestora.

Pentru verificarea indeplinirii de catre solutiile ofertantilor a cerintelor minime solicitate in documentatia de atribuire, Beneficiarul isi rezerva dreptul de a solicita in etapa de evaluare a ofertelor depuse sustinerea unei sesiuni demonstrative. Ofertantii au obligatia ca, in cazul desfasurarii unei astfel de sesiuni, sa utilizeze propriile echipamente si produse software pentru a proba indeplinirea cerintelor. Sesiunile demonstrative vor avea loc la sediul Autoritatii Contractante in termen de 10 zile lucratoare de la data emiterii solicitarii de catre aceasta, detaliile despre componentele care fac obiectul acestei sesiuni fiind puse la dispozitia Ofertantilor in cadrul solicitarii transmise.

Cerintele prezentului capitol se completeaza cu cerintele stabilite la Cap. IV.4.1. – *"Modul de prezentare a propunerii tehnice",* Cap. IV.4.2. – *"Modul de prezentare a propunerii financiare"* si Cap. IV.4.3 – *"Modul de prezentare a ofertei"* enuntate in cadrul fisei de date a achizitiei aferenta documentatiei de atribuire.

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 se considera minimale si sunt insotite de mentiunea „sau echivalent”.

ANEXA 1

In vederea furnizarii tuturor informatiilor necesare cu privire la acest contract, autoritatea contractanta prezinta, in tabelul de mai jos, bugetul aprobat al proiectului.

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
1	Cheltuieli pentru achizitionarea de servere, calculatoare tip desktop / portabile, monitoare, echipamente de retea, dispozitive pentru conectare, echipamente periferice etc., justificate din punct de vedere a implementarii proiectului	Platforma de procesare date [include 1 sasiu blade, 14 servere blade, accesorii]	647.112,00
2	Cheltuieli pentru achizitionarea de servere, calculatoare tip desktop / portabile, monitoare, echipamente de retea, dispozitive pentru conectare, echipamente periferice etc., justificate din punct de vedere a implementarii proiectului	Sistem de stocare a datelor [include echipament stocare centralizata, infrastructura gazduire echipamente si racire, infrastructura de alimentare UPS)	493.560,00
3	Cheltuieli pentru achizitionarea de servere, calculatoare tip desktop / portabile, monitoare, echipamente de retea, dispozitive pentru conectare, echipamente periferice etc., justificate din punct de vedere a implementarii proiectului	Token-uri	297.050,00

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
4	Cheltuieli pentru achizitionarea de servere, calculatoare tip desktop / portabile, monitoare, echipamente de retea, dispozitive pentru conectare, echipamente periferice etc., justificate din punct de vedere a implementarii proiectului	Certificate calificate	308.475,00
5	Cheltuieli pentru achizitionarea de servere, calculatoare tip desktop / portabile, monitoare, echipamente de retea, dispozitive pentru conectare, echipamente periferice etc., justificate din punct de vedere a implementarii proiectului	Terminale mobile	2.193.600,00
6	Cheltuieli pentru achizitionarea de servere, calculatoare tip desktop / portabile, monitoare, echipamente de retea, dispozitive pentru conectare, echipamente periferice etc., justificate din punct de vedere a implementarii proiectului	Platforma comunicatii (include firewall nivel transport 2 bucati, firewall nivel aplicatie 2 bucati, appliance analiza loguri 1 buc, appliance management echipamente 1 buc, licenta management echipamente mobile, appliance de transformare)	541.720,49
7	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma monitorizare infrastructura HW	287.910,00

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
8	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma backup si restaurare	284.711,00
9	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Antivirus servere si terminale	95.970,00
10	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma fluxuri	981.711,68
11	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma baza de date	1.017.335,75
12	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma Raportare si BI	547.131,37
13	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Licente server GIS si optiuni GIS	862.244,38

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
14	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma transformare date	615.753,11
15	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma portal si colaborare	652.596,00
16	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Licente sisteme de operare (14 servere si terminale)	521.635,34
17	Cheltuieli pentru achizitionarea aplicatiilor software/licentelor necesare implementarii proiectului, inclusiv solutii de securitate software	Platforma de certificate digitale	383.880,00
18	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Configurare platforma portal&colaborare, sectiunea portal	1.344.265,50

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
19	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Configurare platforma portal&colaborare, sectiunea colaborare	1.373.330,70
20	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Dezvoltare modul gestiune sesizari on-line	1.318.833,45
21	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Configurare Raportare si BI	1.438.727,40
22	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Dezvoltare modul control preventiv	1.376.963,85

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
23	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Dezvoltare modul consemnare control	1.333.366,05
24	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Dezvoltare modul gestiune teren	1.431.461,10
25	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Dezvoltare modul gestiune centralizata acidente	1.409.662,20
26	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Configurare modul transformare	1.416.928,50

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
27	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Configurare platforma fluxuri	1.424.194,80
28	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Configurare platforma certificate digitale	1.380.597,00
29	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Project management furnizor SIAMC	142.419,48
30	Cheltuieli legate de formarea profesionala a personalului care va asigura mentenanta solutiei daca acesta este angajat al beneficiarului	Servicii instruire administratori	29.065,00
31	Cheltuieli legate de formarea profesionala a personalului care va asigura mentenanta solutiei daca acesta este angajat al beneficiarului	Servicii de instruire utilizatori cheie	72.663,00

Nr. crt.	Activitate	Cheltuiala	Buget proiect exclusiv TVA (LEI)
32	Cheltuieli legate de formarea profesionala a personalului care va asigura mentenanta solutiei daca acesta este angajat al beneficiarului	Servicii de instruire utilizatori standard	145.326,00
33	Cheltuieli pentru achizitionarea de aplicatii informatice (pentru realizarea carora poate fi necesara parcurgerea urmatoarelor etape: analiza cerintelor, proiectare, implementare si testare);	Servicii de consultanta pentru analiza institutionala	1.140.215,20
TOTAL			**27.510.415,35**

AVIZAT,

Coordonator de proiect

Daniel Cornel MITRAN