CUPRINS

CUVANT INAINTE

Prezentul document reprezinta totalitatea informatiilor necesare intocmirii Ofertei cu privire la implementarea Sistemului tip Portal de Aplicare VIZA – denumit in continuare e-VIZA pentru Romania. Acest Sistem va fi in primul rand un serviciu public via internet ce-i va sprijini pe doritori la intocmirea dosarului de aplicare in vederea obtinerii vizei pentru Romania, si, totodata, va reprezenta o interfata cu actualul sistem de vize al Romaniei – SNIV, facilitand aplicantilor operatiunile specifice de pre-aplicare si post-aplicare viza.

1. INFORMATII GENERALE

1.1 DESCRIEREA SITUATIEI ACTUALE

Dupa aderarea la Uniunea Europeana la 1 ianuarie 2007 ca membru deplin, Romania a intrat intr-o noua etapa, care presupune elaborarea si adoptarea unor masuri necesare pentru eliminarea controalelor la punctele de frontiera interne, in vederea aderarii ulterioare la spatiul Schengen.
Astfel, Sectiunea 4 a Conventiei de Aplicare a Acordului Schengen prevede obligatia de a implementa un sistem informatic centralizat privind vizele numit VIS (Sistemul Informatic privind Vizele), care trebuie sustinut prin copii la nivel national, pentru o eficienta sporita. Sistemele nationale trebuie sa permita centralizarea cererilor de viza pentru spatiul Schengen si procesarea rapida si eficienta a acestora, cu urmatoarele scopuri: prevenirea amenintarilor asupra sigurantei interne a fiecaruia dintre statele membre UE, prevenirea cazurilor de nerespectare a criteriilor privind determinarea statului membru responsabil de examinare a cererii, facilitarea luptei impotriva fraudelor, facilitarea controalelor la frontierele externe ale Uniunii Europene si cele dintre Statele Membre, facilitarea identificarii persoanelor care nu indeplinesc sau nu mai indeplinesc cerintele pentru a intra, tranzita sau locui pe teritoriul statelor membre care au eliminat controlul la frontierele interne, inclusiv pentru reintoarcerea acestora.
Crearea Sistemului Informatic National privind Vizele (SNIV), precum si conectarea acestuia la sistemul VIS central (C.VIS) sunt necesare pentru accederea ulterioara la spatiul Schengen.
Aceasta este una dintre masurile cele mai importante pentru facilitarea controlului la frontierele externe ale UE si pe teritoriul statelor membre, in cadrul luptei impotriva infractionalitatii transfrontaliere.
Pana la data aderarii Romaniei la Conventia de aplicare a Acordului Schengen, sistemul SNIV va permite autoritatilor competente accesul la cererile de viza, prin intermediul unei proceduri de cautare automata, pentru indeplinirea atributiilor specifice controlului la frontiera, respectarea regimului vamilor, emiterea vizelor si permiselor de sedere, precum si alte controale si activitati specifice realizate de Politie sau de alte autoritati, in vederea asigurarii ordinii si sigurantei publice.
La data aderarii Romaniei la Conventia de Aplicare a Acordului Schengen (CISA), sistemul SNIV va furniza date Sistemului Informatic Central European C.VIS privind Vizele , conform reglementarilor europene in domeniu.
Sistemul SNIV va contine toate cererile de viza Schengen primite de autoritatile romane si va furniza informatii bazei de date a Oficiului Roman pentru Imigrari (ORI). Sistemul va fi pus la dispozitia institutiilor interesate pentru a fi consultat si / sau actualizat, conform competentelor legale stabilite in conformitate cu CISA.

1.2 COORDONATE GENERALE ALE PROIECTULUI

1.2.1 CADRUL GENERAL

1.2.1.1 DESCRIEREA GENERALA

Sistemul E-Viza va fi in esenta un serviciu electronic pus la dispozitia aplicantilor in vederea obtinerii vizei pentru Romania prin intermediul internetului, care ii va ajuta si asista in procesul de constituire a dosarului de

aplicare. Acest proiect vizeaza atat cresterea gradului de satisfactie in randul publicului aplicant prin oferirea posibilitatii de a-si constitui dosarul de aplicare pentru viza de acasa sau dintr-o alta locatie dotata cu conexiune la internet, cat si eficientizarea muncii angajatilor serviciilor consulare romane prin faptul ca o parte din dosarele aplicantilor se pot constitui fara implicarea lor directa.
Acest Portal de aplicare nu vizeaza gestionarea efectiva a cererilor de viza pentru Romania, care este responsabilitatea actualului sistem de acordare a vizelor pentru Romania - SNIV, ci va juca doar rolul de interfata electronica intre SNIV si utilizatorii aplicanti in cadrul Portalului. Astfel, aplicarea prin intermediul Portalului Aplicare VIZA comporta doua faze, si anume:

- Pre-aplicare: Este principala faza a aplicarii, pe parcursul careia aplicantul se informeaza asupra procesului de acordare a vizei si isi construieste dosarul de aplicare. Acest dosar contine o parte din informatiile necesare angajatilor serviciilor consulare romane pentru acordarea vizei, care, ulterior, vor fi transmise catre sistemul SNIV.
- Post-aplicare: Este faza in care aplicantul este instiintat de decizia cererii acordarii vizei pentru Romania, decizie care se ia in sistemul SNIV, si, in cazul in care aceasta este favorabila, aplicantul va mai putea beneficia si de alte informatii necesare.

Prin implementarea acestui Portal sunt asteptate urmatoarele beneficii, grupate pe cele doua tipuri mari de utilizatori:

- Utilizatorii aplicanti:
  - Reducerea timpului total necesar aplicarii pentru viza;
  - Aplicare comoda si eficienta in orice moment de acasa, de la birou sau de la orice alta locatie dotata cu un computer si conexiune la internet;
  - Posibilitatea de a continua o sesiune de constituire a dosarului de aplicare, daca aceasta a fost intrerupta;
  - Acces facil la informatiile de suport in domeniu, cum ar fi cele legislative sau procedurale;
  - Reducerea numarului de deplasari la sediile serviciilor consulare romanesti;
  - Posibilitatea de programare online a intilnirilor de la sediile consulatelor romanesti;
  - Posibilitatea de a primi confirmarea ca documentele necesare obtinerii vizei sunt sau nu conforme cu legislatia in domeniu, pe baza incarcarii in Portal a unor copii electronice ale acestora;
  - Increderea ca, atunci cand se va prezenta la ghiseul consulatului, aplicantul a furnizat pe parcursul fazei de pre-aplicare toate informatiile necesare;
  - Posibilitatea de consultare a legislatiei si procedurilor de lucru in domeniu prin intermediul echipamentelor tip info-kiosk instalate in sediile serviciilor consulare romane.
- Angajatii serviciilor consulare romane:
  - Foarte inalta calitate a datelor dintr-un dosar de aplicare, deoarece majoritatea acestora vor fi introduse chiar de aplicant;
  - Importanta economie de timp deoarece, in cazul datelor introduse de aplicant, nu va mai fi nevoie de introducerea manuala a acestora in sistemul actual de vize, SNIV;
  - Reducerea pana la eliminare a comunicarii prin intermediul postei;
  - Reducerea timpului de lucru dedicat unui dosar prin posibilitatea efectuarii unor verificari in regim automatizat sau partiale;
  - O mai mare flexibilitate in procesul de acordare a vizei, prin introducerea posibilitatii de creare electronica a dosarului de aplicare, pe langa modalitatea folosita in prezent;
  - Eficientizarea procesului de acordare a vizei prin posibilitatea de monitorizare centralizata a dosarelor electronice in vederea aplicarii;
  - Sprijinirea procesului decizional in domeniul acordarii vizelor prin posibilitatea furnizarii unor indicatori pe baza unui sistem de audit si raportare;
  - O mai buna trasabilitate pe perioada constituirii dosarelor aplicantilor;
  - Facilitate de tip „self-service” cu ajutorul careia angajatii serviciilor consulare romane pot efectua diverse operatiuni de administrare a contului in Portal sau solicitari catre utilizatorii cu rol de management in domeniu;
  - Reducerea substantiala a numarului de aplicanti prezenti in salile de asteptare ale serviciilor consulare romane;

1.2.1.2 Zona geografica a proiectului

Echipamentele hardware centrale tip server vor fi localizate in Romania, la Bucuresti. Componentele hardware pentru posturile consulare ale Romaniei vor fi localizate la posturile respective din intreaga lume. Singura autoritate romana implicata in implementarea proiectului e-VIZA este Ministerul Afacerilor Externe (MAE).

1.2.2 Obiective

1.2.2.1 Obiectivul general

Obiectivul general al contractului consta in imbunatatirea sistemului de procesare a cererilor de viza pentru Romania prin crearea unui nou serviciu electronic deschis publicului aplicant.

1.2.2.2 Obiectivele specifice

Obiectivele proiectului sunt urmatoarele:

- Fluidizarea si rapidizarea procedurii acordarii de viza pentru Romania;
- Cresterea gradului de satisfacere a publicului aplicant pentru vize (prin introducerea posibilitatii ca multe din operatiunile care se efectueaza in prezent doar in cadrul posturilor consulare romanesti sa se poata efectua de acasa sau din alta locatie unde exista un calculator si o legatura la internet);
- Eficientizarea muncii angajatilor posturilor consulare romane.

1.2.3 Rezultate asteptate

Realizarea proiectului E-Viza consta in principal in implementarea unei componente de Portal care sa faciliteze procedurile de pre-aplicare si post-aplicare ale doritorilor de viza pentru Romania. Implementarea proiectului va avea ca rezultat urmatoarele componente cheie:

- Portalul intern si extern de pre-aplicare si post-aplicare in vederea obtinerii vizei pentru Romania, ca produs principal al acestui proiect;
- O infrastructura software de componente de suport care va permite operarea celor doua Portale rapid si securizat in retea intr-un mediu cu multi utilizatori concurenti;
- Infrastructura hardware completa pentru locatiile centrale (compusa in principal din servere, echipamente de stocare, echipamente de retea si echipamente de criptografie);
- Echipamente de infrastructura hardware pentru posturile consulare (posturile de lucru interne, scanere de birou flatbed, terminale de informare, switch-uri layer 2 etc).

1.2.4 Premize

Limba oficiala a proiectului va fi limba romana.
Sistemul e-VIZA va utiliza o parte din infrastructura de comunicatie a MAE si a serviciilor consulare romane, mai precis i se va pune la dispozitie pentru comunicare latimea de banda necesara pe o linie principala si pe o linie de rezerva. Ofertantii vor calcula argumentand riguros necesarul de latime de banda pentru buna functionare a sistemului si o vor comunica in cadrul ofertei.
Se vor utiliza in scopul prezentului proiect anumite echipamente hardware de retelistica, comunicare si criptare aflate in uz la Beneficiar (ex.: elementele de agregare tip switch Layer 1 din fiecare locatie – Layer 1).

1.2.5 Activitati in cadrul proiectului

In conformitate cu rezultatele asteptate din implementarea prezentului proiect se doreste ca ofertantii sa includa in solutiile propuse urmatoarele activitati:
Implementarea Portalului e-Viza, extern si intern, de pre-aplicare, respectiv post-aplicare, cu toate componentele acestuia.

Ofertantul castigator va crea si implementa Portalul intern si extern de pre-aplicare si post-aplicare e-Viza – componenta centrala a arhitecturii software a prezentului proiect, ca interfata electronica intre sistemul SNIV si aplicantii doritori sa foloseasca un serviciu electronic alternativ in vederea crearii dosarului de aplicare pentru viza. Ofertantul castigator va fi responsabil de conceptia, proiectarea si dezvoltarea Portalului precum si de serviciile de garantie si suport pe toata perioada de sustenabilitate a proiectului. Portalul va trebui sa fie conceput intr-o maniera care sa permita ulterior scalabilitatea acestuia, atat pe orizontala, prin adaugarea de module si functionalitati noi, cat si pe verticala, pentru a face fata unei eventuale cresteri a puterii de procesare. Se vor prevedea facilitati de functionare off-line acolo unde este posibil.

Implementarea componentelor software de suport necesare bunei functionari a Portalului Aplicare e-VIZA

Ofertantul castigator va furniza restul componentelor software (COTS si dezvoltate la cerere), necesare functionarii optime si securizate a Portalului, tinand cont ca acesta va fi deschis via internet publicului aplicant si ca va trebui sa sustina lucrul a sute (sau chiar mii) de utilizatori concurenti. Cerintele pentru aceste componente software vor reiesi din capitolele urmatoare si vor include fara a se limita la urmatoarele elemente: platforma de Portal , platforme de virtualizare, sistemul de baze de date, platforme de management, sisteme de securitate, platforma de mesagerie, etc. Toate aceste componente software, care trebuie sa respecte cerintele tehnice detaliale in urmatoarele sectiuni ale prezentului document vor fi furnizate, instalate si configurate de catre Ofertantul castigator pentru buna functionare a Portalului intern si extern de pre-aplicare si post-aplicare VIZA.

Infrastructura hardware pentru locatiile centrale

Ofertantul castigator va trebui sa furnizeze arhitectura completa centrala pentru Portalul intern si extern de pre-aplicare si post-aplicare VIZA (incluzand fara a se limita la servere, servere de stocare, echipamente de retelistica, dispozitive de securitate, dispozitive externe de stocare, etc.) pentru echiparea camerei server de la locatia centrala, locatie ce va fi indicata de catre Beneficiar Ofertantului castigator.

Infrastructura hardware pentru locatiile serviciilor consulare romane

Ofertantul castigator va trebui sa furnizeze componentele hardware pentru locatiile serviciilor consulare romane Aceste componente hardware trebuie livrate de Ofertantul castigator conform detaliilor tehnice din urmatoarele sectiuni ale prezentului document.

Alte tipuri de activitati

Ofertantul castigator va livra serviciile de garantie si de suport tehnic aferent pentru intreaga arhitectura a sistemului.

In plus, sunt solicitate urmatoarele activitati:

- Cursuri pentru administratori si utilizatori;
- Documentatia tehnica si de folosinta pentru toate componentele sistemului;
- Gestionarea proiectului;
- Asigurarea calitatii.

1.2.6 GESTIONAREA PROIECTULUI

Ofertantii vor avea in vedere ca, desi cerintele si caracteristicile minime ale componentelor sunt detaliate in capitolele urmatoare, aceste cerinte nu sunt limitative, fiind necesare dezvoltarea si detalierea lor in cadrul ofertei.

Ofertantul castigator va avea responsabilitatea implementarii unei solutii complete si integrate care sa indeplineasca in totalitate cerintele exprimate in prezentul document.

Ofertantul castigator este responsabil de executarea la timp a tuturor activitatilor ce se vor presta in cadrul proiectului si de obtinerea rezultatelor stabilite in prezentul document.

Ofertantul castigator va indeplini toate cerintele acestui contract in conformitate cu si prin implementarea bunelor practici din domeniu.

Ofertantul va respecta Ordinele administrative emise de Managerul de proiect al Autoritatii contractante. Aceste ordine administrative vor fi emise in conformitate cu cererile / aprobarile primite de la Autoritatea Competenta si de la Beneficiar (conform Conditiilor generale ale contractului). Ofertantul va furniza tuturor partilor implicate in acest proiect (Autoritatea Competenta, Autoritatea de Contractare si Plata) toate informatiile legate de proiect.

Ofertantul are obligatia de a propune angajarea unor experti calificati in vederea indeplinirii activitatilor stipulate in prezentul document. Ofertantul este responsabil de activitatea expertilor si de obtinerea rezultatelor solicitate la timp.

Facilitati oferite Ofertantului castigator:

Autoritatea Contractanta va oferi Ofertantului castigator toate facilitatile de comunicare ce se impun conform prevederilor legale in vigoare, precum si toate informatiile si / sau documentele necesare pentru o implementare eficienta si asigurarea succesului proiectului. Autoritatea Contractanta va putea oferi temporar un spatiu de birouri pentru expertii proprii si cei ai Ofertantul castigator, dar acesta din urma trebuie sa aiba posibilitatea de a folosi si alte birouri proprii sau declarate in Bucuresti.

1.2.7 Logistica si planificarea proiectului

1.2.7.1 Locatia pentru livrare

Exista multiple locatii pentru livrare, conform Anexa 1 – Lista locatiilor. Adresele locatiilor vor fi comunicate de MAE ofertantului castigator in faza de analiza a proiectului.

- Locatia centrala pentru echipamentele server va fi situata in Bucuresti. Toate componentele tip server vor fi livrate la acesta locatie.
- Echipamentele pentru posturile consulare romane vor fi livrate in prima etapa la o locatie din Bucuresti desemnata de MAE. Echipamentele vor fi configurate si verificate la aceasta locatie de catre personalul Ofertantului castigator si vor fi verificate de catre personalul competent al MAE. Dupa aceasta etapa echipamentele vor fi livrate la posturile consulare prin curier comercial, conditie de livrare DDP la locatia finala, cu toate taxele achitate, costurile fiind suportate de catre Ofertantul castigator.
- Echipamentele vor fi instalate la posturile consulare de catre o echipa formata din personal al MAE. La aceste locatii se va face acceptanta provizorie a echipamentelor distribuite la posturile consulare. Costurile de transport, cazare si diurna pentru intreaga echipa vor fi suportate de catre Ofertantul castigator. Locatiile posturilor consulare sunt listate in Anexa 1 – Lista locatiilor.
- Toate componentele software ale sistemului (aplicatia principala) vor fi livrate si instalate in locatiile centrala din Bucuresti.

1.2.7.2 Locatia unitatii de management a proiectului

Sediul operational pentru acest proiect se va afla intr-una una din locatiile MAE din Bucuresti si va fi comunicata Ofertantului castigator in faza de analiza a proiectului.

2. Cerinte tehnice

2.1 Cerinte generale

Pe baza obiectivelor specifice si a descrierii activitatilor din cadrul proiectului se evidentiaza urmatoarele cerinte generale privind implementarea sistemului e-VIZA:

2.1.1 Cerinte generale cu implicatii in zona de servicii livrate in cadrul proiectului

- Livrarea, instalarea si configurarea tuturor echipamentelor hardware de suport in cadrul proiectului la locatia (sau locatiile) indicate de Beneficiar;
- Proiectarea si implementarea unui sistem informatic web based de tip Portal – e-VIZA (extern - expus petentilor si intern expus personalului consular, portale separate clar din punct de vedere al conexiunii, interactiunea intre ele facandu-se prin exportul unor fisire xml, in mod controlat si unidirectional), ce va servi ca serviciu alternativ privind crearea dosarelor in vederea solicitarii vizelor Schengen pentru Romania;

- Instalarea si configurarea tuturor componentelor software de suport pentru proiect (ex.: sisteme de operare, sisteme de baze de date, sisteme de securitate, etc.);
- Interfatarea sistemului informatic E-Viza cu alte sisteme informatice sau componente software utilizate de Beneficiar (sistemul national de vize, sistemul de ticketing, sistemul de plata cu cardul), si care se vor identifica in faza de analiza a proiectului;
- Definirea si implementarea unor proceduri si fluxuri de lucru privind activitatile de lucru din cadrul portalului, atat cele specifice de business, cat si activitatile de monitorizare a infrastructurii hardware-software si a activitatii, administrare, securitate, etc.;
- Definirea si implementarea unor proceduri si fluxuri de lucru privind activitatile financiare din cadrul portalului, integrarea cu echipamentele POS de plata cu cardul, precum si facilitati de raportare privind activitatile financiare;
- Definirea si implementarea unui sistem de raportare coerent constituit atat din rapoarte de lucru utilizator, cat si din rapoarte de analiza pentru suport decizional sau rapoarte de monitorizare a activitatii in cadrul portalului e-VIZA;
- Nevoile de raportare ale Beneficiarului sunt de :
    - minim 30 de rapoarte pentru utilizatorii interni finali referitor la dosarele de pre si post-aplicare,
    - minim 10 rapoarte de date agregate (tip Business Intelligence) pentru utilizatorii interni cu rol de analiza si decizie privind diversi indicatori aferenti dosarelor de pre si post-aplicare, care se vor defini in etapa de analiza a proiectului ;
    - minim 10 rapoarte pentru utilizatorii interni cu rol de conducere privind activitatea in cadrul sistemului e-VIZA a utilizatorilor interni finali.

2.1.2 CERINTE GENERALE PE COMPONENTELE SOFTWARE TIP SERVER DIN PROIECT

Ca urmare a cerintelor de business si dupa identificarea componentelor software tip server din proiect, se evidentiaza urmatoarele cerinte generale per componenta:

Sistem de Operare pentru echipamentele tip server:
- Sa ofere suport pentru instalarea in configuratii cluster tip “high-availability” ;
- Sa ofere suport pentru tehnologia de “virtualizare”;
- Sa ofere mecanisme avansate pentru administrare, monitorizare, diagnosticare si recuperare in cazul incidentelor software;
- Sa includa mecanisme avansate pentru controlul accesului utilizatorilor la resurse.

Platforma de virtualizare tip server:
- Sa fie compatibila cu toti producatorii hardware recunoscuti;
- Sa ofere suport pentru multiple sisteme de operare;
- Sa ofere suport pentru adaugarea de resurse de procesare si memorie fara restartarea sistemului de operare din masina virtuala;
- Reteaua virtuala sa poata sa fie unificata la nivelul intregii infrastructuri virtuale, indiferent de numarul de servere ce fac parte din aceasta infrastructura.

Sistem Antivirus:
- Protectie completa (antivirus, antispyware si antirootkit) pentru sistemul de fisiere;
- Scanare in tip real, optimizata;
- Actualizarea zilnica a bibliotectii de semnaturi de virusi;
- O consola de administrare centralizata pentru toate modulele/componentele solutiei de antivirus.

Platforma de Gestiune a Bazelor de Date:
- Sa fie sistem de gestiune a bazelor de date de tip relational;
- Sa ofere suport pentru lucrul cu comenzi tip SQL, proceduri stocate, indexi, triggeri si sa permita efectuarea de tranzactii autonome;
- Sa ofere suport pentru salvarea/restaurarea precum si arhivarea/dezarhivarea datelor in regim de lucru online;
- Sa ofere suport pentru definirea de multiple niveluri de autorizare asupra datelor din baza de date.

Platforma de Portal extern:

- Solutia va constitui singura modalitate de acces la informatii prin intermediul unui portal la care vor avea acces utilizatori externi (aplicantii).
- Solutia trebuie sa fie capabila sa gestioneze volume mari de date.
- Solutia trebuie sa se bazeze pe un sistem de gestiune al bazelor de date relationale, un server pentru gestiunea bazelor de date mari in conditii de siguranta si care permite un control riguros al accesului la diferite tipuri de informatii.
- Aplicatiile trebuie sa fie dezvoltate in tehnologie internet (web). Nu se vor agrea solutii de tip Client-Server sau distribuite pe statii de lucru, accesul utilizatorilor trebuie sa se faca prin intermediul unui browser.
- Administrarea sistemului si a bazei de date trebuie sa posede instrumente puternice pentru asigurarea protectiei si confidentialitatii datelor, bazate pe un sistem consistent de profile si autorizatii de acces.
- Solutia trebuie sa ofere posibilitatea unei dezvoltari graduale prin punerea la dispozitia utilizatorilor de noi servicii.
- Utilizatorul va avea acces la aplicatie printr-un simplu browser web fara a fi nevoit sa instaleze alte aplicatii.
- Solutia va oferi mecanisme avansate de autentificare a utilizatorilor si securizare a informatiilor.
- Solutia va fi dimensionata din punct de vedere software si hardware astfel incat sa asigure functionalitatile necesare utilizatorilor descrisi.
- Sistemul va avea un sistem de securitate care permite protejarea informatiei, atat fata de accesul neautorizat intern, cat si fata de accesul neautorizat extern. Protectia va fi asigurata atat la nivel hardware cat si software.
- Utilizatorii (aplicantii) vor avea acces numai la aplicatie.
- Sistemul va fi proiectat si implementat din punct de vedere al securitatii pe baza legilor, regulamentelor si instructiunilor in vigoare privind securitatea, confidentialitatea si protectia datelor cu caracter personal.
- Vor fi asigurate mecanisme de securitate implementate pe mai multe niveluri, la nivel de aplicatie si la nivel de baza de date si se vor permite autentificarea, identificarea, verificarea drepturilor si permisiunilor, supravegherea cererilor de servicii si operatiilor executate de persoana care a generat, a modificat sau a sters o informatie.
- Accesul la pagina de Portal se va face printr-un navigator de Web de tip Internet Explorer, Mozilla Firefox, Crome sau Netscape;

Platforma de Portal intern:

- Solutia va constitui singura modalitate de acces la informatii prin intermediul unui portal la care vor avea acces utilizatori interni (lucratorii consulari).
- Solutia trebuie sa fie capabila sa gestioneze volume mari de date.
- Solutia trebuie sa se bazeze pe un sistem de gestiune al bazelor de date relationale, un server pentru gestiunea bazelor de date mari in conditii de siguranta si care permite un control riguros al accesului la diferite tipuri de informatii.
- Aplicatiile trebuie sa fie dezvoltate in tehnologie internet (web). Nu se vor agrea solutii de tip Client-Server sau distribuite pe statii de lucru, accesul utilizatorilor trebuie sa se faca prin intermediul unui browser.
- Administrarea sistemului si a bazei de date trebuie sa posede instrumente puternice pentru asigurarea protectiei si confidentialitatii datelor, bazate pe un sistem consistent de profile si autorizatii de acces.
- Solutia trebuie sa ofere posibilitatea unei dezvoltari graduale prin punerea la dispozitia utilizatorilor de noi servicii.
- Utilizatorul va avea acces la aplicatie printr-un simplu browser web fara a fi nevoit sa instaleze alte aplicatii.
- Solutia va oferi mecanisme avansate de autentificare a utilizatorilor si securizare a informatiilor.
- Solutia va fi dimensionata din punct de vedere software si hardware astfel incat sa asigure functionalitatile necesare utilizatorilor descrisi.

- Sistemul va avea un sistem de securitate care permite protejarea informatiei, atat fata de accesul neautorizat intern, cat si fata de accesul neautorizat extern. Protectia va fi asigurata atat la nivel hardware cat si software.
- Utilizatorii vor avea acces numai la aplicatie.
- Sistemul va fi proiectat si implementat din punct de vedere al securitatii pe baza legilor, regulamentelor si instructiunilor in vigoare privind securitatea, confidentialitatea si protectia datelor cu caracter personal.
- Vor fi asigurate mecanisme de securitate implementate pe mai multe niveluri, la nivel de aplicatie si la nivel de baza de date si se vor permite autentificarea, identificarea, verificarea drepturilor si permisiunilor, supravegherea cererilor de servicii si operatiilor executate de persoana care a generat, a modificat sau a sters o informatie.
- Accesul la pagina de Portal se va face printr-un navigator de Web de tip Internet Explorer, Mozilla Firefox, Crome sau Netscape;

Cataloage de identitate:

- Posibilitati de autentificare multi nivel combinand diverse metode de autentificare disponibile ;
- Sa se permita stocarea politicilor de acces si a configuratiei de sistem intr-un sistem de tip director;
- Sa se permita rularea de fluxuri pentru inregistrarea utilizatorilor, recuperarea si resetarea parolei, precum si inregistrarea in grupuri;
- Sa se ofere un mod flexibil si unitar privind gestiunea drepturilor si politicilor de acces ale utilizatorilor la toate resursele sistemului integrat (aplicatii, module, categorii de informatie) prin definire, modificare, stergere, explorare, pastrare istoric sesiuni de acces.

Platforma de management si investigatie centralizata a evenimentelor de securitate IT

- Sa se realizeze managementul evenimentelor de securitate IT in scopul cresterii nivelului de securitate si asigurarii unui raspuns eficient la atacuri asupra infrastructurii si componentelor sistemului oferit;
- Nu se vor include echipamentele hardware;
- Vor fi furnizate toate componentele software (aplicatii, module, agenti, software de management) pentru a fi asigurata integrarea aplicatiilor de colectare, analiza, corelare a log-urilor de securitate, alertare si investigare specifica IT.
- Sa se asigure fiabilitate in sensul asigurarii mecanismelor functionarii neintrerupte pentru componentele sale critice;
- Sa se asigure managementul evenimentelor provenite de la diverse platforme hardware si software: echipamente tip firewall, sisteme de detectie / prevenire a intruziunilor (IDS / IPS), echipamente de comunicatii, aplicatii, sisteme de management al accesului, log-uri ale sistemelor de operare, log-uri ale bazelor de date si ale sistemelor de audit, alte echipamente electronice generatoare de log-uri.

Platforma de mesagerie:

- Solutia trebuie sa ofere utilizatorilor experienta comunicatiilor unificate si integrate, sa gaseasca persoanele potrivite ca sa comunice cu acestea, in orice moment, din aplicatiile pe care le utilizeaza cel mai frecvent. Fara o infrastructura costisitoare si fara upgrade-uri ale retelei, sa se poata beneficia de comunicatii optimizate, inclusiv comunicatii VoIP bazate pe software, conferinte Web, prezenta avansata si mesagerie instantanee, pastrand controlul operational necesar.
- Sa ofere integrare nativa cu Active Directory
- Solutia sa fie independenta din punct de vedere platforma hardware si sa suporte virtualizare.

Platforma de recunoastere a semnaturii olografe:

- Sa tina cont in procesul de recunoastere a semnaturilor de aspectul grafic si de caracteristicile acceleratiile gestului utilizatorului cand semneaza.
- Respingerea incercarilor de frauda prin imitarea semnaturii corecte a unui utilizator (adica respingerea accesului la semnalarea semnaturilor false).

2.2 CERINTE FUNCTIONALE

Sistemul e-Viza va reprezenta un serviciu public alternativ la actuala modalitate de creare a dosarului in vederea solicitarii vizei Schengen pentru Romania. Acest Sistem va fi accesibil via online atat de catre publicul aplicant cat si de catre angajatii posturile consulare romane, facilitand crearea dosarelor aplicantilor chiar de acestia, cu sprijinul, la nevoie, al angajatilor serviciilor consulare.
e-Viza va avea rol de interfata cu actualul sistem de gestiune a vizelor Schengen pentru Romania – SNIV, asigurand utilizatorilor aplicanti servicii de pre-aplicare in vederea obtinerii vizei si de post-aplicare dupa decizia care este responsabilitatea sistemului SNIV. Totodata, sistemul va avea si o puternica componenta de raportare in sprijinul personalului MAE pentru obtinerea a diverse informatii utile vizand procesele de pre si post aplicare.

Principalele facilitati care trebuie sa fie oferite de catre Portalul e-Viza sunt:

- Pentru utilizatorii aplicanti:
  - Informare privind legislatia in domeniu si procedurile de rigoare privind constituirea dosarului de pre-aplicare in vederea obtinerii vizei;
  - Pregatirea dosarului de pre-aplicare pentru viza:
    - Selectare a serviciului consular cu care aplicantul va colabora in vederea obtinerii vizei;
    - Ghid;
    - Aplicare pentru un tip de viza din cele disponibile.
  - Planificare a intilnirilor la sediul serviciului consular cu unul din angajatii acestuia;
  - Calcul privind taxele aferente emiterii vizei;

Pentru angajatii serviciilor consulare romane:

- Suport acordat utilizatorilor in constituirea dosarului de pre-aplicare in vederea obtinerii vizei (posibilitati de vizualizare si adaugare/modificare a datelor – daca e cazul);
- Finalizarea electronica a cererii de viza,
- Raportare privind activitatea dosarelor de pre-aplicare ale utilizatorilor;
- Eficientizarea intalnirilor cu utilizatorii la sediul serviciului consular;
- Calculul taxelor ce trebuiesc platite de aplicant
- Raportarea directa si imediata in cadrul apllicatiei a partii financiare
- Integrarea aplicatiei cu sistemul de plata POS la ghiseu

Pentru administratorii sistemului informatic E-Viza:

- Facilitati avansate de monitorizare a infrastructurii hardware-software a sistemului E-Viza;
- Facilitati administrative privind salvarea si restaurarea datelor;
- Facilitati centralizate si avansate de securitate puse la dispozitie prin intermediul infrastructurii complexe de securitate;
- Posibilitati de audit specific IT privind activitatea in cadrul portalului E-Viza.

Conform specificului activitatii Beneficiarului, procesele si functiile principale pe baza carora ar trebui sa se consituie dosarele de pre-aplicare sunt urmatoarele:

- Emiterea vizelor Schengen la Posturile consulare;
- Emiterea vizelor la frontiera;
- Prelungirea valabilitatii vizelor Schengen;
- Anularea, revocarea si reducerea duratei de valabilitate a vizei uniforme;
- Verificarea vizelor la frontiera;
- Procesele de consultare a informatiei din domeniu;
- Colectarea datelor pentru emiterea vizelor nationale pentru sedere de lunga durata.

Beneficiarul isi rezerva dreptul de a modifica aceasta lista cu procese si functii principale in cadrul etapei de analiza a proiectului, astfel ca sistemul E-Viza sa sprijine cat mai eficient colectarea tuturor datelor necesare si

exportul acestora catre sistemul SNIV, raportarea acestor date, raportarea statistica aferenta, precum si raportarea financiara aferenta operatiunilor efectuate in portal.

2.3 CERINTE PRIVIND COMPONENTELE SOFTWARE

2.3.1 COMPONENTE SOFTWARE TIP SERVER

2.3.1.1 SISTEME DE OPERARE

Sistemele de operare ce se va instala pe echipamentele hardware tip server trebuie sa indeplineasca urmatoarele cerinte:

- Sa ofere suport pentru minim 2 socketuri procesor;
- Sa ofere suport pentru urmatoarele tipuri de procesoare:
  - x86;
  - x86-64;
  - Itanium.
- Sa ofere suport pentru tehnologia 64-bit;
- Sa ofere suport pentru urmatoarele tipuri de conectivitate cu echipamentele de stocare :
  - NAS;
  - SATA;
  - SAS;
  - SCS;
  - FC;
  - FcoE;
  - iSCSI.
- Sa permita instalarea in configuratii cluster tip “high-availability” ;
- Sa ofere suport pentru tehnologia de “virtualizare” (virtualizarea nodurilor de procesare, vezi cap 2.3.1.2 – “Platforma de virtualizare tip server”);
- Sa ofere o interfata unica pentru configurarea si monitorizarea serverului;
- Sa ofere o componenta shell cu linie de comanda si limbaj de script;
- Sa ofere instrumente de diagnosticare asupra mediului serverului, fizic si virtual;
- Sa permita administrarea serverului de la locatii de la distanta;
- Sa permita instalari in configuratie minimala;
- Sa includa mecanisme de “backup” a datelor.

Se vor oferi licentele de utilizare a sistemelor de operare dimensionate dupa necesitati, dar nu mai putin de 20 de instante virtualizate care sa ruleze distribuite pe serverele fizice.

2.3.1.2 SOLUTIA DE VIRTUALIZARE TIP SERVER

Platforma de virtualizare tip server trebuie sa indeplineasca urmatoarele cerinte specifice:

- Platforma de virtualizare trebuie sa fie bazata pe Hypervizor propriu, fara dependenta de un sistem de operare anume.
- Hypervizorul sa fie independent de metoda de stocare interna/externa a serverului/serverelor pe care ruleaza.
- Platforma de virtualizare sa fie compatibila si recunoscuta de toti producatorii hardware recunoscuti:
  - IBM,
  - Dell,
  - HP,
  - Sun,
  - Intel.
- Administrarea platformei virtuale sa se poata face atat prin consola locala / la distanta cat si prin browser web si prin platforma de management dedicata.

- Sa aiba suport pentru urmatoarele sisteme de operare :
    - Windows XP/Vista/7/2003/2008/2008 R2,
    - Linux Suse/Red Hat/CentOS,
    - FreeBSD,
    - Solaris,
    - Netware.
- Sa se poata adauga cu usurinta spatiu de stocare pentru masinile virtuale prin folosirea a cel putin urmatoarelor protocoale :
    - NAS – NFS/CIFS ;
    - SAN – iSCSI/FCP.
- Sa se poata adauga cu usurinta spatiu de stocare pentru masinile virtuale prin folosirea a cel putin urmatoarelor sisteme de fisiere :
    - FAT32,
    - NTFS,
    - EXT2,
    - EXT3.
- Componentele platformei hardware virtuale prezentate sistemelor de operare din masina virtuala sa poata fi modificate cu usurinta (adaugare/eliminare).
- Sa suporte adaugarea de resurse de procesare si memorie fara repornirea sistemului de operare din masina virtuala.
- Hypervizorul si platforma de management a infrastructurii virtuale sa fie de la acelasi producator.
- Platforma de virtualizare sa permita independent sau prin conectori/componente proprietare/terte virtualizarea componentelor de procesare, retea si stocare.
- Sa permita configurarea retelei virtuale prin integrarea directa cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea.
- Reteaua virtuala a platformei sa fie unificata la nivelul intregii infrastructuri virtuale, indiferent de numarul de servere ce fac parte din aceasta infrastructura.
- Reteaua virtuala sa fie configurabila la nivelul intregii infrastructuri virtuale si nu prin configurarea individuala a fiecarui server in parte.
- Sa permita agregarea conexiunilor fizice de retea precum si distribuirea incarcarii pe aceste conexiuni indiferent de producatorul serverelor si/sau placilor de retea folosite.
- Sa ofere redundanta la nivelul conexiunilor de retea fizice/virtuale indiferent de producatorul serverelor si/sau placilor de retea folosite.
- Sa permita configurarea spatiului de stocare virtual prin integrarea directa cu platforma de stocare aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de stocare.
- Sa permita extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri, daca sistemul de operare permite aceasta operatiune.
- Sa permita balansarea dinamica automata/manuala a resurselor de procesare existente in platforma virtuala in functie de necesitati si/sau pe baza unor reguli/politici prestabilite.
- Sa permita distribuirea dinamica si/sau manuala a masinilor virtuale in functie de gradul de ocuparea a resurselor de procesare.
- Sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati.
- Platforma de virtualizare sa permita izolarea acestor grupari de resurse dar in acelasi timp sa fie suficient de flexibila incat sa se poata mari cantitatea de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari.
- Sa permita crearea de politici dinamice de acces la resursele de procesare, precum si de disponibilitate ale acestora.
- Pentru administrarea platformei de virtualizare sa permita autentificarea utilizatorilor prin intermediul unui sistem de tip director (LDAP, Kerberos sau similar) sau local.
- Sa permita separarea privilegiilor administrative in functie de roluri predefinite sau roluri configurabile manual.
- Separarea privilegiilor administrative sa se poata face pe orice element disponibil in interfata de administrare (server, utilizator, resursa de procesare, stocare, retea, etc).
- Sa permita crearea de zone/domenii de securitate in functie de aplicatii si/sau roluri functionale, nu numai in functie de server/servere.

- Separarea zonelor de securitate si a rolurilor administrative sa se faca integrat din platforma de management a infrastructurii virtuale.
- Din platforma de management sa se poata defini si aplica profile de configuratie standard pentru serverele ce fac parte din infrastructura virtuala. De asemenea sa permita configurarea de politici de aplicare a acestor profile in functie de necesitatile de moment sau in concordanta cu politica stabilita in prealabil.
- Sa permita integrarea prin intermediul unor conectori/componente cu platforma de stocare in vederea realizarii backup-ului direct din platforma de stocare.
- Sa asigure concomitent suport de pana la 8 procesoare logice si maxim 256 GB ram pentru oricare masinila virtuala, daca sistemul de operare din masina virtuala poate adresa aceasta cantitate de resurse de procesare.
- Sa permita mutarea masinilor virtuale de pe un server pe altul sau dintr-un datacenter in altul fara oprirea sistemului de operare ce ruleaza in masina virtuala si fara intreruperea serviciului oferit de aplicatia/aplicatiile din masina virtuala.
- Sa permita mutarea intregului harddisk virtual concomitent pentru oricare masina virtuala in cadrul aceluiasi datacenter sau intre datacenter-e diferite, independent de platforma de stocare folosita si de mecanismele de replicare ale acesteia.
- Sa permita extinderea automata a harddisk-urilor virtuale pe masura ce sistemul de operare si aplicatiile din masinile virtuale o cer.
- Sa permita in mod automat, prin politice predefinite, consolidarea masinilor virtuale pe un numar prestabilit de servere si sa opreasca automat serverele fara activitate sau cu subutilizare a resurselor de procesare.
- Crearea rapida a unor zone izolate atat din punct de vedere al securitatii cat si al gruparilor de resurse de procesare, stocare si retea, in scopul testarii si dezvoltarii.

Se vor oferi licentele de utilizare a platformei de virtualizare tip server pentru toate procesoarele fizice si logice oferite (a se vedea cerintele privind echipamentele hardware din capitolul 2.4.1.1 – „Platforme de procesare tip server”).

2.3.1.3 SISTEMUL ANTIVIRUS

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

Sistemul antivirus trebuie sa indeplineasca urmatoarele cerinte tehnice:

- Sa ofere protectie antivirus, antispyware si antirootkit pentru fluxul de fisiere la nivelul sistemului de operare;
- Sa ofere protectie euristica proactiva impotriva pericolelor informatice pe durata “ferestrei de vulnerabilitate”;
- Sa permita optimizarea scanarii pentru accesarea mai rapida a fisierelor;
- Sa permita scanare pe multiple fire de executie pentru reducerea timpului necesar acestui proces;
- Sa permita scanarea la acces si la cerere pentru protectia completa a serverului de fisiere;
- Sa ofere compatibilitate cu consola de administrare centralizata care reduce eforturile de administrare;
- Sa ofere compatibilitate cu arhitectura pe 64 de biti;
- Sa permita scanarea si marcarea fisierele “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 ofere posibilitatea de programare a scanarilor antivirus la cerere si a actualizarii bibliotecilor de semnaturi;
- Sa alerteze utilizatorii in privinta scanarilor efectuate precum si a actualizarilor prin intermediul unui modul de alerte;
- Sa pemita scanarea in timp real a fiecarui fisier accesat sau copiat fara a afecta functionarea serverului de fisiere ;
- Sa permita programarea de scanari antivirus la cerere sau realizarea unor scanari imediate pentru un plus de siguranta a serverului de fisiere;

- Sa ofere o capacitate sporita de administrare si acces rapid la majoritatea setarilor prin intermediul unei interfete tip MMC, usor de folosit si intuitiva ;
- Sa permita afisarea informatiilor legate de cele mai importante evenimente si sa ofere un buton de remediere directa intr-o pagina de garda tip dashboard ;
- Sa ofere rapoarte legate de activitatea produsului prin intermediul sistemului de monitorizare si a unui modul de statistici ;
- Sa dispuna de alerte adaptabile pentru diferite tipuri de evenimente, cum ar fi:
    - actualizari de semnaturi antivirus,
    - actualizari de produs,
    - scanari la cerere,
    - detectari de virusi;
- Sa ofere posibilitatea administrarii centralizate a tuturor modulelor/aplicatiilor din cadrul solutiei de Antivirus si sa se permita ca prin intermediul unei consolei de management a serverului sa se poata:
    - accesa setarile de configurare ale modulelor/aplicatiilor solutiei antivirus;
    - obtine informatii legate de evenimente esentiale, cum ar fi: avertismentele legate de configurare, anunturile legate de expirarea licentei ;
    - genera statistici usor de interpretat si rapoarte bazate pe informatiile primite de la module/aplicatii din cadrul solutiei de antivirus.

Se vor oferi licentele de utilizare a sistemului antivirus pentru toate platformele de procesare tip server si client din cadrul ofertei .

2.3.1.4 PLATFORMA DE GESTIUNE A BAZELOR DE DATE

Solutia trebuie sa fie o solutie comerciala independenta de sistemul dezvoltat (COTS) si trebuie sa ofere un suport implicit scalabil, disponibil si sigur pentru baze de date relationale, incluzand instrumente integrate de raportare si analiza, business intelligence, consolidare / integrare de date si Data Mining.
De asemenea sistemul trebuie sa includa o platforma care sa permita procesarea complexa a evenimentelor, consistenta a datelor in medii heterogene, facilitati avansate pentru dezvoltare si servicii proprii de Business Intelligence (self-service BI). Solutia trebuie sa ofere urmatoarele functionalitati:

- Raportare consolidata si managementul depozitelor de date:
    - Depozit de date relational si instrumente OLAP: sistemul sa ofere solutii OLAP si data warehouse; data warehouse sa permita lucru in mod partitionat pentru incarcarea rapida si mentenanta usoara a tabelelor foarte mari
    - ETL (Extract, transformation, load): functionalitati native de extragere a datelor din diferite surse de date (Oracle, SQL Server, Excel, Web services), realizarea de filtrari, agregari si diferite alte transformari asupra datelor si in final stocarea datelor in data warehouse.
    - Baze de date multidimensionale native: stocarea datelor intr-un cub cu mai multe dimensiuni, in vederea interogarii mai usoare a datelor si construirii rapoartelor relevante.
    - Posibilitatea de utilizare a serviciilor de raportare pentru vizualizarea datelor.
    - Extragerea si editarea dinamica a rapoartelor utilizand instrumente familiare de tip Office (i.e. Excel) si interfete noi intuitive si productive care includ harti, sparklines si indicatori.
- 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 proiectarea bazelor de date atat relationale cat si multidimensionale, pentru proiectarea 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
    - Sa ofere posibilitatea administrarii entitatilor de date si ierarhiilor din multiple baze de date cu posibilitatea versionarii
    - Administrarea datelor master (vizualizare, editare, audit, si aprobare de date) din interfata web

- Performante ridicate ale sistemului de baze de date:
  - 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: auditarea trebuie sa includa informatii despre momentul in care au fost citite datele, in plus fata de orice modificare a datelor. Produsul trebuie sa ofere caracteristici precum configurarea imbunatatita si managementul auditurilor in server. Produsul sa defineasca specificatiile de audit in fiecare baza de date, astfel incat configuratia auditului sa poata fi adaptata pentru diversele bazele de date.
  - Posibilitatea adaugarii online a resurselor de memorie la masinile fizice sau virtuale care gazduiesc bazele de date, pentru scalarea la cerere a acestora.
  - Colectarea datelor de performanta: 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
  - Comprimarea backup-urilor: mentinerea online a backup-urilor pe disc este o operatie scumpa si laborioasa, astfel incat este necesara implementarea unei solutii de comprimare 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. Sistemul trebuie sa ofere stabilitate si predictibilitate asupra performantelor de interogare,
  - Asigurarea continuitatii activitatii: duplicarea datelor prin tehnologii de tip data replication and integration
- Implementarea structurilor de date complexe:
  - 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.
  - Posibilitatea crearii de tabele cu mai mult de 500 de coloane.
  - 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).
- Utilizarea unei platforme avansate pentru dezvoltarea de aplicatii complexe de procesare a evenimentelor (CEP):
  - Posibilitatea de dezvoltarea de aplicatii bazate pe evenimente folosind platforma de procesare a evenimentelor pentru a se permite interogari continue si latenta de milisecunde.
  - Posibilitatea de dezvoltare de aplicatii cu posibilitatea de extragere, analiza si corelare a datelor permitand monitorizarea si managementul datelor in timp real.
- Sistemul trebuie sa ofere mecanisme pentru:
  - Definirea si managementul politicilor de configurare a sistemului
  - Monitorizarea si prevenirea modificarilor asupra sistemului prin crearea de politici impotriva configurarii

- Detectarea problemelor de conformitate cu politicile direct din interfata de administrare a server-ului
- Posibilitati de virtualizare pentru a creste flexibilitatea prin consolidare si virtualizare

2.3.1.5 PORTAL EXTERN

2.3.1.5.1 CERINTE GENERALE

Solutia propusa in prezentul proiect trebuie sa indeplineasca urmatoarele cerinte tehnice generale:

- Solutia va oferi suport pentru urmatoarele limbi: romana, engleza, franceza, germana, spaniola, rusa, italiana, chineza, araba, portugheza, limbile vor putea fi interschimbabile prin intermediul unui switch; Continutul specific in fiecare dintre limbile enumerate mai sus va fi pus la dispozitie si avizat de catre Beneficiar.
- Solutia va constitui singura modalitate de acces la informatii prin intermediul unui portal la care vor avea acces utilizatori externi (aplicantii).
- Solutia trebuie sa se integreze cu diverse surse interne de informatii existente in cadrul organizatiei.
- Sa fie capabila sa se integreze cu sisteme diferite de back-office provenite de la producatori diferiti sau dezvoltate intern.
- Solutia trebuie sa fie capabila sa gestioneze volume mari de date.
- Solutia trebuie sa se bazeze pe un sistem de gestiune al bazelor de date relationale, un server pentru gestiunea bazelor de date mari in conditii de siguranta si care permite un control riguros al accesului la diferite tipuri de informatii.
- Aplicatiile trebuie sa fie dezvoltate in tehnologie internet (web). Nu se vor agrea solutii de tip Client-Server sau distribuite pe statii de lucru, accesul utilizatorilor trebuie sa se faca prin intermediul unui browser.
- Administrarea sistemului si a bazei de date trebuie sa posede instrumente puternice pentru asigurarea protectiei si confidentialitatii datelor, bazate pe un sistem consistent de profile si autorizatii de acces.
- Documentatia completa de utilizare si administrare va fi livrata cu produsul.
- Procesul de implementare trebuie sa se desfasoare in conformitate cu o metodologie verificata, care sa asigure controlul fazelor, activitatilor, atributiilor, planificarea in timp, alocarea resurselor, continutul si rezultatul etapelor, confirmarea rezultatelor si documentarea procesului de implementare.
- Solutia trebuie sa ofere posibilitatea unei dezvoltari graduale prin punerea la dispozitia utilizatorilor de noi servicii.
- Solutia trebuie sa ofere o interfata prietenoasa si usor de folosit, consistenta din punct de vedere al design-ului in toate punctele de contact si sa ofere instrumente de navigare intuitive.
- Utilizatorul va avea acces la aplicatie printr-un simplu browser web fara a fi nevoit sa instaleze alte aplicatii.
- Solutia va oferi mecanisme avansate de autentificare a utilizatorilor si securizare a informatiilor.
- Solutia va fi dimensionata din punct de vedere software si hardware astfel incat sa asigure functionalitatile necesare utilizatorilor descrisi.
- Infrastructura hardware trebuie complet licentiata din punct de vedere licente software pentru toate produsele care vor rula pe infrastructura respectiva.

2.3.1.5.2 CERINTE DE SECURITATE PORTAL EXTERN

Portalul extern va indeplini urmatoarele cerinte de securitate:

- Sistemul va avea un sistem de securitate care permite protejarea informatiei, atat fata de accesul neautorizat intern, cat si fata de accesul neautorizat extern. Protectia va fi asigurata atat la nivel hardware cat si software.
- In acest sens, sistemul va indeplini anumite cerinte din punct de vedere al securitatii, cum ar fi autentificarea unica a utilizatorilor interni (administratori) si autorizarea acestora in sistem prin mecanisme de tip autentificare unica prin intermediul rolurilor si privilegiilor.
- Utilizatorii (aplicantii) vor avea acces numai la aplicatie.

- Sistemul va fi proiectat si implementat din punct de vedere al securitatii pe baza legilor, regulamentelor si instructiunilor in vigoare privind securitatea, confidentialitatea si protectia datelor cu caracter personal.
- Vor fi asigurate mecanisme de securitate implementate pe mai multe niveluri, la nivel de aplicatie si la nivel de baza de date si se vor permite autentificarea, identificarea, verificarea drepturilor si permisiunilor, supravegherea cererilor de servicii si operatiilor executate de persoana care a generat, a modificat sau a sters o informatie.
- Utilizatorul nu va avea acces la baza de date decat prin intermediul aplicatiei. Acesta va putea vizualiza, modifica sau sterge doar acele date care au fost introduse de el si asta doar pe timpul valabilitatii sesiunii de lucru.
- Protectie impotriva atacurilor web commune
- SSL offloading in cazul securizarii comunicatiei client/server fara a aloca resurse de procesate pentru criptare/decriptare la nivelul server-ului de aplicatii
- Reducerea incarcarii server-elor de aplicatii prin mecanisme de cache-ing al continutului de tip static
- Reducerea traficului client/server prin mecanisme de compresie a continutului
- Distribuirea incarcarii provenita de la cererile clientilor catre mai multe server-e de aplicatii reducerea numarului de IP-uri publice in cazul existentei mai multor server-e de aplicatii.

2.3.1.5.3 Cerinte functionale Portal extern

Din punct de vedere functional aplicatia ce se va dezvolta pentru Portalul extern va trebui sa acopere cerintele privind procedurile de preaplicare pentru un anumit tip de serviciu.
In acest sens vom detalia in cele ce urmeaza un flux de serviciu pentru o intelegere deplina a ceea ce inseamna fluxul de prelucrare in aplicatie.
In ceea ce priveste serviciul de vize, legislatia aplicabila in perioada in care Romania nu este parte a Spatiului Schengen este diferita de legislatia pe care Romania este obligata sa o respecte in calitate de Stat Membru. Astfel, in perioada de pre-aderare la Spatiul Schengen viza romana se acorda de catre misiunile diplomatice si oficiile consulare ale Romaniei in conformitate cu prevederile OUG nr. 194/2002 privind regimul strainilor in Romania, republicata si modificata prin Legea 157/2011, in timp ce de la data aplicarii in totalitate a acquis-ului Schengen, Romania va elibera vize in conformitate cu prevederile Regulamentului (CE) 810/2009 al Parlamentului European si Consiliului din 13 iulie 2009, privind instituirea unui Cod Comunitar de Vize (Codul de Vize).
Conform legislatiei aplicabile, Romania poate elibera, in perioada de pre-aderare, 4 tipuri de viza: viza de tranzit aeroportuar, viza de tranzit, viza de scurta sedere si viza de lunga sedere, iar post-aderare 2 tipuri de viza: viza uniforma de scurta sedere (care include vizele de tranzit, tranzit aeroportuar si vize de scurta sedere in diverse scopuri) si viza nationala de lunga sedere.
Procedura de completare in portalul extern a solicitarii de serviciu consular consta, pentru vize, in completarea cererii de viza.
Pentru a elimina unele solicitari de vize ce nu pot si acceptate, vor fi introduse un numar de filtre, prin furnizarea de informatii legate de articolele 5 si 6 din Codul Comunitar de Vize.
Solicitantul selecteaza mai intai MD/OC in a carui circumscriptie consulara isi are domiciliul sau resedinta sau MD/OC la care doreste sa se prezinte, dar in a carui jurisdictie nu isi are resedinta sau domiciliul. In al doilea caz alegerea consulatului va fi insotita si de justificarea solicitarii vizei la consulatul respectiv.
Procedura parcursa de catre solicitant presupune verificarea faptului ca Romania este statul membru competent sa examineze si sa decida asupra solicitarii (Art. 5), cat si a competentei consulare teritoriale (Art. 6).
Daca viza solicitata este viza uniforma atunci solicitantul va trebui sa specifice conform carui punct si carei litere a articolului 5 din Codul Comunitar de Vize considera ca Romania este statul membru competent pentru a examina si a decide asupra cererii sale de viza:

Articolul 5 - Statul membru competent pentru a examina si a decide cu privire la o cerere
(1) Statul membru competent pentru a examina si a decide cu privire la o cerere de viza uniforma este:
(a) statul membru al carui teritoriu reprezinta singura destinatie a vizitei (vizitelor);
(b) daca vizita include mai multe destinatii, statul membru al carui teritoriu constituie principala destinatie a vizitei (vizitelor) din punctul de vedere al duratei sau al scopului sederii; sau

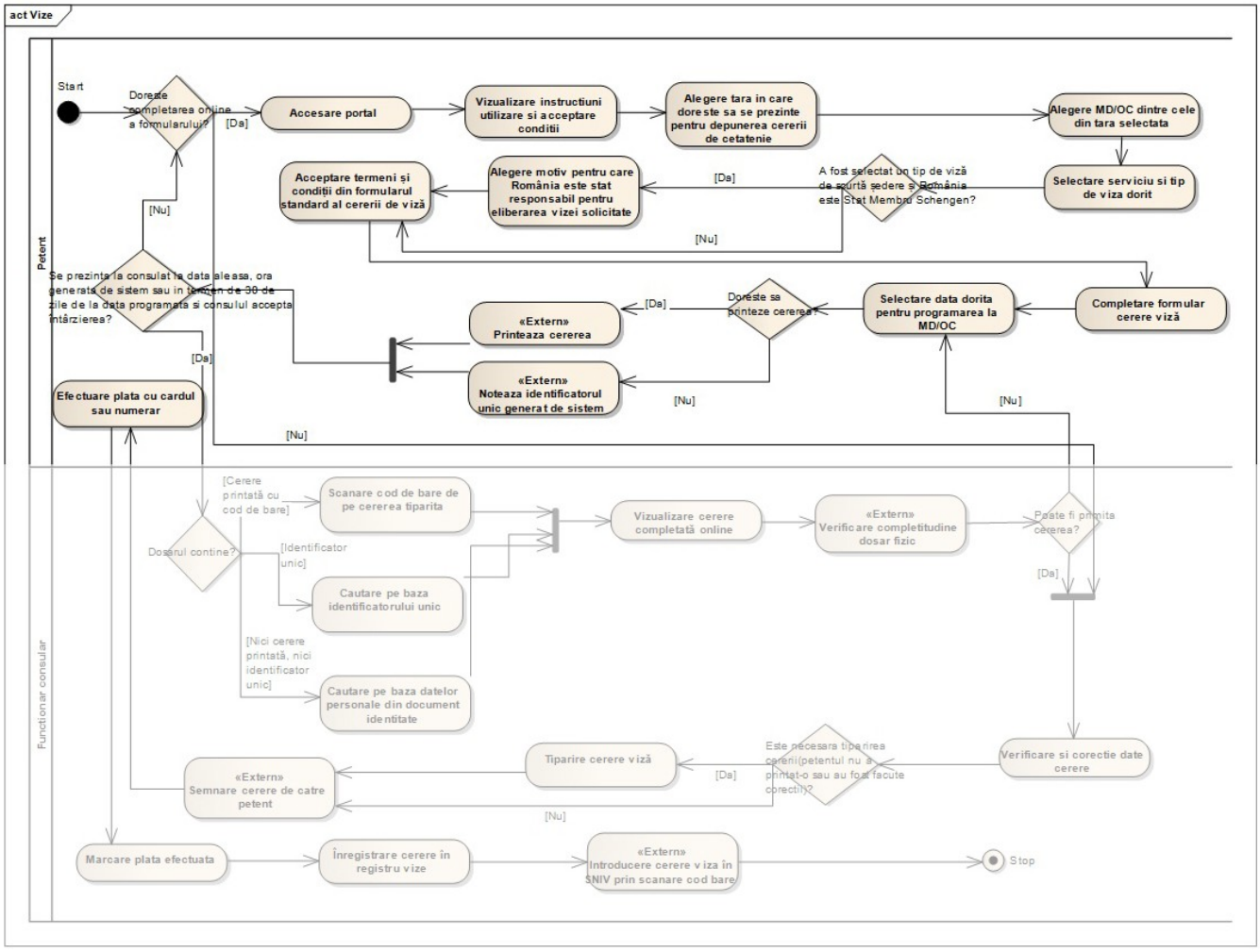
(c) daca destinatia principala nu poate fi stabilita, statul membru a carui frontiera externa urmeaza sa fie traversata de solicitant pentru a intra pe teritoriul statelor membre.

(2) Statul membru competent pentru a examina si a decide cu privire la o cerere de viza uniforma de tranzit este:
(a) in caz de tranzitare a unui singur stat membru, respectivul stat membru; sau
(b) in caz de tranzitare a mai multor state membre, statul membru a carui frontiera externa urmeaza sa fie trecuta de solicitant pentru a-si incepe tranzitul.

(3) Statul membru competent pentru a examina si a decide cu privire la o cerere de viza de tranzit aeroportuar este:
(a) in caz de tranzitare a unui singur aeroport, statul membru pe al carui teritoriu se afla aeroportul tranzitat; sau
(b) in cazul tranzitului aeroportuar dublu sau multiplu, statul membru pe al carui teritoriu se afla primul aeroport tranzitat.
(4) Statele membre coopereaza pentru a preveni situatia in care o cerere nu poate fi examinata si nu se poate decide cu privire la aceasta ca urmare a faptului ca statul membru competent, in conformitate cu alineatele (1)-(3), fie nu este prezent, fie nu este reprezentat in tara terta in care solicitantul depune cererea de viza in conformitate cu articolul 6.

Ulterior, petentul isi exprima acordului cu privire la termenii si conditiile din formularul standard al cererii de viza corespunzatoare tipului de viza dorit.
Solicitantul isi va selecta, dintr-o lista, cetatenia, astfel incat procedura sa conduca la identificarea corecta a procedurii pe care solicitantul trebuie sa o urmeze, acest pas scurtand, totodata, si timpul petrecut de catre solicitant la completarea procedurii online.
In urma selectarii cetateniei, exista trei variante posibile pe care solicitantul trebuie sa le parcurga, in functie de necesitatea obtinerii vizei sau de exceptarea de la aceasta obligativitate, de tipul de viza solicitat si de necesitatea de a obtine o invitatie avizata de Oficiul Roman pentru Imigrari.
Solicitantul va fi atentionat cu privire la exceptarea de la obligativitatea de a obtine viza in cazul in care detine un permis de sedere valabil pentru o perioada mai mare de 5 ani / tipul permisului - cu drept de sedere pe termen lung emis de state membre UE.
Dupa parcurgerea mai multor pasi petentului i se va deschide formularul aferent scopului de viza ales, iar solicitantul completeaza datele corespunzatoare cererii de viza.
La salvarea cererii, petentul va primi un identificator unic al cererii introduse, sub forma unui cod unic – atunci cand petentul alege sa nu isi listeze cererea, sau sub forma unui cod de bare – pe cererea listata.
Dupa salvarea datelor introduse, solicitantul isi va alege data la care se poate prezenta la MD/OC ales pentru analiza cererii de viza. Ca si in cazul celorlalte servicii, datelor pot fi selectate in functie de disponibilitatea, configurata pentru acea misiune, pentru serviciul de vize. Pentru ziua selectata, sistemul va prezenta orele disponibile, in concordanta cu sistemul de tiketing, petentul putand selecta dintre ele. Orice cerere completata online, pentru care solicitantul nu s-a prezentat la MD/OC, se va sterge automat din sistem in 30 de zile de la data pentru care a fost facuta programarea. In acest caz, solicitantul va relua fluxul de adaugare a unei cereri de viza in portalul extern.
Prezentam in continuare si modele ale cererilor de viza aplicabile in acest moment in sistem, modelele ce vor fi aplicate dupa aderarea Romaniei la Spatiul Schengen vor fi prezentate ofertantului castigator.
In **Anexa nr. 2** sunt prezentate modelele de cereri de viza ce vor trebui implementate in Portalul extern.

Exemplificam pentru calcul complexitatea unui flux. Se va lua in calcul implementarea unui numar de 40 de fluxuri de busines de complexitate similara.



Dintre cerintele functionale ale aplicatiei portalului extern enumeram, fara a ne limita la acestea:

- Sistemul trebuie sa permita organizarea logica a informatiilor pentru a putea fi stocate diferentiat in portalul intern, respectiv portalul extern
- Sistemul trebuie sa permita crearea sau modificarea conturilor pentru petentii care completeaza on-line cererile de viza
- Sistemul trebuie sa permita completarea on-line de catre petent si stocarea formularelor specifice serviciului de vize
- Sistemul trebuie sa permita generarea unui identificator unic pentru formularele completate
- Sistemul trebuie sa permita petentilor alegerea datei la care doresc sa se programeze pentru prezentarea la misiunea diplomatica in concordanta cu sistemele de tiketing instalate in fiecare consulat
- Sistemul trebuie sa permita stergerea automata a datelor introduse in portalul extern in cazul in care petentii nu se prezinta la misiune intr-un termen prestabilit de la data programata
- Sistemul trebuie sa permita completarea si modificarea dinamica de catre administrator a unor sectiuni informative referitoare la serviciul de vize, din portalul extern
- Sistemul trebuie sa permita petentilor cunoasterea valorii financiare a serviciilor solicitate
- Sistemul trebuie sa permita petentului consultarea stadiului cererii depuse
- Sistemul trebuie sa permita configurarea diferita a fluxurilor de lucru in functie de statutul Romaniei in relatia cu Spatiul Schengen
- Sistemul trebuie sa permita generarea de rapoarte predefinite
- Sistemul trebuie sa permita crearea si adaugarea de noi rapoarte
- Sistemul trebuie sa permita copierea datelor si a instantelor de aplicatie astfel incat sistemul sa poata fi readus la o stare prealabila fara pierdere de date
- Sistemul trebuie sa permita readucerea sistemului la o stare prealabila fara pierdere de date.

- Sistemul trebuie sa permita stergerea automata a formularelor si cererilor introduse in portalul extern odata cu inceperea fluxurilor de solutionare, in portalul intern.

2.3.1.5.4 CERINTELE TEHNICE PORTAL EXTERN

Solutia de portal extern trebuie sa fie o componenta comerciala independenta de sistemul dezvoltat (COTS) si va indeplini urmatoarele cerinte tehnice minime:

- Accesul la pagina de Portal se va face printr-un navigator de Web de tip Internet Explorer, Mozilla Firefox, Crome, Netscape etc;
- Sa ofere o vedere unica, consistenta asupra unei game variate de surse de informatii si in concordanta cu actiunile pe care utilizatorul le are de realizat;
- Interfata cu utilizatorii sa fie bogata in functionalitati, care sa ofere un nivel ridicat de accesibilitate, conform cu cerintele de accesibilitate WCAG versiunea 1.0;
- Interfata web cu template disponibil pentru look & feel comun organizatiei;
- Grad ridicat de securitate a sistemului, care sa garanteze confidentialitatea si securitatea datelor utilizatorilor pentru accesul neautorizat atat dinafara cat si din interiorul sistemului;
- Un framework unic de dezvoltare a portalului, astfel incat indiferent de tipul de continut publicat in portal sau de tipul de aplicatii, modul de integrare al acestora in portal sa fie consistent si sigur;
- Servicii si extensii ale portalului modulare, care sa permita dezvoltarea ulterioara de noi functionalitati;
- Sa contina un motor de cautare performant, care se permita efectuarea de interogari in toate sursele de informatie prezente in mediul portal
- Solutia de portal trebuie sa ofere un motor de cautare avansat, care sa permite utilizarea unor criterii de relevanta pentru obtinerea rapida a informatiilor cautate;
- Motorul de cautare va permite utilizarea expresiilor booleene in cadrul cautarilor.
- Suport pentru o platforma tehnologica recunoscuta (.Net, Java, etc.)
- Suport pentru bazele de date relationale (MySQL, Microsoft SQL Server, etc)
- Suport pentru un server de aplicatie recunoscut (IIS, Jboss, etc.)
- Suport pentru un numar mare de utilizatori concurenti; ofertantul va explica intr-un capitol separat modul in care intentioneaza sa implementeze aceasta facilitate
- Suport pentru UTF-8
- Editor al continutului de tip WYSIWYG care sa permita editarea continutului paginilor web
- Suport pentru notificari, versionare, loguri de audit si posibilitate de anularea a modificarilor. Aceasta facilitate va permite administratorilor sa vizualizeze cand continutul a fost modificat, cine a facut aceste modificari, sa vizualizeze versiunile anterioare si sa anuleze modificarile efectuate daca este cazul.
- Orar de publicare care sa permita determinarea timpului exaxt cand un anume continut va fi publicat sau eliminat de pe site.
- Configurarea rolurilor utilizatorilor. Spre exemplu, anumiti utilizatori pot avea dreptul de a crea continut dar nu si de al publica. Alti utilizatori pot avea dreptul de a revizui si aproba continutul. Accesul utilizatorilor poate fi restrictionat la anumite pagini sau sectiuni de pagini.
- Suport pentru reducerea traficului de internet; ofertantul va explica modul de implementare al acestei facilitati
- Va fi posibila vizualizarea istoricului autentificarilor de catre un administrator
- Suport pentru operatiuni de Drag'n'Drop al continutului
- Suport pentru redimensionarea imaginilor
- Obligativitatea autentificarii pentru accesul in anumite zone ale site-ului.
- Suport pentru Feed-uri RSS
- Posibilitatea integrarii cu alte componente ale proiectului
- Suport pentru LDAP
- Suport pentru SSL
- Integrare cu program tip office pentru editarea documentelor

- Motor de fluxuri de lucru (Workflow) pentru procesul de aprobare a publicarii si pentru notificari legate de evenimentele legate de site
- Sistem de gestiune a traducerilor bazat pe motorul de fluxuri de lucru
- Facilitate de biblioteca multimedia pentru stocarea imaginilor, documentelor, fisierelor de tip video sau flash
- Suport pentru teme si skin-uri
- Facilitate de tip „Cos de gunoi" pentru recuperarea continutului sters
- Functionalitati de cautare
- Functionalitate de tip „Site Map"

2.3.1.5.5 Cerinte de arhitectura a platformei de Portal extern

- Accesul la aplicatie trebuie sa se realizeze in intregime prin intermediul unei interfete WEB, accesibila printr-un browser consacrat. Nu se admit solutii tip client-server;
- Interfata cu utilizatorii trebuie sa fie consistenta, avand aceeasi logica de prezentare a informatiei pentru toate punctele de acces;
- Pentru optimizarea productivitatii trebuie sa existe separare intre incarcarea formelor de interfata cu utilizatorii si incarcarea datelor;
- Interfata cu utilizatorii trebuie sa asigure facilitati avansate de navigare intre ecrane prin functiuni de:
  - inainte si inapoi,
  - link-uri,
  - tab-uri .
- Trebuie sa existe functionalitati de help-online si ghidare prin ecranele unei aplicatii (in limbile enumerate);
- Ghidurile online de navigare si operare trebuie sa permita afisarea continua pe ecran a pasilor efectuati si a celor care urmeaza a fi efectuati;
- Platforma ofertata va utiliza o solutia unica de autentificare a utilizatorilor interni (administratori), indiferent de canalul de acces folosit;
- Platforma trebuie sa ofere propria interfata de management pentru a permite administratorilor sa faca schimbari in sistem, fara sa aiba acces la date private despre utilizatori;
- Platforma oferita trebuie sa asigure functionalitati proprii de securitate si audit;
  Functionalitatea de audit trebuie sa constea intr-un mecanism prin care sa se creeze un istoric al tuturor schimbarilor operate in sistem;

Arhitectura solutiei trebuie sa includa o componenta tip Server de Aplicatii. Intr-o arhitectura serverul de aplicatii este cel care expune nivelul logic si procesele de business, pentru a fi accesate si utilizate de clientii solutiei. Deoarece sistemul informatic este construit pe o arhitectura n-tier cu tehnologii web, sistemul va include clustere de servere de aplicatii.
Se vor oferi licente de utilizare a platformei de portal extern, dimensionate dupa necesitati, dar nu mai putin de 4 instante virtualizate de portal (cu server de aplicatii).

2.3.1.6 Portalul Intern

2.3.1.6.1 Cerinte generale

Solutia ceruta in prezentul proiect trebuie sa indeplineasca urmatoarele cerinte tehnice generale:

- Solutia va constitui singura modalitate de acces la informatii prin intermediul unui portal la care vor avea acces utilizatori interni (lucratori consulari).
- Solutia trebuie sa se integreze cu diverse surse interne de informatii existente in cadrul organizatiei.
- Sa fie capabila sa se integreze cu sisteme diferite de back-office provenite de la producatori diferiti sau dezvoltate intern.
- Solutia trebuie sa fie capabila sa gestioneze volume mari de date.

- Solutia trebuie sa se bazeze pe un sistem de gestiune al bazelor de date relationale, un server pentru gestiunea bazelor de date mari in conditii de siguranta si care permite un control riguros al accesului la diferite tipuri de informatii.
- Aplicatiile trebuie sa fie dezvoltate in tehnologie internet (web). Nu se vor agrea solutii de tip Client-Server sau distribuite pe statii de lucru, accesul utilizatorilor trebuie sa se faca prin intermediul unui browser.
- Administrarea sistemului si a bazei de date trebuie sa posede instrumente puternice pentru asigurarea protectiei si confidentialitatii datelor, bazate pe un sistem consistent de profile si autorizatii de acces.
- Documentatia completa de utilizare si administrare va fi livrata cu produsul.
- Procesul de implementare trebuie sa se desfasoare in conformitate cu o metodologie verificata, care sa asigure controlul fazelor, activitatilor, atributiilor, planificarea in timp, alocarea resurselor, continutul si rezultatul etapelor, confirmarea rezultatelor si documentarea procesului de implementare.
- Solutia trebuie sa ofere posibilitatea unei dezvoltari graduale prin punerea la dispozitia utilizatorilor de noi servicii.
- Solutia trebuie sa ofere o interfata prietenoasa si usor de folosit, consistenta din punct de vedere al design-ului in toate punctele de contact si sa ofere instrumente de navigare intuitive.
- Utilizatorul va avea acces la aplicatie printr-un simplu browser web fara a fi nevoit sa instaleze alte aplicatii.
- Solutia va oferi mecanisme avansate de autentificare a utilizatorilor si securizare a informatiilor.
- Solutia va fi dimensionata din punct de vedere software si hardware astfel incat sa asigure functionalitatile necesare utilizatorilor descrisi.

Infrastructura hardware trebuie complet licentiata din punct de vedere licente software pentru toate produsele care vor rula pe infrastructura respectiva.

2.3.1.6.2 Cerinte de securitate Portal intern

Portalul extern va indeplini urmatoarele cerinte de securitate:

- Sistemul va avea un sistem de securitate care permite protejarea informatiei, atat fata de accesul neautorizat intern, cat si fata de accesul neautorizat extern. Protectia va fi asigurata atat la nivel hardware cat si software.
- In acest sens, sistemul va indeplini anumite cerinte din punct de vedere al securitatii, cum ar fi autentificarea unica a utilizatorilor interni (administratori) si autorizarea acestora in sistem prin mecanisme de tip autentificare unica prin intermediul rolurilor si privilegiilor.
- Autentificarea unica a utilizatorilor interni (lucratori consulari) si autorizarea acestora in sistem prin mecanisme de tip autentificare unica prin intermediul rolurilor si privilegiilor.
- Utilizatorii vor avea acces numai la aplicatie.
- Sistemul va fi proiectat si implementat din punct de vedere al securitatii pe baza legilor, regulamentelor si instructiunilor in vigoare privind securitatea, confidentialitatea si protectia datelor cu caracter personal.
- Vor fi asigurate mecanisme de securitate implementate pe mai multe niveluri, la nivel de aplicatie si la nivel de baza de date si se vor permite autentificarea, identificarea, verificarea drepturilor si permisiunilor, supravegherea cererilor de servicii si operatiilor executate de persoana care a generat, a modificat sau a sters o informatie.
- Utilizatorul nu va avea acces la baza de date decat prin intermediul aplicatiei. Acesta va putea vizualiza, modifica sau sterge doar acele date care au fost introduse de el si asta doar pe timpul valabilitatii sesiunii de lucru.

2.3.1.6.3 Cerinte de audit si jurnalizare a platformei de Portal Intern

Portalul intern va indeplini urmatoarele cerinte de audit si jurnalizare:

- Ofertantul va oferi o aplicatie comerciala independenta de sistemul dezvoltat (COTS), care va realiza auditarea bazei de date, a nivelului de business si a interfetei grafice
- Toate operatiile realizate in cadrul sistemului vor trebui jurnalizate astfel incat, ulterior rezolvarii incidentului, sa se poata reface parcursul desfasurarii actiunilor. Astfel, aplicatia va include piste de

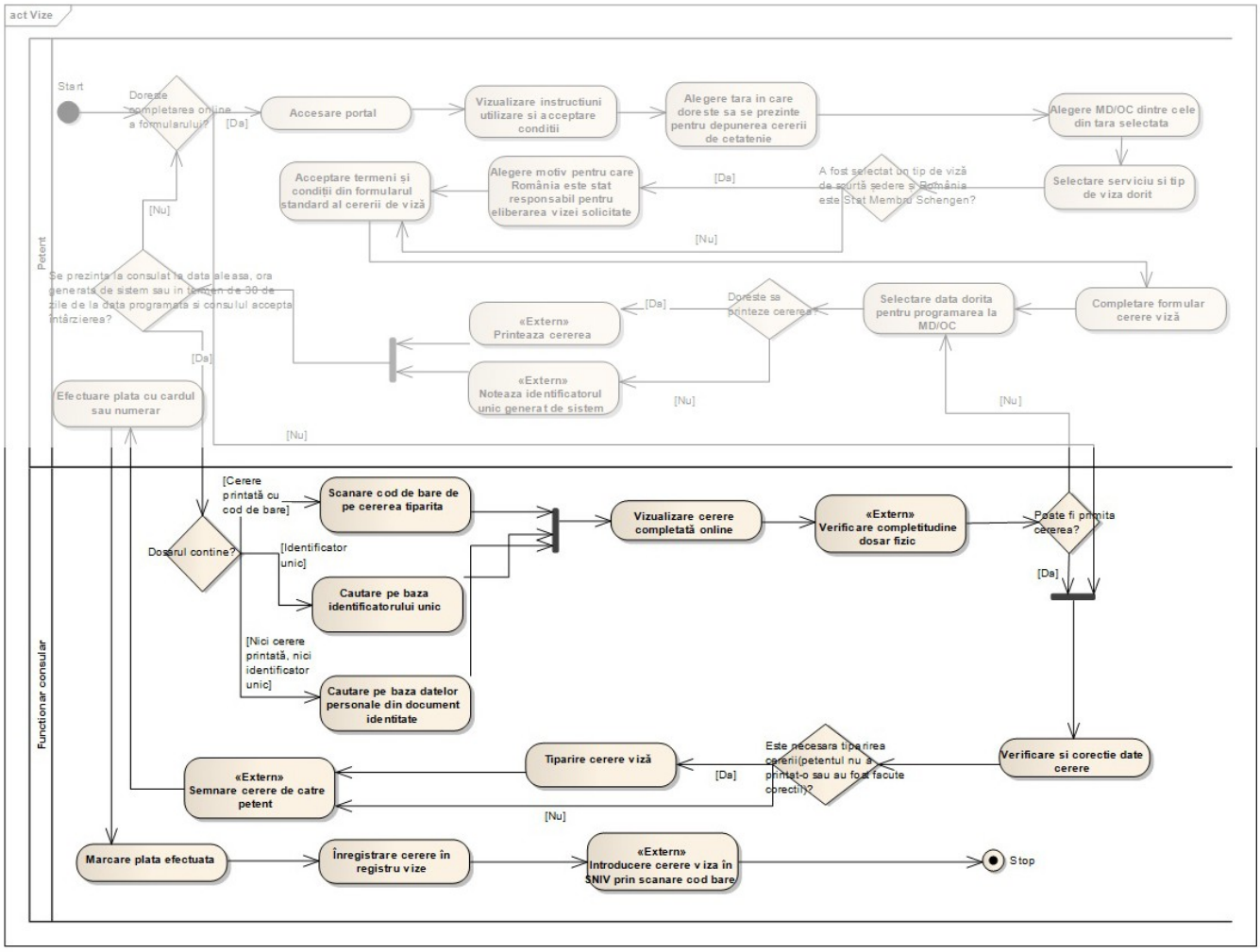
audit complete pentru toate operatiile efectuate, inclusiv cele administrative. Sistemul va pune la dispozitie un mecanism de urmarire a schimbarilor efectuate de un operator incepand cu nivelul de interfata grafica, nivelul de logica de aplicatii si pana in baza de date. Se va oferi astfel o pista completa de audit a interactiunii operator - sistem.

- Sistemul va pune la dispozitie rapoarte care vor determina toate schimbarile operate in baza de date de catre un operator intr-un interval de timp, avand formatul: date existente inainte de tranzactie; date modificate dupa tranzactie. Sistemul va permite configurarea tabelelor si entitatilor asupra carora se va face audit la nivel de schimbare de date.
- Beneficiarul poate sa activeze sau sa dezactiveze sistemul de audit, iar acesta nu va afecta viteza de raspuns a aplicatiei. Sistemul de audit va utiliza fisierele de tranzactii ale sistemelor de baze de date pentru a identifica schimbarile aduse datelor.
- Sistemul va gestiona corespondenta intre ecrane, operatii de logica de business si datele modificate. In acelasi timp se va inregistra adresa de la care operatorul a efectuat operatiile, data, ora precum si alte date utile identificarii acestuia.
- In cadrul unei activitati de investigare, sistemul va permite interogarea bazei de date de istoric pentru a afla valoarea unei anumite coloane dintr-o tabela asa cum se regasea aceasta la momentul de timp cand s-a petrecut incidentul investigat.
- Sistemul trebuie sa auditeze urmatoarele operatii:
    - Operatiile facute intr-o sesiune de lucru a unui utilizator;
    - Operatiile facute de un anumit utilizator;
    - Operatiile facute de la o anumita statie de lucru
    - Operatiile facute pe toate tabelele din baza de date precum si datele modificate de acestea memorand datele inainte si dupa operatia respectiva;
    - Operatiile facute pe anumite entitati de business
- Sistemul trebuie sa puna la dispozitie un sistem complex de filtrare al datelor istorice astfel incat sa se poata determina precis cand, ce si cum s-a executat in sistem, cine este autorul si ce impact a avut asupra sistemului.
- Sistemul trebuie sa permita regasirea valorilor prin care a trecut orice inregistrare din baza de date precum si utilizatorii si procesele de business care au cauzat acele schimbari. Trebuie sa se poata regasi istoricul complet al inregistrarilor si evolutia acestora in timp.
- Sistemul trebuie sa permita activarea auditului doar pe un set restrans de tabele din baza de date, permitand astfel reducerea dimensiunii auditului si indreptarea acestuia numai asupra tabelelor relevante acestei activitati.
- Sistemul trebuie sa poata face audit la audit astfel incat sa inregistreze toate schimbarile aduse pe baza de audit. Permisiunile sunt diferite. Nu se accepta ca baza de date de audit sa fie aceeasi cu baza operationala.
-

2.3.1.6.4 Cerinte functionale a platformei de Portal Intern

Portalul intern va indeplini urmatoarele cerinte functionale:
La data programata, solicitantul se prezinta la MD/OC selectat in momentul completarii cererii de sevicii consulare si prezinta functionarului consular identificatorul unic pentru a cauta cererea de viza completata online de catre petent. Functionarul consular verifica corectitudinea cererii de viza completata online. Pentru eventualele inconsistente, functionarul editeaza cererea electronica astfel incat datele completate sa fie in concordanta cu documentul de calatorie prezentat.
Solicitantul semneaza cererea de viza, dupa care realizeaza plata pentru serviciul consular solicitat.
Dupa inregistrarea platii, functionarul consular implementeaza aceasta cerere in SNIV, preluand datele din cererea electronica din portalul intern si inregistreaza cererea de viza in registrul de vize.

Exemplificam pentru calcul, complexitatea unui fluxde lucru. Se va lua in calcul implementarea unui numar de 40 de fluxuri de busines de complexitate similara.



Dintre cerintele functionale ale aplicatiei Portalului intern, enumeram fara a ne limita la acestea:

- Sistemul trebuie sa permita organizarea logica a informatiilor pentru a putea fi stocate diferentiat in portalul intern, respectiv portalul extern
- Sistemul trebuie sa permita completarea on-line de catre petent si stocarea formularelor specifice serviciului de vize
- Sistemul trebuie sa permita generarea unui identificator unic pentru formularele completate
- Sistemul trebuie sa permita petentilor alegerea datei la care doresc sa se programeze pentru prezentarea la misiunea diplomatica si sa se sincronizeze cu portalul extern in care sunt prezentate datele de programare in colaborare cu sistemele de tiketing instalate in cadrul consulatelor
- Sistemul trebuie sa permita stergerea automata a datelor introduse in portalul intern in cazul in care petentii nu se prezinta la misiune intr-un termen prestabilit de la data programata
- Sistemul trebuie sa permita gestiunea financiara a platilor realizate de catre petenti prin intermediul POS sau cash la ghiseu
- Sistemul trebuie sa permita petentului consultarea stadiului cererii depuse
- Sistemul trebuie sa permita autentificarea responsabililor consulari pe baza de nume utilizator si parola
- Sistemul trebuie sa permita utilizatorilor sa acceseze functionalitatile si seturile de date conform drepturilor acordate
- Sistemul trebuie sa permita configurarea diferita a fluxurilor de lucru in functie de statutul Romaniei in relatia cu Spatiul Schengen
- Sistemul trebuie sa permita inlocuirea registrului in format fizic cu registrul de vize electronic
- Sistemul trebuie sa permita realizarea schimbului de informatii suplimentare cu autoritatile nationale competente
- Sistemul trebuie sa permita generarea de rapoarte predefinite
- Sistemul trebuie sa permita crearea si adaugarea de noi rapoarte

- Sistemul trebuie sa permita copierea datelor si a instantelor de aplicatie astfel incat sistemul sa poata fi readus la o stare prealabila fara pierdere de date
- Sistemul trebuie sa permita readucerea sistemului la o stare prealabila fara pierdere de date
- Sistemul trebuie sa permita stergerea automata a formularelor si cererilor introduse in portalul extern odata cu inceperea fluxurilor de solutionare, in portalul intern

2.3.1.6.5 CERINTELE TEHNICE A PLATFORMEI DE PORTAL INTERN

- Accesul la pagina de Portal se va face printr-un navigator de Web de tip Internet Explorer, Mozilla Firefox, Crome sau Netscape;
- Sa ofere o vedere unica, consistenta asupra unei game variate de surse de informatii si in concordanta cu actiunile pe care utilizatorul le are de realizat;
- Interfata cu utilizatorii sa fie bogata in functionalitati, care sa ofere un nivel ridicat de accesibilitate, conform cu cerintele de accesibilitate WCAG versiunea 1.0;
- Interfata web cu template disponibil pentru look & feel comun organizatiei;
- Grad ridicat de securitate a sistemului, care sa garanteze confidentialitatea si securitatea datelor utilizatorilor pentru accesul neautorizat atat dinafara cat si din interiorul sistemului;
- Un framework unic de dezvoltare a portalului, astfel incat indiferent de tipul de continut publicat in portal sau de tipul de aplicatii, modul de integrare al acestora in portal sa fie consistent si sigur;
- Servicii si extensii ale portalului modulare, care sa permita dezvoltarea ulterioara de noi functionalitati;
- Sa contina un motor de cautare performant, care se permita efectuarea de interogari in toate sursele de informatie prezente in mediul portal;
- Solutia de portal trebuie sa ofere un motor de cautare avansat, care sa permite utilizarea unor criterii de relevanta pentru obtinerea rapida a informatiilor cautate;
- Motorul de cautare va include mecanisme de invatare pe baza cautarilor deja efectuate pentru strangerea informatiilor referitoare la relevanta;
- Motorul de cautare va permite utilizarea expresiilor booleene in cadrul cautarilor.

2.3.1.6.6 CERINTE DE INTEGRARE A PLATFORMEI DE PORTAL INTERN

Avand in vedere necesitatea integrarii Portalului Intern cu SNIV (Sistemul National de Informatii privind Vizele), ofertantul va propune si explica, o solutie de integrare, care sa respecte urmatoarele cerinte:

- Capabilitati avansate de transformare a mesajelor
- Persistarea mesajelor pentru a facilita retransmisia in caz de erori
- Suport pentru definirea modului de transformare a mesajelor
- Suport pentru conversatii asincrone
- Suport pentru standarde deschise (cel putin XML, SOAP)
- Procesare tranzactionala precum si ne-tranzactionala a mesajelor
- Sistemul va fi tolerant la erori
- Regulile de transformare sa poata fi stocate centralizat

Ofertantul va explica modul in care intentioneaza sa foloseasca Solutia de integrare a platformei de Portal Intern cu SNIV.

2.3.1.6.7 CERINTE DE ARHITECTURA A PLATFORMEI DE PORTAL INTERN

- Accesul la aplicatie trebuie sa se realizeze in intregime prin intermediul unei interfete WEB, accesibila printr-un browser consacrat. Nu se admit solutii tip client-server;
- Interfata cu utilizatorii trebuie sa fie consistenta, avand aceeasi logica de prezentare a informatiei pentru toate punctele de acces;
- Pentru optimizarea productivitatii trebuie sa existe separare intre incarcarea formelor de interfata cu utilizatorii si incarcarea datelor;
- Interfata cu utilizatorii trebuie sa asigure facilitati avansate de navigare intre ecrane prin functiuni de:

- inainte si inapoi,
- link-uri,
- tab-uri .

- Trebuie sa existe functionalitati de help-online si ghidare prin ecranele unei aplicatii (in limbile enumerate);
- Ghidurile online de navigare si operare trebuie sa permita afisarea continua pe ecran a pasilor efectuati si a celor care urmeaza a fi efectuati;
- Platforma ofertata va utiliza o solutia unica de autentificare a utilizatorilor interni (administratori), indiferent de canalul de acces folosit;
- Platforma trebuie sa ofere propria interfata de management pentru a permite administratorilor sa faca schimbari in sistem, fara sa aiba acces la date private despre utilizatori;
- Platforma oferita trebuie sa asigure functionalitati proprii de securitate si audit;
  Functionalitatea de audit trebuie sa constea intr-un mecanism prin care sa se creeze un istoric al tuturor schimbarilor operate in sistem;

Arhitectura solutiei trebuie sa includa o componenta tip Server de Aplicatii. Intr-o arhitectura serverul de aplicatii este cel care expune nivelul logic si procesele de business, pentru a fi accesate si utilizate de clientii solutiei. Deoarece sistemul informatic este construit pe o arhitectura n-tier cu tehnologii web, sistemul va include clustere de servere de aplicatii.

Se vor oferi licente de utilizare a platformei de portal intern, dimensionate dupa necesitati, dar nu mai putin de 2 instante virtualizate de portal (cu server de aplicatii).

2.3.1.7 PLATFORMA DE MANAGEMENT SI INVESTIGATIE CENTRALIZATA A EVENIMENTELOR DE SECURITATE IT

Solutia ceruta in prezentul proiect trebuie sa indeplineasca urmatoarele cerinte tehnice generale::

- Administrarea evenimentelor
  - Sa poata administra evenimentele din sisteme de opere (de ex: Windows Server), LDAP Directory (de ex: Active Directory), Server de aplicatie (de ex: Internet Information Services - IIS), server de mail (de ex: Exchange Server), baza de date (de ex: SQL Server) printr-un jurnal de evenimente la nivel de organizatie care colecteaza si raporteaza problemele si informatiile generate referitoare la sistemele si aplicatiile din reteaua institutiei.
  - Sa poata administra evenimentele si din alte sisteme precum Red Hat Enterprise Server, Windows Server, Suse Linux Enterprise Server, Sun Solaris Server, IBM AIX Server, HP-UX Server.
  - Sa permita monitorizarea switch-urilor, routerelor, imprimantelor si altor dispozitive prin SNMP si Syslog.
- Monitorizare
  - Sa permita monitorizarea proactiva si generarea de mesaje de avertizare prin capacitatile distribuite care urmaresc si monitorizeaza informatiile si trimit problemele prin e-mail sau prin alte medii externe; aceste avertizari sa poata produce actiuni care duc la rezolvarea problemelor.
  - Sa poata sa monitorizeze performanta si starea serverelor Microsoft, Linux, Unix, Windows Server, servere Linux RedHat Enterprise Server; Suse Linux Enterprise Server; Sun Solaris Server; IBM AIX Server; HP-UX Server
  - Sa poata sa monitorizeze aplicatiile din punct de vedere al performantei si disponibilitatii.
  - Sa poata sa monitorizeze masinile virtuale si aplicatiile din masinile virtuale (medii VMware si Hyper-V)
  - Sa permita monitorizarea aplicatiilor distribuite pe mai multe servere precum si definirea in mod grafic a componentelor unui serviciu
  - Sa poata sa monitorizeze si sa raporteze evenimentele, sa permita urmarirea nivelului de sanatate a sistemului precum si sa ofere un dashboard centralizat cu informatiile critice despre resursele IT “business critical”

- Raportare si analiza
  - Sa efectueze raportarea si analiza tendintelor necesare pentru urmarirea problemelor in timp si generarea rapoartelor detaliate despre starea de functionare generala a mediului administrat.
  - Rapoartele sa poata fi accesate local sau publicate in site web pentru accesul facil la informatiile de administrare ale sistemelor.
- Administrarea operatiunilor
  - Sa permita administrarea operatiunilor specifice domeniului prin pachete de administrare detaliate pentru tehnologii si produse diferite, incluzand sisteme de operare, LDAP Directory, Server de aplicatie, Distributed Transaction Coordinator (MDTC sau echivalent), Internet Naming Service (WINS sau echivalent), Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), Routing and Remote Access Service, Message Queuing (MSMQ sau echivalent), Mail Server (de ex: Exchange), Baze de date (de ex: SQL Server), Server proxy.
- Scalabilitate
  - Sa permita monitorizarea unei infrastructuri ce poate contine sute de servere, aplicatii, statii client.
- Management End-to-End Services
  - Sa permita monitorizarea aplicatiilor distribuite pe mai multe servere;
  - Sa permita definirea in mod grafic a componentelor unui serviciu;
  - Monitorizeaza si raporteaza evenimentele si permite urmarirea nivelului de sanatate al sistemului
- Monitorizarea statiilor de lucru
  - permite monitorizarea statiilor de lucru la nivelul sistemului de operare sau la nivelul aplicatiilor;
  - permite monitorizarea fara agent (agentless) prin capturarea erorilor de aplicatii;
  - permite crearea unor rapoarte si alerte pentru administratori privind problemele cu impact asupra sistemelor si utilizatorilor
- Management Packs
  - sa includa cele mai bune practici pentru descoperirea, monitorizarea, depanarea si rezolvarea problemelor pentru o componenta specifica (sistem de operare, aplicatie)
- Securitate
  - serverul sa refuze conexiuni de la agenti instalati manual, iar comunicarea intre agenti si servere sa poata fi criptata folosind certificate digitale;
  - administratorii sa poata avea niveluri de securitate diferite si accesa separat consola de administrare;
  - posibilitatea de integrare cu LDAP Directory astfel incat prin introducerea unui nou dispozitiv intr-un Organizational Unit (OU) acesta sa fie automat detectat, iar agentul de monitorizare automat instalat si configurat sa comunice cu serverul de monitorizare;
  - sa ofere posibilitatea de a colecta jurnalele de securitate din sistemele de operare Windows, Linux, Unix sau dispozitive de retea si stocarea lor intr-o baza de date separata
- Integrare cu alte sisteme de management si monitorizare
  - Sa ofere conectori pentru integrare cu solutii de management precum IBM Tivoli, HPOpen View, BMC Remedy, Microsoft System Center, precum si Universal Connector pentru integrare cu alte solutii de monitorizare.
- Suport pentru baza de date

Produsul trebuie sa fie livrat impreuna cu baza de date necesara functionarii corecte.

- Sistemul trebuie sa detina un editor in mod grafic de componente ale unui serviciu;
- Sistemul trebuie sa permita monitorizarea si raportarea evenimentelor, urmarirea nivelului de sanatate al sistemului
- Sistemul trebuie sa permita identificarea fiecarui echipament din retea printr-o icoana grafica;
- Aceste rapoarte sa poata fi accesate local sau sa poata fi publicate in site-urile Web pentru accesul facil la informatiile de administrare ale sistemelor.

- Modulul trebuie sa permita definirea de harti de monitorizare intr-un editor grafic, cu posibilitati de a crea prin operatii de tip wizard si drag-n-drop
  - Harta echipamentelor in rack
  - Harta aplicatiilor pe echipamente
  - Harta echipamentelor/aplicatiilor in camerele unde sunt instalate
  - Harta camerelor in cadrul cladirilor
  - Harta cladirilor in cadrul oraselor
  - Harta tuturor elementelor monitorizate la nivel de tara sau glob
- Utilizatorul trebuie sa poata naviga intre harti astfel incat sa comute de la un nivel de detaliere la altul, vizualizand oricand, in timp real, starea aplicatiilor si a echipamentelor monitorizate
- In cadrul unui proces informational utilizatorul trebuie sa poata sa ajunga repede, din elementele de proces monitorizate pana la pozitia in rack a echipamentului care a produs defectiunea.
- Modulul trebuie sa permita crearea de harti de proces, geografice, topologice sau de tip panou de bord pe care sa se pozitioneze elementele monitorizate
- Hartile elementelor monitorizate sa poata fi afisate in baza rolurilor utilizatorilor printr-un browser web.
- Sa prezinte portleti specifici pentru cel putin un portal (ex: Sharepoint, Websphere, WebLogic)
- Sa permita crearea de rapoarte de disponibilitate a aplicatiilor pe baza interdependentelor intre harti

Se vor oferi licentele de utilizare a platformei de management si investigatie centralizata a evenimentelor de securitate IT dimensionate dupa necesitati care sa se poata instala pe minimum 2 instante virtualizate de server.

2.3.1.8 SERVER DE AUTENTIFICARE

Solutia va include o componenta server de autentificare care va respecta urmatoarele cerinte tehnice:

- Sa functioneze ca un serviciu de interfatare intre utilizatori si orice tip de interfata / aplicatie ce necesita autentificare;
- Sa suporte urmatoarele metode de autentificare :
  - OTP (inclusiv cele ce folosesc algoritmul OATH HOTP),
  - MasterCard CAP,
  - VISA DPA,
  - SMS,
  - Card-uri PKI,
  - Card-uri cu numere (coduri) de autorizare de tranzactie,
  - Card-uri cu display,
  - Parole statice, PIN-uri, parole partiale.
- Sa permita integrarea cu usurinta in aplicatiile existente, fara a aduce modificari extensive acestora;
- Sa permita accesul la functiile administrative doar prin folosirea de smartcard-uri sau tokenuri USB;
- Sa mentina un jurnal securizat al tuturor activitatilor de administrarea si sa nu permita accesul la acest jurnal decat prin autentificare cu smartcard sau token USB;
- Sa se poata integra facil cu modulele hardware de protectie a materialului criptografic;
- Sa permita administrarea de la distanta;
- Sa permita criptarea comunicatiei de retea cel putin prin algoritm de criptare AES;
- Sa permita integrarea in multiple ahitecturi de autentificare;
- Sa permita configurarea parametrilor de validare a autentificarii indiferent de metoda de autentificare folosita;
- Sa suporte cel putin urmatoarele sisteme de operare :
  - Microsoft Windows Server 2003/2008/2008 R2,
  - Red Hat Enterprise,
  - AIX.
- Sa suporte cel putin urmatoarele baze de date :
  - Oracle 10 si 11,

- Microsoft SQL 2005 si 2008,
- ODBC.

- Sa suporte cel putin urmatoarele module hardware de protectie a materialului criptografic :
  - SafeNet ProtectServer (atat PCI cat si de retea);
  - nCipher nShield (atat PCI cat si de retea);
  - IBM 4764;
  - Emulatoare software ale functiilor de protectie a materialului criptografic.
- Sa nu fie dependent de un anume tip sau marca de token de autentificare;
- In configuratia livrata solutia trebuie sa dispuna de urmatoarele functionalitati:
- Sa suporte cel putin urmatoarele metode de autentificare :
  - OTP (inclusiv cele ce folosesc algoritmul OATH HOTP);
  - Card-uri PKI;
  - Parole statice, pin-uri, parole partiale.
- Sa permita accesul la functiile administrative doar prin folosirea de smartcard-uri sau tokenuri USB;
- Sa suporte configuratiile de tip cluster atat pentru balansarea distribuirii cererilor de autentificare cat si pentru redundanta maxima.

Se vor oferi licentele de utilizare a serverului de autentificare dimensionate dupa necesitati care sa se poata instala pe minimum 2 instante virtualizate de server.

2.3.1.9 SERVER DE SEMNARE CENTRALIZATA

Solutia trebuie sa contina un server de semnare centralizata a semnaturii digitale cu perechi de chei private / certificate digitale pe baza autentificarii multifactor a operatorilor titulari, care va oferi urmatoarele functionalitati:

- Functionalitatea specifica, de invocare si de control al executarii semnaturii digitale, va fi disponibila, in mediu client de tip browser, integrat in aplicatii de tip portal sau asimilate, si va putea fi utilizata de pe terminale de post de lucru.
- Functionalitate specifica va putea fi configurata ca flux de proceduri, inclusiv pentru executare de semnaturi multiple concurente, pe acelasi document si pentru a asigura mecanisme interactive de tip What You See Is What You Sign (WYSIWYS).
- Solutia va genera si stoca centralizat, in mod protejat cheile private de semnatura, pentru a permite un nivel maxim de securitate a materialului criptografic stocat si pentru a asigura integritatea si securitatea procesarii criptografice specifice.
- Solutia va genera o arhitectura care va avea minim impact (tip zero footprint) pe platformele client, la nivel de post de lucru, si va permite astfel atat pastrarea mobilitatii operatorului care va putea executa semnatura de pe oricare din terminalele sistemului, fara a face rabat de la securitate si cu mentinerea controlului semnatarului asupra procesului de generare a semnaturii.
- Mecanismul centralizat va asigura si un nivel maxim de securitate a gestiunii ciclului de viata al cheilor private de semnatura si, respectiv, al certificatelor digitale de verificare corespondente.
- Solutia va include mecanisme de audit operational si va permite o jurnalizare stricta a tuturor semnaturilor executate de fiecare operator, in parte, precum si pentru intreg sistemul.

Totodata, solutia va respecta urmatoarele cerinte tehnice :

- Formate de semnatura suportate:
  - PKCS#1,
  - PKCS#7,
  - ISO 9796-1.
- Metode de autentificare suportate:
  - OATH (de tip event based, time based si challenge/response) ,
  - Metode dinamice de tip OTP bazate pe comunicatii SMS ,
  - Metode statice de tip OTP ,
  - Metode specofice EMV, inclusiv MasterCard CAP si Visa DPA ,
  - Parole statice si partiale.

- Integrare cu autoritati de certificare:
  - Solutia va permite integrare cu autoritatile de certificare bazate pe standardele X.509v3 via functionalitati standard PKCS#10.
- Integrare cu servicii de de aplicatie in tehnologie Web:
  - Applet dedicat pentru serviciu de semnare integrat,
  - SDK Java pentru integrare functiilor de autentificare si semnare,
  - API bazat pe ANSI C, disponibil si ca biblioteca cu incarcare dinamica pentru medii Microsoft Windows.
- Integrare cu medii de tip sistem de post de lucru:
  - Suport pentru sisteme de operare Microsoft Windows,
  - Suport pentru CryptoAPI, respectiv integrare ca structura CSP,
  - Sport pentru metode standard PKCS#11.
- Suport pentru sisteme de gestiune a bazelor de date:
  - Microsoft SQL Server,
  - Oracle.
- Suport pentru infrastrucutra criptografica de securitate specializata:
  - Thales,
  - SafeNet,
  - IBM.
- Cerinte de securitate operationala:
  - Baza de date interna a solutiei, protejata criptografic, asigura integritatea informatiei stocate si confidentialitatea datelor critice ,
  - Toate informatiile martor de audit operational si de securitate sunt stocate, in mod securizat, in baza de date interna a solutiei,
  - Controlul accesului operatorilor la sistem include autentificare multifactor cu smartcard si autorizare pe baza de roluri ,
  - Accesul administrativ la functiile cheie presupune autentificarea concurenta a doi administratori .
- Alte functionalitati:
  - Functii interne de monitorizare a performantei sistemului,
  - Solutia asigura nivelul optim de disponibilitate operationala si permite cresterea capacitatii de procesare prin mecanisme de clustering multi-nod ,
  - Solutia poate executa in paralel semnaturi pe baza de perechi de cheie privata / certificat digital emise de mai multe autoritati de certificare,
  - Solutia asigura separatia interna a serviciilor de autentificare / autorizare fata de serviciul de executare a semnaturii digitale.

Se vor oferi licentele de utilizare a serverului de semnare centralizata dupa necesitati care sa se poata instala pe minimum 2 instante virtualizate de server.

2.3.1.10 SERVER DE MARCARE TEMPORALA

Solutia va include o componenta server de marcare temporala, care va indeplini urmatoarele cerinte tehnice specifice:

- Sa permita administrarea de la distanta;
- Producatorul sa puna la dispozitie in mod gratuit SDK-ul de dezvoltare a aplicatiei, in vederea extinderii functionalitatii;
- Sa se poata integra facil cu modulele hardware de protectie a materialului criptografic;
- Sa suporte urmatoarele tipuri de marci temporale:
  - RFC 3161;
  - Direct TCP;
  - SOAP peste HTTP.

- Sa permita folosirea cheilor criptografice RSA de la 104-bit pana la 4096-bit;
- Sa permita folosirea certificatelor digitale bazate pe x.509 versiunea 3 si a cererilor de certificate bazate pe PKCS#10 sau a celor auto-semnate bazate pe x.509 versiunea 3;
- Sa permita definirea de roluri administrative;
- Sa mentina un jurnal securizat al tuturor activitatilor de administrarea si sa nu permita accesul la acest jurnal decat prin autentificare cu smartcard;
- Sa ofere suport pentru sistemele de operare Microsoft;
- Sa ofere suport pentru servere de timp (NTP/SNTP) hardware;
- Sa suporte cel putin urmatoarele baze de date:
  - Microsoft SQL 2005 si 2008;
  - ODBC.
- Sa suporte cel putin urmatoarele module hardware de protectie a materialului criptografic :
  - SafeNet ProtectServer (atat PCI cat si de retea);
  - nCipher nShield (atat PCI cat si de retea);
  - IBM 4764;
  - Thales.

In configuratia livrata solutia trebuie sa dispuna de urmatoarele functionalitati:

- Sa permita accesul la functiile administrative doar prin folosirea de smartcard-uri sau tokenuri USB;
- Sa suporte configuratiile de tip cluster atat pentru balansarea distribuirii cererilor de autentificare cat si pentru redundanta maxima.

Se vor oferi licentele de utilizare a serverului de marcare temporala dupa necesitati care sa se poata instala pe minimum 2 instante virtualizate de server.

2.3.1.11 Platforma de mesagerie

Solutia va include o platforma de mesagerie electronica tip server care trebuie sa indeplineasca urmatoarele cerinte tehnice :

Usurinta in utilizare:

- In cazul accesului la casuta postala prin Web sa se permita convertirea documentelor (de tip Office sau PDF) astfel incat sa poata fi vizualizate chiar daca aplicatiile respective nu sunt instalate pe calculatorul client. Deasemenea, accesul prin Web sa aduca functionalitati extinse gen schedule assistant, categorii de mesaje, cautari avansate
- Lucru colaborativ facil din interfata Web, adica daca un utilizator primeste o legatura la un document de pe un site (portal) sau alt sistem de partajare a fisierelor, sistemul de mesagerie sa preia linkul si sa faca cererea in numele utilizatorului pentru a afisa documentul.
- Usurinta in realizare de reguli pentru a redirecta corespondenta in diverse arhive, containere sau destinatii,
- Posibilitatea de a marca corespondenta cu diferite culori in functie de importanta, pentru o vizibilitate mai buna.
- Posibilitatea de a grupa e-mailurile in functie de topic, destinatar, identificator etc.
- Informatii oferite in legatura cu destinatiile din interiorul institutiei catre care dorim sa trimitem corespondenta (exemplu: daca persoana respectia este in concediu; daca in componenta grupului catre care dorim sa trimitem un mesaj exista si oameni din afara institutiei etc)

Eficienta in administrare si securitate

- Sistemul de mesagerie trebuie sa asigure performante ridicate si fiabilitate, pe masura ce cresc dimensiunile casutelor postale si numarul de conturi de utilizator per server. Sa aiba capacitatea sa acomodeze cantitati foarte mari de mesaje la performante ridicate.
- Sistemul sa ofere un grad ridicat de securitate, care sa poate fi integrat nativ cu PKI (infractrucura de chei publice) sau cu RMS (sistem de gestionare a drepturilor de acces la informatie) usor de folosit si integrat nativ cu LDAP Directory.
- Platforma trebuie sa fie extensibila pentru servicii web pentru a le putea permite dezvoltatorilor sa integreze informatii din casutele postale sau calendar cu aplicatii specifice companiei sau alte aplicatii personalizate.

- Sistemul sa permita filtrarea antispam disponibila de la instalare, fiind gestionata de rolul de server Edge Transport, in perimetrul retelei si sa ofere un mecanism de protectie impotriva virusilor si al viermilor de retea.
- Arhitectura sa asigure o inalta disponibilitate si replicarea bazelor de date cu casutele postale. Baza de date sa poata sa fie replicata si pe alte servere de mesagerie din institutie, si in cazul in care baza de date primara este corupta, automat utilizatorul sa fie redirectat catre alta copie a casutei postale.
- E-mailurile din interiorul organizatiei sa fie criptate automat, de la plecarea din clientul de e-mail al expeditorului, pana la primirea in clientul de e-mail al destinatarului.
- Configurarea aplicatiei client de e-mail (Outlook sau echivalent), in vederea conectarii la server, sa se faca usor, de genul daca utilizatorul este conectat la retea, serverul de mesagerie prin componentele sale sa configureaze automat profilul de client de mail al utilizatorului.
- Pentru a putea impune anumite reguli (interne, guvernamentale sau locale) sistemul trebuie sa fie capabil, prin control detaliat asupra fluxurilor de e-mailuri, sa implementeze un motor pentru politici.
- Pentru a asigura certificarea mesajelor administratorii trebuie sa poata utiliza reguli de transport pentru a aplica clasificari ale mesajelor pentru e-mailurile in tranzit, in functie de subiect, continut sau adresa expeditorului/destinatarului. Sa existe posibilitatea folosirii unui un proces automat care sa scaneze foldere predefinite de administrator pentru a retine, expira sau jurnaliza mesajele, in functie de normele care trebuie respectate.
- Sistemul sa poata permite realizarea de cautari text rapide in cadrul tuturor casutelor postale din organizatie, daca este necesara aceasta actiune din punct de vedere legal.
- Sistemul de mesagerie sa permita integrarea cu centrala telefonica existenta pentru a adauga functionalitati de cutie vocala cat si IVR (recunoasterea inteligenta a vocii) pentru utilizatorii din institutie.
- Produsul sa ofere sistemului de operare contorii necesari pentru a putea fi urmarita starea de functionare si performanta in fiecare clipa cat si integrarea cu diferite unelte de monitorizare.
- Consolele de aministrare sa fie intuitive si usor de utilizat.
- Sistemul sa poata delega drepturi diferite pentru anumite departamente sau grupuri de persoane pentru a asigura segregarea drepturilor in functie de responsabilitatile fiecarui utilizator.
- Sistemul sa dispuna de unelte care sa permita rularea de comenzi text cat si realizarea facila de scripturi pentru a automatiza diverse actiuni cat si pentru a automatiza instalarea aplicatiei pe o platforma noua.
- Sistemul sa ofere interfata de autoadministrare pentru utilizatori.
- Sistemul sa ofere protocoale de acces la casuta postala: POP, IMAP, WEB plus protocolul MAPI pentru integrare cu clientul de mail.
- Sistemul sa ofere unelte de jurnalizare si arhivare la nivel global sau pentru un numar restrans de utilizatori, sa afere capabilitate utilizatorului sa isi arhiveze singur e-mailurile.
- Sistemul sa ofere interfata de autoadministrare pentru utilizatori, astfel incat utilizatorii sa poata realiza urmatoarele sarcini pentru gestiunea casutei postale: resetare parola, reguli de gestiune a mesajelor, sa schimbe apartenenta la grupuri de distributie, sa poata face cereri de a deveni membru la grupuri de distributie, setare Out-of-office cu customizare mesaj de auto-raspuns, sa poata obtine rapoarte de livrare mesaje dupa diverse criterii, posibilitatea de a seta limba pentru interfata de utilizare (Romana sau alte limbi).

Se vor oferi licentele de utilizare a platformei de mesagerie dimensionate dupa necesitati si care sa sustina lucrul celor 275 utilizatori interni ai sistemului e-VIZA.

2.3.1.12 PLATFORMA PENTRU RECUNOASTEREA SEMNATURII OLOGRAFE

Solutia va include o platforma pentru recunoasterea semnaturii olografe in scopul asigurarii unei protectii sporite in zona utilizatorilor interni cu drept de administrare de continut (adaugare/stergere/modificare) in cadrul Portalului e-VIZA. Acest continut vizeaza domenii precum legislatia in domeniu, instructiuni de utilizare a Portalului, informatii utile pentre aplicanti, date cu caracter personal etc. Platforma va solicita astfel acestor utilizatori, in mod suplimentar, semnatura olografa la fiecare incercare de autentificare cu nume utilizator si parola.

Aceasta platforma va asigura urmatoarele functionalitati de baza:

- Inregistrarea utilizatorilor in sistem prin stocarea in sistem de la utilizatori a unui numar de specimene efectuate cu pixul electronic.
- Recunoasterea semnaturii (la accesul in sistem) utilizatorilor (semnatura originala) efectuata cu acel tip de pix electronic.
- Respingerea incercarilor de frauda prin imitarea semnaturii corecte a unui utilizator (adica respingerea accesului la semnalarea semnaturilor false).
- Nivelul de respingere a semnaturilor false sa fie apropiat de 100%.

Se vor oferi licentele de utilizare a platformei software pentru recunoasterea semnaturii olografe cu suport pentru minimum 2 utilizatori cu drept de administrare de continut in Portalul e-VIZA astfel ca procesul de recunoasterea a semnaturii olografe sa se poata efectua cu succes incepand cu prima zi a perioadei Go-Live a proiectului.

2.3.1.13 PLATFORMA DE MANAGEMENT PENTRU CONSTRUCTIA MODULARA A IMAGINILOR SISTEM

Platforma de management oferita pentru constructia modulara a imaginilor sistem va indeplini urmatoarele cerinte tehnice :

2.3.1.13.1 COMPONENTE SI OBIECTIVE OPERATIONALE

Componente :
Solutia va include, respectiv:
- Componenta de management al instalarii sistemelor de operare si a aplicatiilor software;
- Componenta pentru managementul platformelor software de tip server.

Obiective operationale :
- administrarea tuturor serverelor de la o singura consola centrala web ;
- asigurarea vizibilitatii asupra resurselor IT asociate si a controlului asupra ciclului de viata al acestora ;
- reducerea efortului necesar pentru asigurarea suportului, imbunatatirea calitatii serviciului si a SLA-urilor;
- reducerea costurilor cu crearea imaginilor sistem, respectiv cu instalarea si/sau migrarea acestora ;
- automatizarea proceselor manuale;
- consolidarea, optimizarea si standardizarea procedurilor ;
- reducerea perioadelor de indisponibilitate neplanificata datorate erorilor, sau inconsistentei, in configurare, sau erorilor umane .

2.3.1.13.2 COMPONENTA DE MANAGEMENT A INSTALARII SISTEMELOR DE OPERARE SI A APLICATIILOR SOFTWARE:

Solutia va asigura suportul pentru programele de instalare si de administrare a platformelor de tip server. Ea va permite instalarea sistemelor de operare, migrarea configuratiilor, precum si a programelor software de aplicatie pentru o multitudine de platforme hardware si sisteme de operare, inclusiv Microsoft Windows 7, Windows Server 2008, Linux etc. Pentru aceasta este nevoie de o componenta de management a instalarii sistemelor de operare si aplicatiilor software care va indeplini urmatoarele functionalitati :

Functionalitati :
- Permite instalarea pe scara larga a imaginilor software de sistem, in maniera independenta de platformele hardware, pe baza unor configuratii standardizate de referinta ;
- Permite configurarea fiecarui sistem pe baza de criterii standardizate, inclusiv referitoare la profilul sau rolul utilizatorilor, sau la datele locatiei de instalare si functionare a sistemului ;
- Ofera criterii de selectie si mecanisme integrate de filtrare pentru definirea optima a grupurilor dinamice de sisteme tinta ;
- Permite crearea facila si executarea neasistata de operator de scenarii de automatizare a activitatilor specifice pentru pentru situatii de prelevare de imagini sistem existente, respectiv pentru instalarea pe scara larga (deployment) sau configurarea si migrarea instalarilor parametrizate (scripted) ale

sistemelor de operare si ale programelor software de aplicatii ;

- Activitatile configurate si programate, politicile de control al accesului respectiv aplicabile, imaginile sistem si pachetele software respectiv necesare vor putea fi sincronizate automat intre toate sistemele de management implicate ;
- Sistemul va permite raportarea in timp real a progresului instalarilor, cu indicarea task-urilor puse in asteptare, respectiv a duratei de asteptare, precum si a celor intrerupte sau esuate ;
- Accesul la resursele specifice va fi asigurat exclusiv pentru operatorii autorizati, iar managementul politicii respectiv aplicabile va putea tine seama de rolul efectiv asumat / delegat operatorului autorizat, de definirea sarcinilor respectiv autorizate, precum si de definirea sistemului pe care se autorizeaza instalarea / configurarea ;

2.3.1.13.4 COMPONENTA DE MANAGEMENT A PLATFORMELOR DE TIP SERVER

Solutia necesita o componenta de management a serverelor fizice si a instantelor server virtualizate, care va permite instalarea, configurarea si controlul administrativ al acestora de la o consola centrala. Aceasta componenta va oferi urmatoarele functionalitati :

Functionalitati de baza:

- Suport pentru multiple sisteme de operare, inclusiv pentru inventarul si managementul componentelor hardware si software, precum si monitorizarea proactiva a parametrilor cheie ai acestora.
- Posibilitatea de descoperire automata a inventarului efectiv de componente si, respectiv de catalogare a informatiilor specifice, la nivel de server, atat pentru echipamentele fizice, cat si pentru instantele virtualizate.
- Integrarea de tehnologii de generare si de utilizare de imagini sistem, cu posibilitatea de a modifica (edita) offline si de a reutiliza imagini sistem existente.
- Automatizarea configuratiilor complexe asociate cu instalarea initiala si cu managementul post-instalare al serverelor, inclusiv in ceea ce priveste managementul out-of-band.
- Remedierea de la distanta a serverelor, prin instrumente integrate de monitorizare, de modificare si de control al configuratiilor, precum si de oprire si (re-) pornire a serviciilor.
- Monitorizarea centralizata a parametrilor cheie ai serverelor, cu posibilitate de reactie rapida de remediere administrativa a problemelor identificate.

Functionalitati - Instalarea si configurarea serverelor:

Platorma integrata de management pentru instalarea si configurarea pe scara larga a serverelor, inclusiv cu functionalitati specifice de:

- Suport pentru tehnologii PXE, scripturi de instalare parametrizate si cu posibilitati de administrare a acestora in mod multicast, pentru instalare si migrare de sisteme de operare server;
- Control al accesului la resursele specifice prin grupuri dinamice, definire a domeniului de aplicare a resurselor pe baza rolului asociat operatorului, raportare structurata.
- Asigurare a scalabilitatii platformei de management, inclusiv prin organizarea ierarhica si replicarea multi-site a resurselor, automatizarea procesarii de arbori de decizie in aplicarea politicilor configurate.
- Capacitatea de a combina activitatile specifice de instalare, configurare si alocare a resurselor hardware si software, cu orice alte activitati de management.

Functionalitati - Vizualizarea resurselor administrate :

Consola grafica consolidata de vizualizare a resurselor cheie ale serverelor, pentru a permite:

- Vizualizarea, in timp real, a gradului de utilizare a procesorului, a memoriei active (RAM), a spatiului ocupat pe discuri, a efortului de procesare I/O si a consumului de resurse de retea, pentru fiecare server administrat.
- Completarea perspectivei asupra resurselor sistem, prin integrarea informatiilor despre topologia resurselor de retea relevante.
- Adoptarea rapida si eficienta de decizii imediate de remediere a situatiilot sub-optimale, pe baza indicatorilor de stare a componentelor cheie ale serverelor administrate.

Functionalitati - Managementul ciclului de viata al componentelor software :
Solutia ca include functiile specifice de suport pentru remedierea problemelor identificate, si de actualizare la versiunile curente, ale componentelor software ale solutiei, respectiv:

- Organizarea ierarhica si replicarea multi-site a pachetelor de modernizare si de remediere (patch);
- Mecanisme de generare rapida, asistata (wizard-based), a activitatilor de instalare a pachetelor de modernizare si de remediere;
- Capacitatea de remediere automata, pentru o multitudine de platforme server, inclusiv Windows, Linux si Unix;
- Capacitatea de a genera raportari sinoptice (dashboards) pentru a indica starea procedurilor de aplicare de pachete de modernizare si de remediere (patch) aflate in curs.

Functionalitati - Monitorizare si alertare :
Pentru monitorizarea administrativa a echipamentelor si a instantelor virtualizate de tip server, solutia oferita va include:

- Mecanisme de generare rapida, asistata (wizard-based), a politicilor de moitorizare a serverelor;
- Categorii pre-configurate de componente, inclusiv metrici specifice relevante, pentru o maxima eficienta a monitorizarii;
- Capacitatea de a opera in mod transparent si neintruziv, pentru anumite functii de inventariere de resurse si/sau de monitorizare, fara a folosi componente software rezidente (agenti) pe sistemele tinta;
- Optimizarea consumului de resurse de procesare si de resurse de comunicatie, prin posibilitatea de pre-selectare numai a acelor criterii specific relevante pentru monitorizare, la nivelul fiecarui server;
- Capacitate de auto-remediere a sistemului, prin mecanisme pre-configurate, declansate conditionat la aparitia de evenimente critice, sau la depasirea tolerantelor pre-stabilite la valorile parametrilor cheie;
- Consola de vizualizare centralizata a starii curente a sistemului, inclusiv a starii proceselor de remediere declansate, si care va putea regrupa componentele pentru indicarea starii de sanatate a acstora;
- Vizualizare a starii curente, dar si a evolutiei historice a datelor ce caracterizeaza stabilitatea si performanta sistemului;
- Posibilitatea de configurare specifica a calendarului de mentenanta de sistem pentru servere.

Totodata, componenta de management al platformelor de tip server va oferi si urmatoarele beneficii :

Beneficii :

- Sporirea eficientei activitatii administrative centralizate, inclusiv pentru un patrimoniu eterogen hardware si software.
- Reducerea incidentei erorilor prin automatizarea activitatilor de instalare si de configurare.
- Reducerea duratei de configurare si de implementare a serverelor, inclusiv prin utilizarea de configuratii standardizate pentru instalarea de la zero (bare-metal) a unor multiple tipuri de servere.
- Marirea disponibilitatii operationale, cu suport pentru remediere dinamica (patching) a configuratiilor software care ruleaza pe serverele administrate.
- Micsorarea intreruperilor neplanificate ale serviciilor sustinute, prin monitorizarea proactiva a starii serverelor administrate.
- Imbunatatirea parametrilor MTTR (Mean Time To Recovery or Mean Time To Repair) prin utilizarea instrumentelor de management centralizat incluse in solutie.

Se vor oferi licentele de utilizare a platformei de management pentru constructia modulara a tuturor imaginilor din sistemului e-VIZA.

2.3.1.15 Platforma de detectie pro-activa de malware prin metode de reverse engineering dinamic

2.3.1.15.1 Obiectiv operational

Solutia trebuie sa sigure protectia continua a sistemelor pentru asigurarea integritatii mediului de lucru, inclusiv pentru contracararea atacurilor avansate, directionate, precum si a celor coordonate, bazate pe retele

de tip bot-net. Solutia trebuie sa permita o reactie rapida, in timp real, si sa micsoreze semnificativ dependenta de investigatii costisitoare post-incident.

2.3.1.15.2 FUNCTIONALITATI

Solutia trebuie sa includa capacitate de detectie a atacurilor avansate, capacitate de raspuns rapid in caz de incident de securitate, precum si mijloace tehnice de contracarare.
In acest scop, solutia va permite:

- detectia si modelarea eficienta a vulnerabilitatilor identificate si a riscurilor care pericliteaza integritatea datelor;
- In plus, la detectarea prezentei unor vulnerabilitati, sau a unor atacuri, pe oricare din statiile protejate, solutia va permite declansarea automata, pe toate statiile de lucru protejate din sistem, a unor scanari pentru identificarea specifica a simptomelor unor posibile atacuri.

Solutia trebuie sa permita scanarea statiilor pentru semnalarea indiciilor tipice de compromitere a securitatii acestora.
In acest scop:

- Solutia include o biblioteca, constant actualizata, de indicatii specifice cunoscute, care tin de simptomatica atacurilor, care permite identificarea rapida a artefactelor digitale specifice prezentei acestora, in orice sistem a carui securitate a fost compromisa.
- Solutia va permite extinderea si particularizarea seturilor de date specifice din biblioteca de referinta, pe baza datelor unice specifice care tin de atacurile identificate si catalogate in sistemele locale protejate.
- Solutia va permite scanari detaliate pentru a identifica si cataloga pana si cele mai fine alterari — la nivel de atribute respectiv pentru: fisierele de date, fisierele executabile, cheile de cataloage sistem (registry), informatia martor de eveniment sistem sau de securitate — care vor putea fi corelate.
- Tiparele de cautare necesare vor putea fi aplicate programatic, respectiv pe datele culese din:
    - memoria activa (RAM);
    - structurile de date identificate si artefactele extrase din analizele pe fisiere binare;
    - datele brute extrase la nivel de sistem de fisiere (e.g. NTFS);
    - tabele de intializare a sistemului (MBR, sau asimilate);
    - fisiere obiect, fie ca sunt in uz, sau chiar blocate administrativ;
    - orice alte obiecte, sau referinte la obiecte accesibile, precum si date obtinute prin interogari structurate pe baza structurilor de acces functional de tip Win API si asimilate.
- Scanarile vor putea include ca tinta, sau ca factori de filtrare sau praguri conditionale, orice indicatori sau referinte obtinute din (sau relative la):
    - structuri de tip sir specifice, de cod malitios;
    - valori ale unor chei de catalog sistem (registry);
    - cai de acces la fisiere;
    - dimensiuni de fisier;
    - marci de timp;
    - masti generice;
    - expresii regulate asimilate.
- Operatorii vor putea defini cu usurinta, direct in interfata utilizator, diverse scanari particularizate pentru identificarea de simptome specifice de vulnerabilitate si de atac, simple sau complexe, prin generarea de expresii, interogari si filtre logice de tip AND/OR.

Solutia trebuie sa permita determinarea eficienta a modului specific de actiune pentru atacurile detectate si conducerea de investigatii coordonate, in timp real, la nivelul intregului sistem protejat, pentru a permite intelegerea tacticilor si a tehnicilor specifice atacurilor identificate.
In acest scop :

- Solutia va dispune de o interfata centralizata care va permite coordonarea activitatilor:
    - detectie automata prin scanari neasistate programate;

- investigatii la nivel de memorie (RAM) si de disc (HDD);
- analiza si deconstructia (reverse-engineering) a codului de tip malware identificat;
- corelarea si analiza evenimentelor sistem catalogate si a incidentelor semnalate.

- Functionalitatile solutiei vor permite:
  - identificarea rapida a statiilor a caror integritate si securitate au fost compromise;
  - determinarea eficienta a punctelor initiale de infectare;
  - determinarea specifica a interactiunii codului malitios cu sistemul (statia) gazda atacat, precum si
  - identificarea si catalogarea artefactelor digitale generatoare (cod malitios, date si configuratii, etc.) sau obiect (respectiv generate de codul malitios).

2.3.1.15.3 ARHITECTURA SOLUTIEI

Cerinte administrative:

Solutia va oferi urmatoarele facilitati:

- administratorii de sistem vor putea programa scanari la nivel de statie de lucru, precum si analize automate, direct din interfata web;
- operatiile programate se vor executa pe statiile tinta prin intermediul agentilor respectiv instalati;
- componenta agent, rezidenta pe terminalul protejat va putea fi instalata ca serviciu, dar va putea fi rulata si in mod interactiv, in linie comanda;
- arhitectura si modelul flexibil de licentiere a solutiei vor permite atat protectia proactiva, prin agenti instalati permanent pe echipamentele compatibile, cat si reactia rapida specifica la incidente de securitate, pe terminalele tinta;
- rezultatele scanarilor si ale analizelor, de la nivelul tuturor statiilor protejate, vor fi colectate rapid in baza de date centralizata a sistemului;
- analiza si corelarea datelor va fi insotita de marcarea terminalelor a caror integritate sau securitate sunt considerate compromise, de identificarea modulelor software considerate a prezenta trasaturi specifice malware, respectiv de descrierea modului specific de actiune si de elementele caracteristice de tip metadata disponibile;
- operatorii vor putea identifica, cu usurinta, inclusiv indicatorii de severitate a riscului de securitate si modul specific;
- serverul central al solutiei va putea arhiva istoricul alertelor, programe care prezinta elemente de structura si de actiune tipice codului malware, precum imagini ale memoriei active de pe sistemele analizate;
- toate comunicatiile, respectiv atat pe bucla de comanda si pe cea de reactie (feedback), intre agenti si serverele centrale de management al solutiei se vor efectua in mod comprimat si protejat criptografic prin mecanisme de tip HTTPS. Utilizand aceasta informatie solutia va permite generarea automata de semnaturi de atac, care vor include profile si tipare de actiune multiple, ceea ce ve permite imbunatatirea permanenta a capacitatii sistemului de a se adapta la atacuri si de a ameliora permanent postura generala de securitate a acestuia.

Solutia trebuie sa implementeze o arhitectura cu impact minim asupra sistemelor protejate si a retelelor in care acestea sunt integrate.

Sisteme de operare suportate pe statiile de lucru protejate:

- Windows Server 2000 ;
- Windows XP ;
- Windows Server 2003 ;
- Windows Vista;
- Windows Server 2008/R2 ;
- Windows 7, respectiv atat versiunile 32-bit, cat si cel 64-bit.

Se vor oferi licentele de utilizare a platformei de detectie pro-activa de malware prin metode de reverse engineering dinamic care sa sustina lucrul a celor 275 de utilizatori interni ai sistemului e-VIZA.

2.3.2 COMPONENTE SOFTWARE TIP CLIENT - STATII DE LUCRU

2.3.2.1 Componenta software tip sistem de operare desktop

- Toate statiile de lucru de la posturile consulare vor fi livrate cu minim sistem de operare tip Windows 7 Professional OEM sau echivalent

Se vor oferi licentele de utilizare a platformei software tip sistem de operare desktop pentru 275 utilizatori interni ai Sistemului e-VIZA.

2.3.2.2 Componenta software desktop tip Office si mesagerie electronica

Autoritatea contractanta va pune la dispozitia furnizorului licentele pentru instalarea pachetelor tip Office si mesagerie electronica

2.3.2.3 Client pentru autentificarea multi-factor

Sistemul e-VIZA va implementa autentificarea multi-factor printr-o solutie formata dintr-un echipament token tip Smart Card (descris la capitolul 2.4.2.2 – « Echipament token tip Smart Card ») si clientul (software) pentru autentificarea multi-factor.
In configuratia livrata, solutia trebuie sa dispuna de urmatoarele functionalitati:

- Sa permita extinderea aplicatiilor de securitate prin folosirea capabilitatilor JAVA integrate ;
- Sa permita etichetarea facila ;
- Sa poata fi folosit in aplicatii bazate pe certificate de tipul :
  - Autentificare in medii pre-boot;
  - Acces la distanta prin VPN;
  - Autentificarea utilizatorilor in sistemele de operare :
    - Windows,
    - Linux,
    - MacOS X.
  - Autentificarea in retea;
  - Managementul parolelor;
  - Semnarea digitala a documentelor si aplicatiilor ;
  - Criptare si decriptare.

Se vor oferi licentele de utilizare a clientului pentru autentificarea multi-factor pentru 275 de utilizatori interni ai sistemului e-VIZA.

2.4 Cerinte privind echipamentele hardware

2.4.1 Echipamente hardware tip server

2.4.1.1 Platforme de procesare tip server

2.4.1.1.1 Server de procesare

Pentru procesare solutia prevede echipamente de tip Blade pe arhitectura x86_64, sau asimilata. Fiecare din aceste echipamente va avea urmatoarea configuratie minima:

Sasiu Blade
Arhitectura hardware
Sasiu:
Serverele blade trebuie sa fie instalate intr-un sasiu rack-abil, cu urmatoarele caracteristici minimale:

- Dimensiuni maxime: 10 U
- Sistemul trebuie sa suporte blade-uri dual si quad socket cu procesoare Xeon Quad, Hexa si Eight Core.

- Sursele de curent trebuie sa fie in numar de minimum 4 cu redundanta (capabile sa asigure consumul de curent al sasiului la echiparea maximum posibila).
- Sasiul trebuie sa poate acomoda cel putin 8 switch blade-uri de tip Ethernet, Fiber Channel, Infiniband, SAS.

Interfete I/O:

- Implementarea fizica a conexiunilor trebuie realizata printr-un 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. Aceasta functionalitate trebuie sa poata fi activata ulterior prin licente software.
- Interfetele I/O trebuie sa fie consolidate cu ajutorul a minim 4 switch blade-uri (pentru redundanta) intr-un numar de porturi externe dupa cum urmeaza:
  - minimum 12 porturi Ethernet Gigabit impartite pe minim 2 switch-uri pentru redundanta.
  - minimum 12 porturi Fiber Channel impartite pe minim 2 switch-uri pentru redundanta
  - minimum 1 x port VGA, 4 x port USB
  - minimum 2 porturi seriale redundante si 2 porturi Ethernet redundante dedicate pentru management..
- Arhitectura sistemului trebuie sa permita implementarea unor solutii de Load Balancing si FailOver pentru porturile de Ethernet si Fiber Channel

<u>Administrare</u>

Interfata de management centralizat:

- Sistemul trebuie sa beneficieze de o interfata de management centralizat capabila sa administreze si sa controleze toate resursele si mecanismele integrate:
  - blade-uri (masini fizice)
  - interfete I/O
- Sistemul trebuie sa suporte adaugare si integrarea ulterioara a blade-urilor, toate putand fi controlate de la aceeasi interfata de management
- Interfata de management trebuie sa fie instalata pe o resursa hardware dedicata si complet redundanta, alta decat blade-urile solicitate a fi instalate. Fiecare modul de management trebuie sa ofere minimum 1 porti Ethernet (RJ-45)
- Interfata trebuie sa fie accesibila cu o consola si ca serviciu WEB pe porturile dedicate

Se vor include in oferta 2 echipamente tip sasiu blade, in configuratie identica.

Server tip Blade

Procesor	2 procesoare instalate tip Six Core Intel Xeon 2.66 GHz (12MB Third Level Cache ECC) 6.4GT, bus QPI, 1333Mhz FSB, sau echivalent
Memorie cache (TLC)	12 MB
Memorie RAM	mnimum 192 GB DDR3 1333, PC3-10600 SDDC instalata; Suport pentru protectie de tip memorie in oglinda (memory mirroring) Suport pentru protectie memorie de tip rezerva calda (hot spare memory)
Interfata retea	minimum 4 porturi 1Gbit/s Ethernet
Interfata fibra optica	minimum 2 porturi x 8Gb/s
Sloturi	2 x slot-uri pentru expansiune (conectivitate dupa standardul PCI-Express Gen2 x8)
Hard disk	2 x SAS 300 GB interne, controller SAS RAID 0,1

Interfata video	Integrata, minimum 16 Mb memorie video
Management	Aplicatie de management operational dezvoltata de producatorul sistemului de calcul, cu functii de monitorizare a starii sistemului, management al evenimentelor si alarmelor, diagnoza si analiza performantei, inventar al componentelor, up-date-urilor si patch-urilor. Chipset pentru remote management integrat compatibil IPMI 2.0 cu acces prin web browser cu securizare prin criptare SSL 128 bit
Compatibilitate cu sisteme de operare	Microsoft® Microsoft® Hyper-V™ Server 2008 R2 Microsoft® Windows Server® 2008 R2 Datacenter, Enterprise, Standard Microsoft® Windows HPC Server® 2008 R2 Suite Microsoft® Windows® Small Business Server Standard 2011 Microsoft® Windows® Server 2008 Datacenter, Enterprise, Standard Microsoft® Windows Server® 2003 Enterprise Edition Microsoft® Windows Server® 2003 Standard Edition VMware vSphere™ Red Hat® Enterprise Linux 6, 5, 5 with XEN

- Se vor include in oferta 15 echipamente server tip blade, in configuratie identica.

2.4.1.2 SERVER DE STOCARE MULTIPROTOCOL

Pentru partea de stocare a datelor, solutia prevede echipamente tip server de stocare - sistem de stocare de tip SAN/NAS. Fiecare din aceste echipamente va indeplini urmatoarele cerinte tehnice minime:

- Echipamentul trebuie sa fie echipat cu doua controller-e in acelasi spatiu din rack pentru a putea dispune de o configuratie redundanta de tip cluster la nivelul echipamentului.
- Echipamentul trebuie sa permita scalarea la minim 136 de discuri cu conectare de tip Serial SCSI(FC sau SAS) sau SATA.
- Echipamentul trebuie sa permita utilizarea in paralel a discurilor de tip FC 4Gb/s, SAS 3Gb/s si SATAII minimum 3Gb/s.
- Capacitatile pentru un HDD minim disponibile trebuie sa fie de 2TB pentru discurile SATA si 600GB pentru cele FC/SAS.
- Minim 4 GB memorie cache instalati si utilizabili pe sistemul de stocare. Memoria Cache trebuie sa fie protejata cel putin cu acumulatori (baterie). In configuratie dual controller capacitate maxima de memorie cache trebuie sa fie de minim 8GB.
- Minim 1 Procesor pe fiecare controller.
- Sistemul trebuie sa permita conecatarea atat in standard File Access(NAS) cat si in standard Block Access(SAN) in acelasi timp.
- In configuratia livrata echipamentul trebuie sa fie echipat cu cel putin 4 porturi Ethernet cu o latime de banda de 1 Gb/s si minim 2 porturi FC cu o latime de banda de minim 4 Gb/s.
- Echipamentul trebuie sa suporte utilizarea in paralel a urmatoarelor protocoale de acces si comunicatie:
  - NFS,
  - CIFS,
  - FTP,
  - iSCSI,
  - HTTP,
  - FC.

- Echipamentul trebuie sa ofere posibiitatea de a utiliza nivele avansate de management al datelor si volumelor cel putin pentru urmatoarele platforme/aplicatii (metoda/aplicatia de integrare si management al aplicatiilor trebuie sa fie produsa de producatorul echipamentului):
  - SQL,
  - Oracle,
  - Exchange,
  - VmWare Virtual Infrastructure.
- Sistemul trebuie sa suporte conectarea prin protocolul FC la urmatoarele sisteme de operare:
  - Microsoft Windows,
  - AIX,
  - HP-UX,
  - Linux,
  - Oracle (SUN) Solaris.
- Echipamentul trebuie sa suporte realizarea copiilor de tip Snapshot precum si replicarea datelor la distanta in mod sincron si asincron. Replicarea datelor la distanta trebuie sa fie suportata atata cu echipamentele din aceeasi clasa cat si cu cele din clasa diferite(inferioare sau superioare ca performanta) produse de acelasi producator.
- Unitatile de expansiune cu discuri trebuie sa fie compatibile cu sisteme de stocare din clasa superioara(scalabilitate si performanta) in asa fel incat in situatia unui upgrade/migrari inlocuirea acestora sa nu fie necesara.

In configuratia livrata echipamentul trebuie sa dispuna de urmatoarele functionalitati:
- Realizarea copiilor de tip instantanee - Snapshot, si posiblitatea de restaurare foarte rapida a acestora fara mutarea datelor salvate in copia de tip Snapshot ci prin remaparea blocurilor de date.
- Trebuie sa ofere posibilitatea de a utiliza nuivele avansate de management al datelor si volumelor cel putin pentru urmatoarele platforme/aplicatii: SQL, Oracle, Exchange, VmWare Virtual Infrastructure. Metoda/aplicatia de integrare si management al aplicatiilortrebuie sa fie produsa de producatorul echipamentului.
- Licenta inclusa pentru configurarea si utilizarea volumelor accesabile prin protocol CIFS.
- Licenta inclusa pentru deduplicarea datelor.
- Configurarea si optimizarea matricilor RAID de tip RAID 4 sau RAID DP.
- Conectarea prin protocol iSCSI sa fie disponibila in configuratia initiala.
- Conectarea prin protocol NFS sa fie disponibila in configuratia initiala.
- Sistemul trebuie sa fie echipat in configuratia livrata cu un numar suficient de hardiskuri SATA, pentru asigurarea unei capacitati utile sistemului e-VIZA de minimum 120 TB;

Se vor include in oferta 2 echipamente tip server de stocare multiprotocol, in configuratie identica.

2.4.1.3 ECHIPAMENTE TIP GATEWAY DE PROTECTIE MULTIMODALA

Solutia prevede pentru partea de firewall echipamente gateway integrat de protectie multimodala. Fiecare din aceste echipamente va indeplini urmatoarele cerinte tehnice minime:
- Sa reprezinte o platforma hardware dedicata cu sistem de operare propriu.
- Sa ofere protectie impotriva atacurilor de tip Denial Of Service;
- Sa ofere protectie impotriva atacurilor pe baza de pachete de date fragmentate;
- Sa ofere protectie impotriva scanarilor neautorizate de porturi/aplicatii/servicii.
- Sa permita crearea de politici unice pentru traficul SSL VPN.
- Sa suporte split tunneling pentru a controla accesul clientilor.
- Sa ofere functionalitate NAT.
- Sa ofere functionalitate VLAN la nivelul 2 si 3 OSI.
- Sa suporte minim protocoalele de rutare OSPF si RIP versiunea 2.
- Sa ofere functionalitate de server DHCP precum si de relay DHCP.
- Sa suporte agregarea conexiunilor conform standardului 802.3ad.

- Sa permita controlul traficului pe baza de politici de aplicatie, categorie de aplicatii, subcategorie, tehnologii, factor de risc sau caracteristicile aplicatiilor.
- Sa permita controlul traficului pe baza de politici de utilizator, grup de utilizatori sau adresa IP.
- Sa permita identificarea aplicatiilor independent de port, protocol, criptarea SSL.
- Sa foloseasca politici predefinite/definibile pentru utilizarea aplicatiilor in retea.
- Sa permita modelarea traficului in retea (garantat, maxim si prioritar) pe baza politicilor de aplicatie predefinite/definibile, cat si pe baza politicilor de utilizator, sursei, destinatiei, interfata de comunicatie, tunel VPN Ipsec, etc.
- Sa permita vizibilitate si control asupra utilizatorilor si a aplicatiilor pe care acestia le folosesc, pe baza politicilor predefinite/definibile si prin integrarea cu un sistem de tip director.
- Sa monitorizeze sesiunile de autentificare ale utilizatorilor pentru a face corelarea adreselor ip cu utilizatorii si grupurile de utilizatori
- Sa mentina o tabela de corelare a utilizatorilor si grupurilor de utilizatori cu rolurile lor de acces fara a fi nevoie de instalarea de agenti pe statiile client.
- Sa asocieze utilizatorii cu adresele ip prin intermediul unui formular web in cazul in care utilizatorii nu fac parte din domeniul intern al retelei.
- Sa permita crearea de politici ce detecteaza si inspecteaza accesul si utilizarea serviciilor de webmail si mesagerie instanta.
- Sa permita controlul transferului de fisiere direct in aplicatii independente fara a limita accesul la aceste aplicatii.
- Inspectia fisierelor sa se faca prin inspectarea tipului de continut din fisiere si nu prin recunoasterea extensiilor folosite de aceste fisiere.
- Sa se poata crea politici de tip Quality Of Service pentru a permite si controla traficul aplicatiilor media.
- Sa ofere functionalitate IPS prin detectia anomaliilor la nivel de protocol cat si prin detectia anomaliilor statistice la nivel de pachete de date.
- Sa ofere analiza heuristica a traficului si sa blocheze pachetele ne-valide.
- Producatorul platformei firewall sa aiba/mentina baze proprii de date cu amenintarile informatice cat si cu tipul si continutul adreselor web.
- Sa foloseasca un sistem unificat de semnaturi la nivelul tuturor tipurilor de amenintari informatice.
- Toate politicile definite in sistem sa fie centralizate/unitare indiferent de tipul lor si scopul de aplicare.
- Sa identifice aplicatiile folosite de utilizatori in sesiunile de acces la distanta Citrix si RDP.
- Sa permita controlul sistemelor non-Windows prin autentificare web.
- Sa protejeze impotriva amenintarilor de tip malware.
- Sa limiteze/blocheze transferul neautorizat de fisiere.
- Sa suporte controlul si filtrarea continutului web in interiorul retelei.
- Sa permita blocarea traficului mare consumator de latime de banda de tip P2P/torrent.
- Sa identifice si blocheze incercarile de a folosi servicii de tip proxy externe.
- Functionalitatea IPsec VPN sa permita criptare AES pe 256 biti precum si autentificare SHA1 si MD5.
- Sa permita configuratii activ/pasiv.
- Sa permita sincronizarea configuratiei si sesiunilor intre mai multe echipamente.
- Toata detectia si analiza traficului trebuie sa se faca intr-un singur pas pentru maximizarea performantelor si minimizarea latentei.
- Sa monitorizeze in permanenta starea si calea legaturii IP intre echipamente.
- Administrarea sa se poata face atat prin consola cat si prin aplicatie de administrare dedicata.
- Sa permita administrarea bazata pe roluri administrative.
- Aplicatia de administrare dedicata sa permita partajarea politicilor.
- Interfata cu utilizatorul (administratorul) sa permita vizualizarea traficului aplicatiilor.
- Sa permita crerea de filtre si rapoarte pentru aplicatiile folosite, adresele web scanate si filtrate, filtrarea traficului, si actvitatea factorilor de amenintare/risc.

- Rapoartele sa poata fi exportate in format csv si pdf si sa poata fi trimise pe e-mail automat conform unor politici predefinite/definibile.
- Sa permita inregistrarea si auditul tuturor sesiunilor si pachetelor ce traverseaza reteaua.

In configuratia livrata echipamentele trebuie sa beneficieze de urmatoarele caracteristici:

- Capacitatea de procesare a firewall-ului sa fie de minim 250 Mbps.
- Capacitatea de procesare si detectie a amenintarilor sa fie de minim 100 Mbps.
- Numarul de tunele Ipsec VPN sa fie de minim 250.
- Sa suporte minim 64000 de sesiuni simultane.
- Numarul de conexiuni VPN SSL suportate sa fie de minim 100 simultan.
- Sa ofere minim 8 interfete Gigabit Ethernet.
- Sa ofere minim 1 interfata Gigabit Ethernet dedicata functiilor de management.

Se vor include in oferta 2 echipamente tip gateway integrat de protectie multimodala si balansare a incarcarii, in configuratie identica.

2.4.1.4 Echipamente tip Switch L2+ integrate in structura de tip stiva

Solutia prevede pe partea de retelistica echipamente tip switch L2+ integrate in structura de stiva.
Fiecare din aceste echipamente care vor indeplini urmatoarele cerinte tehnice minime:

- Echipamentele reprezinta module sau echipamente dedicate, in configuratie redundanta pentru interconectare LAN, respectiv (cel putin) 2x module switch a cate 24 porturi 10/100/1000Mbps fiecare si, respectiv cu cate 2 porturi modulare de uplink 10 Gigabit, care sa poata fi echipate fie cu conector extern electric sau cu transceiver optic.
- Modulele de interconectare LAN oferite vor fi echipate complet pentru a oferi efectiv posibilitatea de configurare in mod stack, pe bus independent (cu interconectare pe port/conector dedicat), respectiv cu disponibil de banda destinat comunicarii intre module distinct si independent de resursa alocata pentru comunicarea interna (intre porturile de retea ale fiecarui modul), si capacitate de configurare de tip cross-stack pentru support de link-uri normale sau de tip port agregat (trunk, sau agregat).
- Caracteristicile de performanta vor asigura functionarea la un nivel adecvat aplicatiei de portal, respectiv pentru capacitatea de forwarding (cel putin 75Gbps pentru porturile de acces ale fiecarui modul, si 15Gbps pentru magistrala de stack), pentru rata de forwarding (min.) 50mpps si capacitatea totala de switching de (min.) 175Gbps.
- Administrarea interconectarii LAN se va putea face atat la nivel de element, cat si la nivel de structura stack.
- Modulele vor dispune de interfete dedicate de administrare securizata (inclusiv SSH, Kerberos, SNMP v3) in mod consola, locala sau distanta, precum si de capacitatea de configurare a unor partitii (VLAN, sau asimilate, inclusiv IEEE 802.1Q) care sa poata include porturi din module diferite.
- Modulele vor asigura protectia porturilor de acces, inclusiv prin suport specific pentru protocoale de control al accesului pe baza de descriptor MAC sau de identitate logica (IEEE 802.X si asimilate).
- Pentru protectia functiilor administrative, vor fi disponibile mecanisme de autentificare si autorizare (inclusiv RADIUS si asimilate), precum si mecanisme de tip acces pe multiple nivele de securitate.
- Pentru asigurarea continuitatii operationale, modulele vor dispune de:
    - mecanisme logice standardizate pentru asigurarea convergentei (STP sau asimilate, inclusiv IEEE 802.1D, IEEE 802.1s, IEEE 802.1w etc.),
    - interfete fizice calibrate pentru convergenta rapida (nu mai mult de 100ms).

Se vor include in oferta 2 echipamente tip Switch L2+ integrate in structura de tip stiva, in configuratie identica.

2.4.1.5 Echipamente solutie criptografica tip HSM

Solutia prevede pentru partea de criptografie echipamente criptografice tip HSM. Fiecare din aceste echipamente va dispune de cate un modul hardware pentru suport criptografic destinat procesarii rutinelor specifice pentru functionalitatile de securitate integrate in portal, care indeplineste urmatoarele cerinte tehnice minime:

- asigura generarea si procesarea cheilor in hardware;
- asigura, exclusiv pentru utilizatorii autorizati procesarea transparenta a criptarii si decriptarii, respectiv a rutinelor de amprentare criptografica si/sau de semnare digitale in hardware;
- proceseaza nativ rutine de cifru asimetric, respectiv pe baza de algoritmi standard:
  - DSA;
  - Diffie-Helman;
  - RSA (512-4096bit);
  - ECDSA (512bit).
- proceseaza nativ rutine de cifru simetric, respectiv pe baza algoritmilor standard:
  - AES 256;
  - 3DES.
- proceseaza nativ rutine de amprentare criptografica si de certificare de integritate, pe baza algoritmilor standard:
  - SHA-1;
  - SHA-256;
  - SHA-512;
  - RIPEMD160.
- asigura un nivel adecvat de performanta tipica:
  - (minim) 200 de operatii de executare de semnatura RSA cu chei de 1024bit pe secunda;
  - scaleaza natural in configuratii multicomponenta.
- permit asigurarea nivelului dorit de continuitate operationala si de distributie de sarcina, respectiv:
  - suporta mecanisme specifice de echilibrare de sarcina, cum ar fi distributia intre noduri identice, la nivel de sistem de operare, si preluare de sarcina (fail-over) la nivel de aplicatie.
- implementarea componentelor criptografice ale acestor module vor fi certificate, respective cel putin:
  - FIPS 140-2 Level 3.

Se vor include in oferta echipamente criptografice tip HSM, in configuratie identica din care sa rezulte un numar de 6 partitii criptografice.

2.4.1.6 SERVERE NTP/SNTP

Pentru partea de sincronizare a ceasurilor serverelor solutia prevede integrarea cu echipamentele tip server NTP/SNTP impreuna cu platforma software aferenta. Fiecare din aceste echipamente va indeplini urmatoarele cerinte tehnice minime:

- Sa permita operarea Stratum 1 prin folosirea de sateliti GPS.
- Sa permita operarea Stratum 2 prin folosirea altor servere de timp ca sursa de timp.
- Sa ofere o acuratete la nivel de nanosecunda fata de UTC.
- Sa ofere conectivitate TCP/IP atat prin protocol IPv4 cat si prin protocol IPv6.
- Sa permita configurarea cu adrese ip statice dar si obtinute de la un server DHCP.
- Sa permita administrarea prin interfata web securizata cu certificat SSL.
- Sa permita administrarea de la distanta prin protocol SSH, SCP si Telnet.
- Sa permita managementul prin retea folosind protocolul SNMP versiunea 3.
- Producatorul sa ofere MIB-uri SNMP pentru integrarea facila in unelte de administrare bazate pe SNMP.
- Sa ofere alertarea pe e-mail pentru alarme si erori.
- Sa dispuna de porturi USB.
- Sincronizarea de timp prin intermediul satelitilor GPS sa se faca folosind chiar si un singur satelit.
- Sa permita notificarea administratorilor in momentul disponibilitatii de noi update-uri.
- Sa permita update-ul facil direct din interfata web.
- Sa mentina un jurnal al tuturor operatiunilor efectuate, ata cele de sincronizare cu sursele de timp externe cat si cele de sincronizare a clientilor ce acceseaza serverul de timp. Deasemena trebuie sa mentina un jurnal al tuturor operatiunilor administrative efectuate asupra server-ului de timp.
- Interfata web sa asigure instrumente de asistenta in configurarea initiala a serverului de timp.

In configuratia livrata echipamentele trebuie sa dispuna de urmatoarele functionalitati:

- Sa permita pana la 3200 de cereri de timp pe secunda.
- Sa ofere minim 3 porturi Ethernet.
- Sa suporte urmatoarele protocoale de timp :
  - NTP Server (versiunile 2, 3 si 4),
  - SNTP, Time, Daytime,
  - NTP Peering/Client,
  - NTP Multicast Server/Client,
  - NTP Broadcast Server/Client.
- Sa suporte urmatoarele referinte de timp :
  - GPS,
  - NTP Peering.
- Sa ofere display frontal pentru afisarea datelor legate de sincronizarea ceasului si a metodei de sincronizare folosite.
- Sa ofere in partea frontala tastatura numerica pentru setarea facila si accesul in meniul de configurare si diagnostic.
- Sa ofere led-uri de status in partea frontala.
- Sa ofere un port de consola pentru administrarea locala.
- Sa nu permita o deviere de timp mai mare de 50 nanosecunde.

Se vor include in oferta 2 servere NTP/SNTP, in configuratie identica.

2.4.1.7 ECHIPAMENTE DE CRIPTARE/DECRIPTARE AUTOMATA LA NIVEL DE BAZE DE DATE SI SERVERE DE APLICATII CENTRALE

Pentru partea de criptare si decriptare a datelor la nivelul bazelor de date si serverelor de aplicatii, solutia prevede echipamente de criptare/decriptare automata la nivel de baze de date si servere de aplicatii centrale, impreuna cu platforma software aferenta. Fiecare din aceste echipamente va indeplini urmatoarele cerinte tehnice minime:

- Echipamentele de criptare/decriptare sunt dedicate cu modul hardware pentru protejarea si accelerarea operatiunilor criptografice la nivelul datelor generate de aplicatii.
- Sa permita managementul cheilor de criptare.
- Sa permita aplicarea de versiuni cheilor de criptare (Key Versioning) astfel incat sa se elimine necesitatea rotirii cheilor (Key Rotation).
- Sa ofere politici de acces si control granulare bazate pe definirea de roluri de acces.
- Sa permita criptarea datelor generate, stocate, partajate si accesate:
  - Aplicatiile de baze de date,
  - Aplicatiile ce folosesc date ce contin numere de carti de credit, adrese de e-mail si date cu caracter privat,
  - Aplicatii critice ce ruleaza pe mainframe-uri,
  - Aplicatii ce acceseaza directoare si fisiere localizate pe statiile de lucru, servere, share-uri si medii amovibile.
- Sa permita protejarea datelor generate si manipulate de aplicatii pe durata intregului ciclu de viata al acestor date.
- Sa ofere criptarea transparenta a datelor fara a produce un impact asupra acestor date sau a utilizatorilor si aplicatiilor ce manipuleaza datele.
- Sa permita criptarea integrala a disk-urilor din statiile de lucru, servere, laptop-uri precum si a mediilor amovibile.
- Sa ofere management centralizat pentru toate operatiunile de criptare indiferent si independent de aplicatiile ce genereza datele ce urmeaza a fi criptate.
- Sa permita definirea de politici de autentificare si autorizare ce definesc modul in care utilizatorii au acces la datele generate de aplicatii (in clar sau criptat).

- Sa ofere o singura interfata centralizata pentru operatiunile de logging, audit si raportare atat pentru datele acesate cat si pentru folosirea si administrarea cheilor de criptare, indiferent si independent de aplicatiile ce genereza datele.
- Criptarea sa se poata face granular atat la nivel de baze de date, cat si la nivel de fisiere, directoare, aplicatii, disk-uri si medii amovibile.
- Sa permita managementul prin retea folosind protocolul SNMP.
- Sa permita rotirea automata si semnarea digitala a log-urilor.
- Sa permita efectuarea de backup-uri securizate prin folosirea de semnatura digitala.
- Sa permita upgrade-ul facil.
- Sa ofere statistici exstinse.
- Sa permita administrarea prin interfata web, sesiune SSH, precum si prin consola locala.
- Sa suporte criptarea cu cheie asimetrica si schimbul de chei pentru urmatorii algoritmi criptografici :
    - RSA (de la 512-bit pana la 2048-bit).
- Sa suporte chei simetrice cu urmatorii algoritmi criptografici:
    - DES, 3DES (lunigimi duble si triple de chei),
    - RC-4,
    - AES.
- Sa suporte urmatoarele coduri de autentificare a mesajelor :
    - HMAC-SHA-1,
    - HMAC-SHA-512.
- Sa suporte urmatoarele API-uri :
    - .NET,
    - MSCAPI,
    - JCE,
    - ICAPI,
    - PKCS#11.
- Sa ofere suport pentru datele generate si manipulate de aplicatii bazate pe urmatoarele servere web si de aplicatie :
    - Oracle,
    - IBM,
    - BEA,
    - IIS,
    - Apache,
    - SUN One,
    - Jboss.
- Sa ofere suport pentru datele generate si manipulate de aplicatii bazate pe urmatoarele servere de fisiere :
    - Microsoft,
    - Red Hat Linux,
    - CentOS Linux.

In configuratia livrata echipamentele trebuie sa dispuna de urmatoarele functionalitati:

- Sa permita criptarea datelor generate, stocate, partajate si accesate de aplicatiile de baze de date pe durata intregului ciclu de viata al acestor date.
- Platforma unificata pentru criptarea datelor generate si stocate de catre aplicatiile de baze de date.
- Sa ofere suport pentru datele generate si manipulate de aplicatii bazate pe urmatoarele baze de date :
    - Oracle,
    - Microsoft SQL Server,
    - IBM DB2,
    - Teradata.
- Sa permita pana la 11000 de operatii de criptare pe secunda.

Se vor include in oferta 2 echipamente de criptare/decriptare automata la nivel de baze de date si servere de aplicatie centrale, in configuratie identica.

2.4.1.8 SISTEM CABINET PENTRU INTEGRAREA ECHIPAMENTELOR TIP SERVER

Echipamentele hardware tip server vor fi integrate, in functie de solutia oferita, intr-un sistem cabinet sau mai multe, ansamblul modular fiind dimensionat pentru un total de minim 42U utili. Se vor include reperele de montare necesare, inclusiv sine extensibile telescopic (sau solutii similare) cel putin pentru echipamentele complexe de natura nodurilor de procesare, in scopul de a permite accesul fizic facil la componentele interne de tip hot-plug / hot-swap (surse, ventilatoare, placi de extensie etc.) si deservirea acestora fara a fi necesara oprirea functionarii si/sau deconectarea echipamentului (ori de cate ori acest lucru este posibil din punct de vedere functional).
Fiecare sistem cabinet va indeplini urmatoarele cerinte tehnice minime :

Caracteristica	**Descriere**
Sursa neintreruptibile (UPS)	◷ Structura de alimentare de tip UPS va fi compusa din cel putin o unitate discreta redundanta independenta, de tip on-line dubla conversie, monofazata (1/1), respectiv de minimum 6KVA fiecare, echipata cu baterii care sa permita asigurarea unui nivel de uptime de minimum 20 minute la 70% incarcare. Se va asigura un nivel optim de disponibilitate operationala (cu un minimum de elemente active sau pasive care sa constituie single-point-of-failure); capacitatea preconizata si suportul de uptime vor permite acomodarea echipamentelor solicitate, precum si rezerva necesara pentru extensiile ulterioare previzibile, fara a pune probleme de implementare. ◷ Componentele interne active ale unitatii UPS, inclusiv bateriile, vor fi de tip hot-swap si vor permite deservirea (inclusiv inlocuirea acestora) fara oprirea sarcinii. ◷ Fiecare unitate UPS oferita va fi echipata cu functie interna activa de comutare neasistata, automata si transparenta pe bypass fara oprirea sarcinii atunci cand componentele interne de conversie si corectie ale unitatii nu fac fata sau prezinta erori de functionare.
Componente de distributie (PDU)	◷ Fiecare unitate va fi echipata cu o componenta de tip UPS PDU amovibila, cu functionalitate de bypass manual de serviciu, care va permite oprirea componentei active a unitatii fara oprirea sarcinii. Acestea vor fi prevazute cu alimentare de tip hardwired si cu conectori de iesire de 16A, hardwired sau de tip C19, cu breaker individual, si vor deservi direct componente de tip Server PDU (cu alimentare tipica pe 16A si conectorizare C19/C20). ◷ Pentru alimentarea echipamentelor din cabinet se vor folosi unitati de tip Server PDU, respectiv cu iesiri tipice de 6A si conectorizare C13/C14. ◷ Nu este acceptabila cascadarea pe mai mult de doua niveluri de distributie, inclusiv unitatea UPS PDU. ◷ Ansamblul va fi echipat cu numarul si structura de unitati PDU, precum si cu cablurile aferente, necesare alimentarii tuturor surselor echipamentelor instalate.
Componente de management al alimentarii	◷ Unitatile UPS vor fi echipate cu module interne amovibile de management in retea (SNMP sau asimilat). Solutia va include si instrumente software de management, respectiv: o atat agenti instalabili pe sistemele de operare de pe nodurile de procesare si de management deservite (si care vor putea fi administrati in mediu de retea), cat si :

	○ consola centrala de management care va putea comunica simultan cu unitatile UPS si cu agentii software de pe nodurile de procesare pentru a asigura gruparea sarcinilor pe prioritati, pornirea si oprirea in ordinea de precadere determinata, avand in vedere dependentele functionale intre servicii, etc. Consola centrala de management va putea fi instalata pe echipament fizic dedicat sau in instanta virtuala separata, distinct de alte functii de procesare de date sau de management. Ea va fi accesibila in retea pentru utilizatorii autorizati prin interfata Web si va dispune de un mecanism activ de asigurare a continuitatii operationale.
Consola locala KVM	Va fi montata in rack si va include : ○ monitor TFT, de min. 17 inch si suport pentru afisare de rezolutii native de (min.) 1280x1024 ; ○ tastatura USB cu dispozitive integrate de tip touch-pad si track-point ; ○ consola va ocupa, pliata, un spatiu optim de 1U in rack. Cabinetul sistem va fi echipat cu componente de acces controlat, local si de la distanta, la porturile si consolele de management ale echipamentelor, respectiv: ○ KVM/Cat5 (min. 4 porturi locale); ○ KVM/IP pentru acces la distanta.
Sistem de management	Sistem inteligent de monitorizare de la distanta a accesului pentru unul sau mai multe dulapuri de comunicatie prin intermediul unei interfete web, management bazat pe SNMP sau linie de comanda Telnet sau SSH Permite accesul la interfata de management a mai multor utilizatori simultan Posibilitate de setare a drepturilor de acces pentru fiecare utilizator Rapoarte de eveniment stocate in memoria interna a unitatii Posibilitate de monitorizare a pana la 11 dulapuri (pentru extinderea ulterioara a solutiei)
Ventilare si racire	Ventilare libera front-to-back cu usi fata-spate perforate.

2.4.2 ECHIPAMENTE HARDWARE TIP CLIENT

2.4.2.1 PLATFORMA HARDWARE PENTRU POSTURILE DE LUCRU INTERNE

Ca si posturi de lucru pentru utilizatorii interni ai sistemului e-VIZA solutia prevede o infrastructura hardware dedicata usurintei si confortului in exploatare, impreuna cu minimizarea costurilor administrative aferente. Fiecare din echipamentele hardware incluse in aceasta platforma va indeplini urmatoarele cerinte tehnice minime :

UNITATE CENTRALA		
1	Procesor	Tip: min.Intel Core i5 sau echivalent Frecventa de lucru: min. 3.33 GHz Mod de operare: 64bit

2	Chipset	Chipset proiectat de acelasi producator ca si procesorul Suporta procesoare Intel® Core™ cu tehnologie vPro™
3	Placa de baza	Controller video integrat - Min. 1920 X 1080 la 60 Hz Controller retea integrat 10/100/1000
4	Sloturi de memorie existente pe placa de baza	Min. 2 DIMM slots
5	Memorie RAM	Memorie instalata: minimum 4GB Tip: min.DDR3, dual-channel, PC3-10600 Frecventa: 1333 MHz
6	Controller SATA	Min. 2 porturi - minim Serial ATA II 3Gb/s
7	HDD	Nr. de HDD instalate: min. 1buc. Capacitate instalata: min.320 GB Viteza HDD: min. 7200 rpm Tip interfata: minim S-ATA II 3Gb/s
8	Unitate Optica	Minim DVD+/-RW 16x dual layer
9	Sistem Audio	Sistem audio integrat si difuzor in interiorul carcasei PC-ului
19	Interfata retea	Controller de retea integrat: 10/100/1000 Mbps, full – duplex, conector RJ-45 Nr. de porturi: min. 1 x RJ45, Capabilitati: WOL, AOL, ASF, PXE 2.0
10	Porturi - Intrari/ Iesiri	- Porturi USB: min. 6 • panoul spate: min. 4 x USB 2.0 - Porturi seriale: min. 1 port serial standard - Porturi PS/2: 2 x PS/2 - Conector video: 1x conector monitor care sa fie compatibil cu conectorul monitorului ofertat - Conectori audio: • panoul spate: Line in, Line Out • panoul frontal: Mic In, Headphone - Conector retea: 1x RJ45
11	Carcasa	Carcasa de tip Small Form Factor Sa permita pozitionarea UC atat in pozitie orizontala cat si verticala Culoare inchisa, rezistenta la uzura si praf
12	Sursa alimentare	Plaja de tensiune operabila: 90 – 264 VAC, 50 Hz/60 Hz Plaja de frecventa suportata: 47– 63 Hz Ventilatorul sursei: cu viteza variabila
13	Mouse	Mouse optic cu scroll, conectare USB
14	Tastatura	Tastatura conectare USB
15	Software utilitare furnizate de producatorul sistemului	Drivere pentru toate componentele sistemului; Posibilitate de readucere a sistemului in starea initiala prin CD/DVD Recovery
16	Sistem de operare	Windows 7 Professional 64-bit, preinstalat, licentiat cu drivere pentru toate componentele sistemului
17	Conditii de operare	Temperatura de functionare: min 10° - 35° C
18	Conformitate cu standarde/certificari valabile in Uniunea Europeana	● Standarde/Certificari electromagnetice: - EN 55022 - standard pentru limitarea emisiilor de radiatii electromagnetice

		- EN 55024 - standard privind imunitatea electromagnetica - EN 61000- standard pentru limitarea perturbatiilor induse in reteaua publica de electricitate ● Standarde/Certificari ergonomie: - ISO 9241 ● Standarde/Certificari de siguranta: - EN 60950 (IEC 950) - CE mark ● Standarde/Certificari de mediu - Energy Star - RoHS NOTA: Achizitorul isi rezerva dreptul de a verifica inscrierea sistemelor ofertate in standardele mentionate mai sus. La cererea achizitorului, ofertantul va trebui sa prezinte rezultatele testelor executate in laboratoarele de specialitate. Ofertantul are obligatia de a prezenta certificatele de conformitate a produselor furnizate cu standardele europene.
219	Zgomot Emis	- Maximum 28 dB(A) (in acord cu standardul ISO 7779 si ISO 9296) NOTA: Achizitorul isi rezerva dreptul de a verifica inscrierea sistemelor ofertate in standardele mentionate mai sus. La cererea achizitorului, ofertantul va trebui sa prezinte rezultatele testelor executate in laboratoarele de specialitate.
220	Compatibilitate cu sistemul de operare	Sistemele informatice trebuie sa se regaseasca pe site-ul www.microsoft.com/hcl, validate pentru sistemele de operare Windows Vista Business si Windows 7. Pentru verificare se solicita specificatiile tehnice date de producator pentru sisteme, in care sa se specifice ca acestea sunt cuprinse in lista HCL (*Hardware Compatibility List)* la Microsoft, sau copie dupa lista HCL cu mentionarea pozitiilor la care acestea sunt prevazute.
221	Uniformitate	Unitatea centrala, monitorul, tastatura si mouse-ul vor apartine aceluiasi producator (brand name). Ofertantul are obligatia de a prezenta documente relevante care dovedesc acest lucru.
MONITOR		
11	**Monitor**	Monitor LCD sau LED cu ecran plat fabricat de acelasi producator cu unitatea centrala, mouse si tastatura
22	Dimensiune	Diagonala: min. 21 inch Wide-Aspect Active Matrix TFT, max 23 inch
33	Tip/Tehnologie ecran	LCD sau LED
4	Dimensiune pixel	Max. 0,245 mm
5	Rata Contrast	Min. 1000:1
6	Luminozitate	Min. 250 cd/m2
7	Unghi de Vizibilitate	Min. 170° orizontal

		Min. 160° vertical
8	Timp de raspuns	Max. 5 ms
9	Interfata video	Min. 1 x 15-pin mini D-sub analog VGA si 1 x DVI-D cu HDCP
10	Panou de control	Digital OSD
11	Rezolutie nativa	Min. 1920 X 1080 la 60 Hz
12	Plug & Play	Monitor de tip Plug & Play
13	Cerinte de alimentare	Sursa de alimentare interna auto-senzitiva 90 - 265 V c.a. / 45 - 63 Hz
14	Consum energie	Maxim 50 W, in asteptare (Standby) 1 W
15	Unghiurile de mobilitate ale ecranului	Inclinatie verticala: min. 0˚ to +15˚
16	Aspect imagine	16:9 sau 16:10
17	Montare pe perete	Posibilitate de a se monta pe perete prin dispozitiv compatibil VESA
18	Boxe si intrari audio	Boxe integrate cu control volum, Min. 1 intrare audio stereo
19	Conditii de operare	Temperatura de functionare: min. intre 5° la 35° C
20	Conformitate cu standarde/certificari valabile in Uniunea Europeana	- CE mark Standarde/Certificari de mediu: - ISO 11469 si ISO1043 - RoHS - Energy Star

Se vor include in oferta 275 de echipamente hardware pentru postul de lucru intern (aproximativ cate 2 echipamente pentru fiecare Sediu Consular), in configuratie identica.

2.4.2.2 ECHIPAMENT TOKEN TIP SMART CARD

Pentru partea de autentificare multi-factor a utilizatorilor interni, solutia prevede o platforma formata din echipamente token tip Smart Card si clientul software (local) aferent. Echipamentele token tip Smart Card token oferite vor indeplini urmatoarele caracteristici tehnice minime:

- Sa fie Token de tip smartcard ce permite autentificare two-factor;
- Folosind tehnologie PKI sa permita generarea si stocarea cheilor private, parolelor si certificatelor digitale;
- Sa poata fi folosit in orice port USB obisnuit fara a fi necesar un echipament de tip reader additional;
- Solutia (formata din acest echipament si clientul software pentru autentificarea multi-factor descris la capitolul 2.3.2.6) sa fie validata FIPS 140-2, Level 2 si 3 ;
- Solutia sa fie validata Common Criteria EAL 4+ ;
- Sa permita integrarea facila cu alte aplicatii prin folosirea de module API puse la dispozitie de producator;
- Sa aiba suport pentru urmatoarele sisteme de operare:
  - Windows Server 2003 & 2008 si 2008/R2;
  - Windows 2000, XP, Vista, 7;
  - Linux, MacOS X.
- Sa ofere suport pentru urmatoarele standarde criptografice:
  - PKCS#11 veriunea 2.01;
  - Microsoft CAPI;
  - PC/SC;
  - X.509 versiunea 3 pt stocarea certificatelor;
  - SSL versiunea 3;

- IPSec/IKE.

- Sa suporte urmatorii algoritmi criptografici:
  - RSA 1024-bit / 2048-bit;
  - DES, 3DES;
  - SHA-1.
- Sa suporte USB 1 si 2.0.
- Capacitatea memoriei interne sa fie de 72Kb.

Se vor include in oferta 275 de echipamente token tip Smart Card (aproximativ cate 2 echipamente pentru fiecare Sediu Consular), in configuratie identica.

2.4.2.3 SCANER DE BIROU FLATBED

Pentru partea de scanara a documentelor de catre utilizatorii interni solutia prevede scanere de birou flatbed. Aceste echipamente vor indeplini urmatoarele caracteristici minime :

Caracteristica	**Descriere**
Format suportat	216 x 297 mm (A4)
Rezolutie suportata	Se vor suporta urmatoarele rezolutii : - 2400 x 4800 dpi, - interpolated: 65535 dpi.
Reprezentare registru de culoare	- 48 bit color, - 16 bit greyscale, - 1 bit monocrom.
Senzor	Tip CCD (charged-coupled device).
Interfata de conectare	USB 2.0.
Functii direct accesibile	Se vor suporta urmatoarele functii: - scan, - copy, - email, - OCR, - scan to web, - setup/cancel, - custom - power.
Capac de protectie detasabil	Inclus.
Capacitate de procesare de folii transparente	Inclusa.
ADF	Inclus.
Capacitate	50 pagini.
Performanta	5 ppm la o rezolutie de 200ppi.
Functie economizor (power saver)	Inclusa.
Greutate	Maxim 3 kg.
Dimensiuni tipice	Nu mai mult decat 500 x 300 x 100 mm.
Ciclu de exploatare recomandat de producator	1000 pagini zilnic.
Software	Suport O/S, inclusiv drivere si utilitare compatibile cu sistemul de operare ofertat la statiile de lucru client

Se vor include in oferta 140 de scanere de birou flatbed (aproximativ cate 1 echipament pentru fiecare Sediu Consular), in configuratie identica.

2.4.2.4 ECHIPAMENTE TIP SWITCH LAYER 2 DE ACCES

Fiecare sediu al Serviciilor Consular necesita cate un echipament tip Switch Layer 2 de acces pentru integrarea in cadrul retelei locale a echipamentelor hardware tip client. Aceste switch-uri se vor conecta in echipamente tip Switch Layer 2 de integrare aflate in posesia clientului la sediile acestuia. Echipamentele vor indeplini urmatoarele caracteristici minime :

- Sa ofere minim 24 porturi 10/100/1000 Mbp/s Gigabit Ethernet ;
- Rata de transfer : 16 Gbit/s ;
- Complianta cu cel putin urmatoarele standarde IEEE 803.2 10Base-T, IEEE 803.2u 100Base-TX, IEEE 803.2ab 1000Base-T, IEEE 803.2z 10Base-SX/LX ;
- Sa ofere minim 2 mini-GBIC/SFP sloturi ;
- Sa poata functiona atat in regim half-duplex cat si full-duplex ;
- Sa ofere suport pentru standardul IEEE 802.1Q VLAN (pana la 64 grupuri VLAN);
- Sa ofere support pentru standardul IEEE 802.3ad (« link aggregation » pana la 4 trunk-uri, pana la 8 porturi per trunk);
- Sa ofere suport pentru standardul IEEE 802.1w (rapid-spanning tree);
- Sa ofere suport tip “Port Mirroring”;
- Sa ofere suport pentru standardul IEEE 802.1X Port-Base access control si autentificare tip RADIUS ;
- Sa permita managementul dintr-o interfata web ;
- Sa permita upgrade-ul firewall-ului prin intermediul interfetei de management ;
- Sa ofere suport pentru tehnologia « Cable Diagnostics » sau echivalenta ;
- Sa ofere suport pentru SNMP trap si SNMP v1 cu RFC-1213/1573-interface group.

Se vor include in oferta 275 de echipamente tip Switch Layer 2 de acces, in configuratie identica.

2.4.2.5 TERMINALE DE INFORMARE

Pentru zona de informare a cetatenilor, cateva sali de asteptare ale Serviciilor Consulare vor fi echipate cu terminale de informare tip info-kiosk. Locatiile ce vor beneficia de acest serviciu vor fi comunicate Ofertantului castigator in faza de analiza a proiectului. Fiecare din aceste echipamente (terminale) va indeplini urmatoarele cerinte tehnice minime:

2.4.2.5.1 CERINTE GENERALE

Echipamentele oferite vor indeplini urmatoarele cerinte generale :

- structura bazata pe componente din materiale usoare cu suprafete rezistente;
- posibilitatea prinderii in pardoseala;
- dimensiuni de gabarit minime:
  - inaltime: 1900 mm,
  - latime: 500 mm,
  - adancime: 350 mm.
- inaltimea minima a ecranului : 1200 mm (distanta dintre sol si ultimul rand de pixeli pe partea joasa a ecranului);
- culoare customizabila in proportie de minim 80% in orice culoare conform standardului RAL;
- suprafata pe care nu se vad amprentele (amprentele sunt invizibile);
- accesul in terminal trebuie asigurat din spatele terminalului, printr-un capac securizat cu cheie;
- alimentarea cu electricitate si conectarea la retea sa se poata efectua atat prin picior, cat si prin spatele terminalului;
- componentele exterioare si partile care ies in afara carcasei trebuie confectionate din materiale rezistente la uzura si socuri fizice exterioare.

2.4.2.5.2 CERINTE FUNCTIONALE

Echipamentele oferite vor indeplini urmatoarele cerinte functionale :

- afisarea noutatilor;
- afisarea materialelor informationale despre Romania;
- afisarea materialelor informationale despre Beneficiar si sucursalele acestuia;
- afisarea programului de lucru;
- afisarea informatiilor despre serviciile oferite de Beneficiar;
- afisarea etapelor in cazul solicitarii unui act emis de Beneficiar;
- afisarea conditiilor care sunt necesar pentru solicitarea unui act sau a unui serviciu de la Beneficiar;
- afisarea documentelor necesare obtinerii unui act sau a unui serviciu de la Beneficiar;
- afisarea formularelor;
- afisarea altor informatii utile;
- posibilitati de selectare in mai multe limbi a meniului utilizat si a subiectelor/informatiilor;
- meniu usor de inteles pentru toate categoriile de utilizatori;
- meniu usor navigabil atat in meniul principal cat si in submeniuri;
- meniu animat;
- afisarea subiectelor/informatilor.

2.4.2.5.3 CERINTE TEHNICE

Echipamentele oferite vor indeplini urmatoarele cerinte functionale :

Cerinte tehnice monitor pentru terminalul de informare:

- diagonala: minim 26";
- tehnologie tip active matrix TFT LCD;
- suprafata display: touch screen construit impreuna cu ecran;
- tip touch screen: capacitiv;
- mod pozitionare vertical (90 de grade fata de sol);
- unghi minim de vizibilitate 176 grade atat pe orizontala cat si pe verticala;
- nr. minim culori 16.7 milioane;
- rezolutie optima minima 1360 x 768 pixeli;
- contrast minim 1500:1;
- timp de raspuns maxim: 15 ms;
- luminozitate minima (LCD-typical): 500 cd/mp;
- MTBF Monitor: minim 50 000 ore;
- alimentare cu energie electrica 110 – 230 VAC.

Cerinte tehnice sistem echivalent PC (integrat in terminalul de informare)

- tip procesor tehnologie Intel Core 2 Duo sau echivalent;
- frecventa procesor – minim 3.0 GHz;
- memorie CACHE procesor – minim 6 MB L2;
- FSB – minim 1333 MHz;
- cantitate memorie – minim 2 GB RAM de tipul DDR3 extensibila la 4 GB;
- chipset Intel sau echivalent;
- tip modul audio – placa de sunet incorporata minim 8 canale;
- modul video (placa video) integrat;
- memorie modul video – minim 256 MB;
- interfata serial ATA – minim 4 buc;
- interfata paralel ATA – minim 1 buc;
- interfata de retea integrat – minim 1 x interfata Gigabit Ethernet Controller;
- nr. minim porturi USB 2.0 – 8 buc;
- nr. minim porturi retea de tip RJ 45 – 1 buc;
- nr. minim porturi audio intrare – 1 buc;
- nr. minim porturi audio iesire – 1 buc;
- nr. minim porturi seriale – 2 buc;
- nr. minim porturi VGA – 1 buc;

- nr. minim porturi DVI-D – 1 buc;
- nr. minim sloturi PCI Express 2.0X16 – 1buc;
- nr. minim sloturi PCI Express X1– 1buc;
- nr. minim sloturi PCI – 2 buc;
- nr. minim sloturi PS/2 – 2 buc;
- tip unitate de stocare a datelor/informatiilor fix, fara componente mobile (solid state drive);
- capacitate unitate de stocare a datelor/informatiilor – minim 30 GB;
- viteza de citire unitate de stocare a datelor/informatiilor – minim 180 MB/s ;
- viteza de scriere unitate de stocare a datelor/informatiilor – minim 50 MB/s;
- alimentare cu energie electrica 110 – 230 VAC.

Cerinte tehnice UPS (sursa de putere neintreruptibila):

- capacitate minima 600 VA;
- plaja de tensiune 110 - 230 VAC;
- tip protectie la scurt circuit, supraincarcare, baterie consumata, varfuri de tensiune;
- tip acumulator minim 12 V / 7 Ah;
- timp maxim operare backup 20 minute;
- timp maxim reincarcare 10 ore (la 90% din capacitatea totala);
- prize intrare – minim 1;
- prize iesire – minim 1;
- timp de transfer – maxim 10 ms;
- permite posibilitate management centralizat;
- tip management prin minim 1 x port comunicatie serial.

Cerinte tehnice software preinstalat terminal:

- sistem de operare preinstalat;
- tip sistem operare – Microsoft Windows sau echivalent;
- licenta pentru perioada nedeterminata;
- aplicatie protectie sistem de operare;
- aplicatie protectie fisiere tip scrip si executabil;
- restabilirea fisierelor corupte a sistemului de operare si de tip script sau executabil prin simpla repornire a sistemului.

Se vor include in oferta 6 terminale de informare tip info-kiosk, in configuratie identica.

2.5 ALTE CERINTE

2.5.1 CERINTE DE ARHITECTURA

2.5.1.1 ARHITECTURA SOFTWARE

In imaginea de mai jos se regaseste reprezentarea schematica a pricipalelor blocuri functionale (software) din cadrul proiectului :

Portal extern :

- Portal extern
- Raportare
- Administrare
- Export/import date
- Sistem baze de date :
  - Baza de date portal
  - Baza de date raportare
  - Baza de date export/import alte sisteme

Portal Intern :

- Portal, care grupeaza urmatoarele zone/module functionale:

- Portal intern ;
- Raportare ;
- Interfata export/import de date ;
- Administrare.
- Aplicatie
- Sistem plata POS

Sistem de baze de date, care stocheaza schemele de date pentru urmatoarele sisteme/componente:

- Portal;
- Export Import;
- Raportare;
- Alte sisteme (sisteme de securitate, platforme de management, etc.)
- Sistem plata POS

Platforme de Virtualizare:

- Platforma de virtualizare tip server;

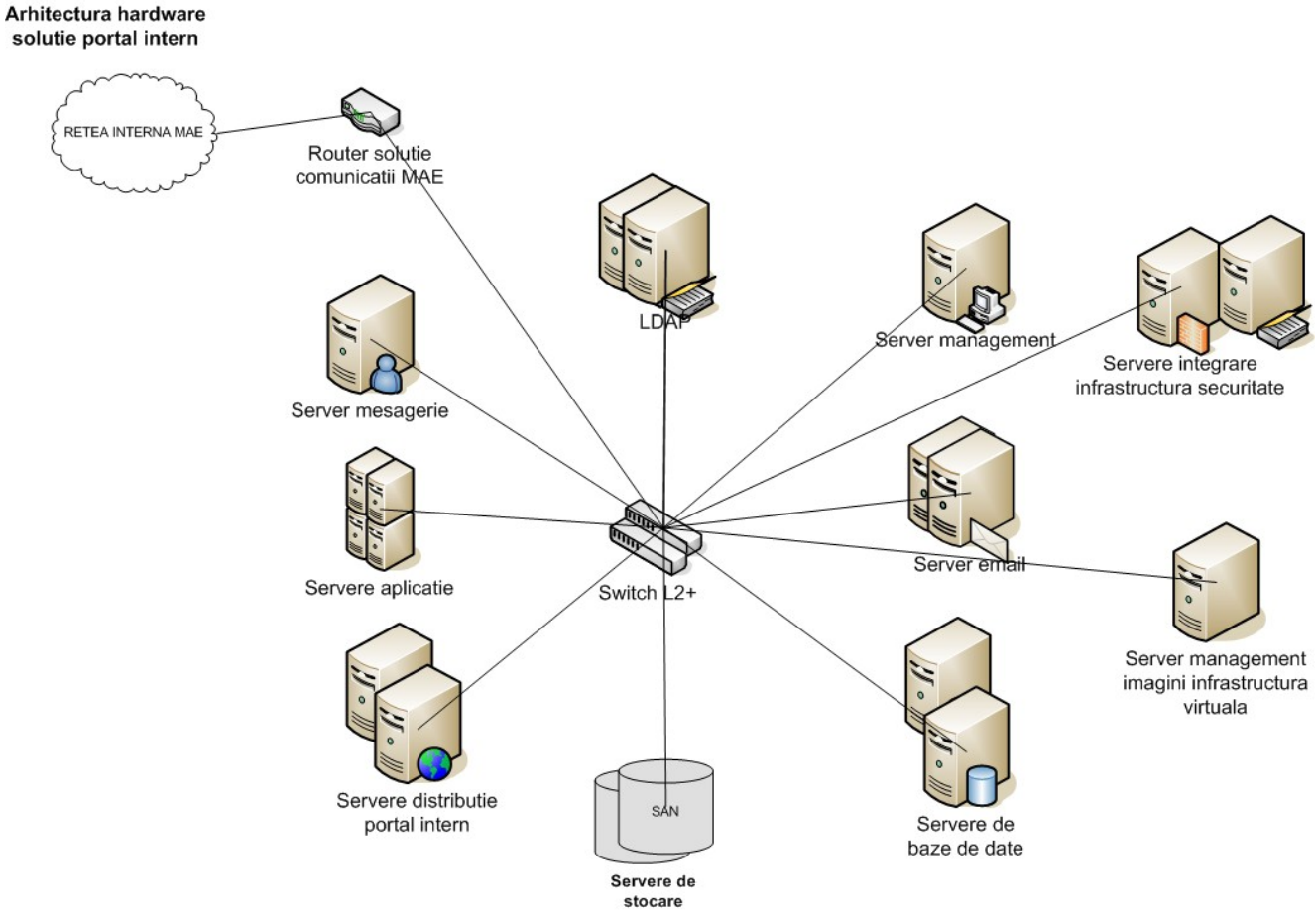
Server de Mesagerie;
Sistem Antivirus;
Sisteme de Securitate:
Managementul Identitatii;
Platforma de Monitorizare Centralizata (management si investigatie centralizata a evenimentelor de securitate IT);
Platforme de Management a Sistemelor Desktop:

Nota : Din motive de claritate unele blocuri functionale nu au fost enumerate.

2.5.1.2 ARHITECTURA HARDWARE

2.5.1.2.1 ARHITECTURA HARDWARE TIP SERVER PORTAL INTERN

In imaginea de mai jos se gaseste reprezentarea schematica a arhitecturii hardware tip server portal intern din cadrul proiectului.



Se identifica astfel urmatoarele echipamente hardware :

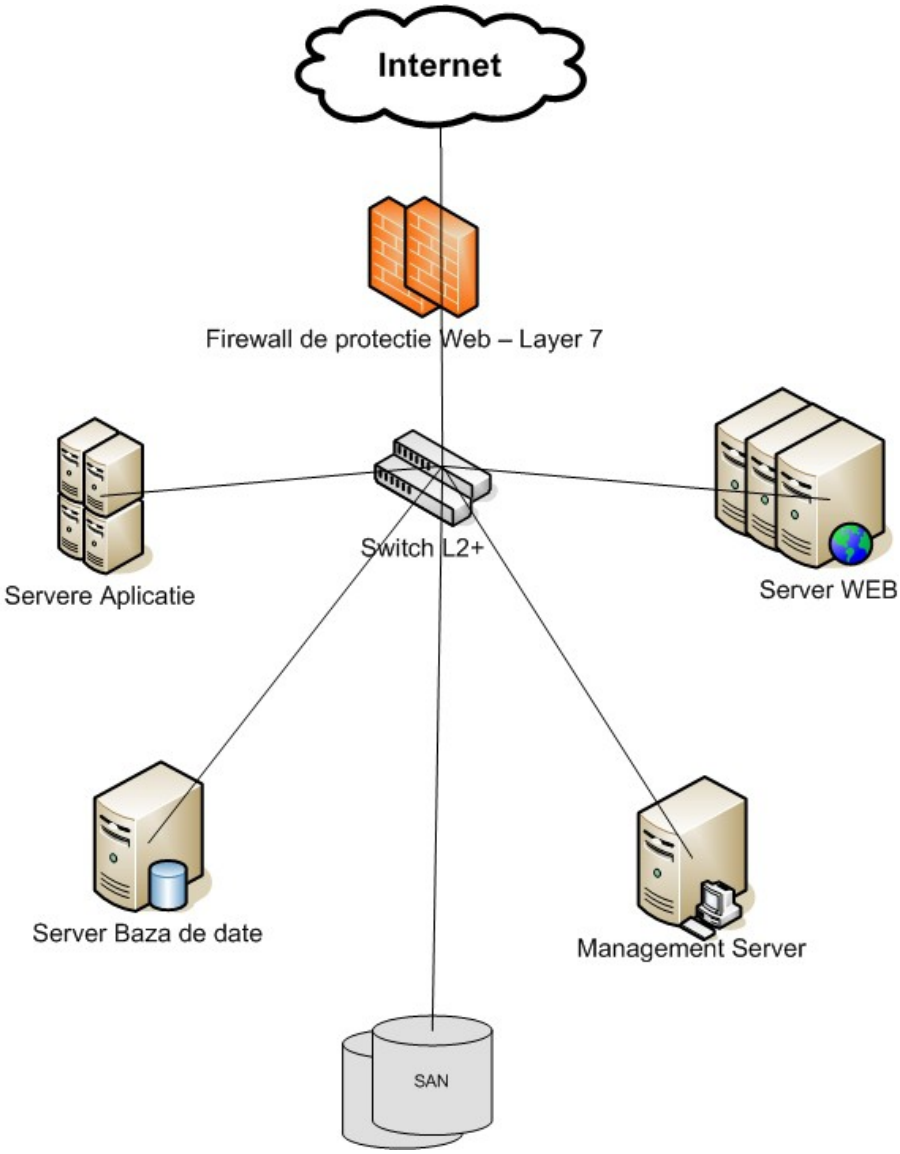
- Platforma de procesare tip server :
  - Servere pentru distributia de Portal intern;
  - Servere de aplicatii, cu rol de suport pentru rularea Portalului ;
  - Servere de baze de date ;
  - Servere integrare infrastructura de securitate :
    - Server de autentificare;
    - Server NTP/SNTP;
  - Servere de mesagerie ;
  - Servere pentru managementul identitatii ;
  - Servere pentru platformele de management.
- Servere de stocare;
- Echipamente de retelistica :
  - Tip Gateway;
  - Tip Switch L2+.
- Sistem cabinet pentru integrarea echipamentelor tip server.

Unele echipamente hardware care sunt incluse in proiect nu au fost reprezentate in imaginea de mai sus din motive de claritate a reprezentarii schematice.

2.5.1.2.2 ARHITECTURA HARDWARE TIP SERVER PORTAL EXTERN

In imaginea de mai jos se gaseste reprezentarea schematica a arhitecturii hardware tip server portal extern din cadrul proiectului.

Arhitectura hardware solutie portal extern



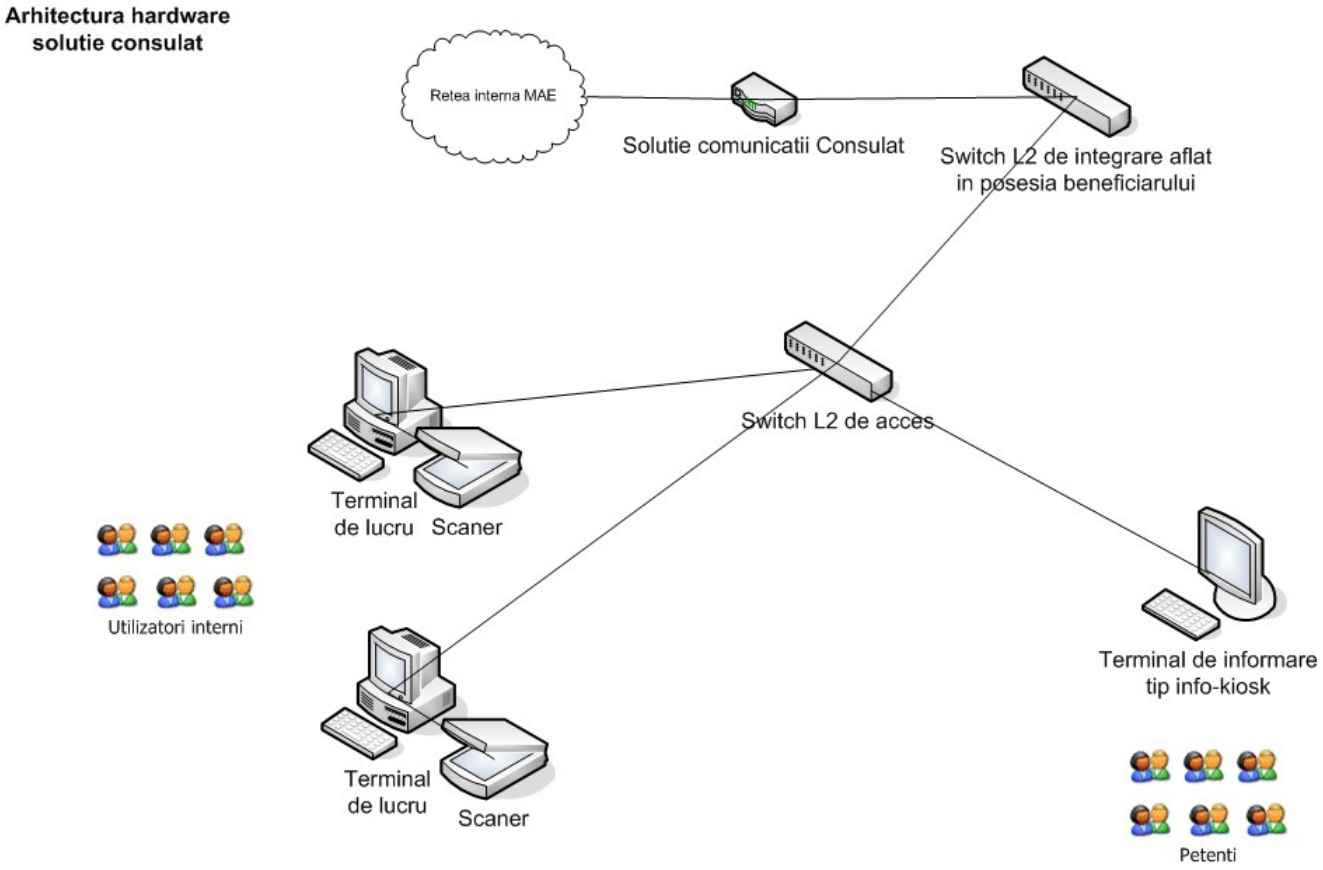
Se identifica astfel urmatoarele echipamente hardware :

- Platforma de procesare tip server :
  - Servere pentru distributia de Portal extern;
  - Servere de aplicatii, cu rol de suport pentru rularea Portalului ;
  - Servere de baze de date;
  - Servere management
- Servere de stocare;
- Echipamente de retelistica :
  - Tip Firewall protectie Web;
  - Tip Switch L2+.
- Sistem cabinet pentru integrarea echipamentelor tip server.

Unele echipamente hardware care sunt incluse in proiect nu au fost reprezentate in imaginea de mai sus din motive de claritate a reprezentarii schematice.

2.5.1.2.3 Arhitectura hardware tip client

In imaginea de mai jos se gaseste reprezentarea schematica a arhitecturii hardware tip client din cadrul proiectului, care se va instala la Sediile Consulare.



Se identifica astfel urmatoarele echipamente hardware :

- Echipament tip Switch Layer 2 de access (care se va conecta in echipamentul Switch Layer 2 de integrare aflat in proprietatea Beneficiarului) ;
- Terminal de informare tip info-kiosk (la Sediile Consulare unde va fi prevazut un astfel de echipament) ;
- Posturile de lucru interne ;
- Scaner de birou tip flatbed.

2.5.2 Cerinte de disponibilitate si scalabilitate

2.5.2.1 Cerinte generale privind disponibilitatea si scalabilitate

Din punct de vedere al disponibilitatii si scalabilitatii, sistemul trebuie sa respecte urmatoarele cerinte :

- Sa ofere suport pentru inalta disponibilitate, atat din punct de vedere hardware cat si software, astfel :
  - Platformele de procesare tip server sa contina minim 2 servere fizice identice configurate pentru lucrul in cluster ;

- Platforma de stocare centralizata si unificata sa permita instalarea si configurarea sa in cluster tip « activ-pasiv» cu minim 2 noduri ;
- Componenta tip Switch pentru interconectare LAN sa fie compusa din minim 2 echipamente identice ;
- Componenta tip Firewall protectie Web –Layer 7;sa fie compusa din minim 2 echipamente identice legate in HA;

Sa ofere suport pentru scalarea sa, atat din punct de vedere hardware cat si software, astfel :

- Sa permita adaugarea de servere fizice platformelor de procesare tip server;
- Sa permita adaugarea de memorie serverelor fizice din platformele de procesare tip server;
- Sa permita adaugarea sau dezvoltarea de noi module in cadrul componentelor de Portal intern si extern fara reproiectarea arhitecturii acestor componente.

Ofertantii vor preciza detaliat in oferte gradul si modul de indeplinire al cerintelor privind disponibilitatea si scalabilitatea stistemului informatic.

2.5.2.2 Cerinte specifice de virtualizare la nivel de server de aplicatii si baze de date

Sa se ofere suport pentru virtualizarea platformei de procesare, cu scopul :

- Separarii nivelului logic al aplicatiilor de platforma hardware de suport compusa din platforma de procesare tip server;
- De a avea posibilitatea crearii de instante virtuale multiple la nivel de aplicatii si baze de date (ex.1 : pe un nod de procesare de tip server de aplicatii componenta de Portal va rula intr-o instanta diferita fata de instanta in care ruleaza platforma de protectie criptografica centralizata a datelor stocate si procesate . Ex. 2 : baza de date aferenta componetei de Portal si baza de date aferenta platformei de protectie criptografica centralizata vor rula in instante diferite pe noduri de procesare tip server de baze de date);
- Alocarii dinamice a resurselor fizice catre instantele virtuale care au cea mai mare nevoie de procesare;
- Eliminarii eventualelor conflicte la nivel de procesor, memorie sau sistem de operare ce ar putea aparea ruland mai multe aplicatii in cadrul aceleiasi instante (non-virtuale) de aplicatie sau de baze de date.

2.5.3 Cerinte de interfatare cu alte sisteme

Din punct de vedere a interfatarii cu alte sisteme informatice aflate in uzul Beneficiarului, sistemul e-VIZA va implementa o interfata tip API standard pentru exportul si (eventual) importul de date catre, respectiv din alte, sisteme informatice, precum si pentru schimbul semnalelor de stare. Exporturile si importurile vor consta (in principiu) in transfer de fisiere si structuri XML de metedata. Sistemele informatice aflate in uz la Beneficiar si care fac obiectul interfatarii cu e-VIZA sunt :

- SNIV (catre SNIV se vor livra cereri printate cu cod de bare);
- Sistemul de ticketing de la Sediile Consulare
- Sistemul de plata electronica cu cardul bancar la ghiseu, prin intermediul POS

Detaliile tehnice privind interfatarea sistemului e-VIZA cu sistemele informatice mentionate mai sus precum si cu alte sisteme informatice (daca va fi cazul) se vor definitiva in perioada de analiza a proiectului si vor fi comunicate ofertantului castigator.

2.5.4 Cerinte de raportare

Sistemul trebuie sa includa functionalitatea de raportare, care sa respecte urmatoarele cerinte:

- sa permita raportarea centralizata, in sensul in care sa existe o interfata comuna atat pentru rapoartele utilizatorilor doritori de viza cat si pentru rapoartele utilizatorilor din partea Beneficiarului sau rapoartele statistice ;

- sa permita configurarea nivelelor de acces al utilizatorilor la aplicatie, prin editarea unor profile de utilizator in functie de nevoile de acces la informatie ale acestora ; aceste nivele de acces se vor lega/sincroniza cu mecanismul tip LDAP;
- sa ofere un mecanism de generare a rapoartelor care sa poata fi folosit ulterior de utilizatorii sistemului din partea Beneficiarului pentru crearea de noi rapoarte;
- sa permita definirea de rapoarte statistice privind activitatea utilizatorilor sistemului din partea Beneficiarului implicati in lucrul cu sistemul e-VIZA;
- sa permita rularea rapoartelor in mod automatizat pe baza unui orar predefinit si configurabil;
- sa permita exportul rapoartelor generate in urmatoarele formate de fisiere: html, xls, csv, pdf;
- sa permita salvarea si arhivarea rapoartelor generate.

Se vor defini cerinte detaliate privind rapoartarea in etapa de analiza din cadrul implementarii proiectului e-VIZA.

3. CERINTE PRIVIND SERVICIILE

3.1 CERINTE PRIVIND METODOLOGIA DE PRESTARE A SERVICIILOR – MANAGEMENTUL PROIECTULUI

3.1.1 CONDITII GENERALE

Activitatile de management ale proiectului se refera la analiza si stabilirea obiectivelor de proiect; evaluarea si controlul riscurilor; estimarea si alocarea resurselor; organizarea proiectului; stabilirea sarcinilor; coordonarea si monitorizarea activitatilor de proiect; raportarea derularii proiectului; previzionarea tendintelor proiectului; managementul calitatii; managementul schimbarilor.

Managementul de proiect este o activitate cu caracter permanent, constand in urmatoarele componente:

a) activitati de incepere a proiectului constau in organizarea biroului de proiect si mobilizarea echipei de management de proiect, precum si informarea factorilor interesati cu privire la startul proiectului, la obiectivele stabilite si la rezultatele asteptate;
b) activitati generale de management de proiect (planificare, organizare si coordonare, monitorizare si control, raportare, incheierea proiectului) imbinate cu activitati speficice proiectelor finantate din fonduri europene: aspecte de management financiar, asigurarea vizibilitatii proiectului si asigurarea calitatii proiectului.

Activitatile generale de management de proiect se deruleaza in baza unei metodologii complete, care stabileste continutul si responsabilitatile pentru toate activitatile de-a lungul fazelor proiectului. Proiectul se fundamenteaza, inca din etapa de concepere, pe metodologia de Project Cycle Management[1], a caror utilitate devine vizibila in perioada de implementare a activitatilor: managementul calitatii, managementul resurselor umane, managementul timpului, managementul financiar, managementul comunicarii, managementul conflictelor, managementul riscurilor, managementul integrator al proiectului, SWOT, analiza de impact.

Pentru intalnirile din cadrul proiectului, este utilizata comunicarea directa. Metoda analizei si sintezei informatiilor este aplicata in realizarea materialelor utile derularii activitatilor proiectului. Aceasta metoda supune analizei informatiile obtinute in urma discutiilor de grup si a celor libere, si identifica aspectele ce urmeaza sa se regaseasca in materialele utilizate in cadrul proiectului.

Monitorizarea se va face pe tot parcursul desfasurarii proiectului si va cuprinde:

- ❖ monitorizarea executarii activitatilor proiectului, care tine evidenta utilizarii resurselor proiectului si a obtinerii rezultatelor preconizate;
- ❖ monitorizarea financiara care va urmari utilizarea corecta a fondurilor, modul de efectuare a platilor, incadrarea in prevederile capitolelor bugetare de cheltuieli ale proiectului. Se va urmari permanent eficienta cheltuielilor realizate;
- ❖ diagnoza proiectului pentru a vedea, in cazul aparitiei unor probleme de implementare, care sunt noile solutii necesare continuarii implementarii.

[1] Manualul este disponibil in limba engleza la urmatoarea adresa: http://ec.europa.eu/europeaid/multimedia/publications/documents/tools/europeaid_adm_pcm_guidelines_2004_en.pdf

Calendarul activitatilor de monitorizare: monitorizarea va fi desfasurata ca o activitate continua, pe tot parcursul implementarii proiectului, ea furnizand informatii si date legate de anumiti indicatori stabiliti in prealabil de catre echipa de implementare, dar pot exista puncte culminante ale activitatii (rapoarte de progres, notificari).
Evaluarea este procesul prin care se obtin informatii asupra calitatii proiectului, masurand rezultatele in raport cu obiectivele stabilite, in vederea luarii deciziilor strategice pentru a sustine implementarea si managementul proiectului. Se va realiza atat evaluarea permanenta (concomitenta proiectului), cat si evaluarea finala, conform schemei de evaluare.
Evaluarea si raportarea rezultatelor finale presupun evaluari ale activitatilor desfasurate si analize privind impactul acestora, precum si discutii cu membrii echipei de proiect, privind actiunile viitoare.
Evaluarea este un proces periodic care se concentreaza asupra a 4 aspecte principale: resursele investite, activitati desfasurate, rezultate obtinute, impact realizat. In cadrul proiectului, va fi realizata o evaluare interna, cat si una externa.
Evaluarea permanenta, realizata pe parcursul duratei proiectului va fi axata pe urmatoarele aspecte: incadrarea in timpul alocat; incadrarea in buget; stadiul realizarilor; efectele implementarii proiectului pentru institutie; cooperarea in randul membrilor echipei de proiect.
In cazul evaluarii permanente se vor folosi multe dintre datele obtinute in urma procesului de monitorizare, insa examinarea acestor date va fi analitica.
Evaluarea finala se va realiza la sfarsitul perioadei de implementare a proiectului, moment in care toate componentele proiectului (proces, relevanta si coerenta masurilor luate, activitatile, valoarea adaugata) vor fi luate in considerare in vederea examinarii rezultatelor. Evaluarea va fi atat cantitativa, cat si calitativa si va viza: resursele investite, activitatile desfasurate, rezultatele obtinute, atingerea nivelului de performanta propus la planificare, schimbarile intervenite si consecintele lor, efectele implementarii proiectului pentru institutie, nivelul de proprietate locala asupra rezultatelor proiectului.
Procedurile de evaluare interna vor urmari:

- masura in care activitatile sunt realizate, in conformitate cu planificarea initiala;
- eficacitatea implementarii aplicatiei software, procedura de evaluare constand in testari repetate ale continutului educational multimedia;
- coerenta continutului didactic al cursurilor care vor fi organizate in sistem e-educatie , ceea ce implica verificari detaliate efectuate de specialisti in detaliu;
- utilizarea eficienta a resurselor, prin observatiile finantatorului la raportul final

Modalitatile de evaluare interna sunt urmatoarele:

- intalniri lunare ale managerului de proiect cu membrii echipei de implementare in care se evalueaza stadiul proiectului pe baza informatiilor culese de responsabilii de activitati, finalizate printr-un proces verbal;
- raport lunar al responsabililor de activitati continand evaluarea stadiului proiectului;
- intocmirea de catre responsabilii de activitati a unui raport la sfarsitul fiecarei activitati parcurse.

Elaborarea raportului final va fi in sarcina managerului de proiect.
In scopul unei analize eficiente si impartiale se va desfasura si o evaluare externa, comandata pentru a evita dezavantajele folosirii unui singur tip de evaluare, deseori subiectiva, si anume aceea a evaluarii interne.
Raportarea activitatilor in cadrul proiectului: beneficiarul va inainta, lunar sau trimestrial, Autoritatii Contractante, odata cu cererea de rambursare si raportul de progres, completat in formatul standard prevazut la Contractul de finantare din Instrumente Structurale.
Raportul de progres va prezenta: activitatile desfasurate in perioada raportata, obiectivele realizate comparativ cu cele planificate, rezultatele obtinute pana la momentul raportarii si cele asteptate pentru perioada urmatoare, stadiul la care se afla achizitiile publice, stadiul realizarii indicatorilor sintetici si fizici, probleme identificate la nivelul proiectului, modificari esentiale fata de ceea ce s-a stabilit in contract, operate sau previzionate la nivelul proiectului, recomandari pentru perioada urmatoare in vederea preintampinarii eventualelor deficiente la momentul raportarii, etc. La fiecare raport de progres, beneficiarul va descrie modul in care proiectul respecta legislatia in domeniul egalitatii de sanse, a dezvoltarii durabile.
Ofertantul trebuie sa asigure Autoritatii Contractante realizarea **managementului proiectului** necesara pentru implementarea cu succes a acestora. Prestatorul are rolul de expert in furnizarea de servicii si va lua o pozitie constructiva in indeplinirea **obiectivelor contractului**, aceasta insemnand urmatoarele:

- Sa asigure alocarea de resurse umane cu inalta calificare, familiarizate pe deplin cu cele scrise in proiect, cu sarcinile primite si sa se asigure in permanenta de disponibilitatea resurselor corespunzatoare;

- Sa se asigure in permanenta ca este pe deplin informat in legatura cu stadiul de progres al proiectului;
- Sa asigure un nivel maxim de transparenta si sa lanseze din timp atentionari, catre Beneficiar sau catre orice alta parte terta implicata in proiect, asupra oricarui element care poate sa puna in pericol indeplinirea la timp si corespunzatoare a unei activitati sau a unui document al proiectului;
- Sa asigure transmiterea la timp, corecta si completa a documentelor si informatiilor aferente implementarii proiectelor, permitand partii destinatare un timp suficient sa raspunda si sa ia masuri pe baza informatiilor primite;
- Sa emita raportari intr-un format ce va fi agreat cu Beneficiarul, in care informatiile furnizate sa fie complete, precise, clare, exacte si fara ambiguitati, cu atentie la detalii si accesibilitate;

Se vor realiza raportarile trimestriale si raportarea finala catre Autoritatea de Management.
Trimestrial se vor realiza raportarile tehnico-financiare, se vor organiza intalniri periodice lunare intre membrii echipei de proiect pentru a identifica progresul proiectului si potentialele probleme si/sau riscuri care pot sa afecteze finalizarea cu succes a proiectului.
Pentru buna implementare a proiectului conform clauzelor contractuale se va constitui cate o echipa multidisciplinara de implementare, formata astfel :

- Managementul de proiect va fi coordonat/supervizat de catre un Comitet de Conducere alcatuit din 5 membrii, angajati ai solicitantului. – de mentionat responsabilii de la beneficiar (reprezentant legal, referent, responsabil financiar, responsabil PR, responsabil tehnic IT)
- expertii firmei de consultanta ce vor asigura managementul proiectului.

Modalitatea de comunicare si de raportare a Prestatorului fata de Beneficiar se va realiza prin intermediul echipei multidisciplinare de implementare a proiectului.
Ofertantii vor oferi in Propunerea tehnica o descriere completa a metodologiei de PM, precum si un plan preliminar de proiect, care vor fi utilizate pe parcursul proiectului de implementare.
Furnizorul va avea o abordare metodologica asupra intregului proces de implementare si va descrie modul in care va urmari derularea proiectului.
Planificarea activitatilor:

- Ofertantul va prezenta planificarea activitatilor propuse, in interdependenta acestora – un plan Gantt este asteptat;
- Planul trebuie sa mentioneze care sunt jaloanele de proiect (milestones) pe care ofertantul si-a propus sa le respecte pentru atingerea obiectivelor in concordanta cu etapele de realizare ale proiectului;
- Ofertantul va detalia care sunt resursele pe care le va aloca pentru fiecare etapa a proiectului, eventual activitati pe care le considera mai importante.

Planul preliminar de proiect va trebui sa acopere urmatoarele puncte:

- metodologia de management a proiectului;
- organizarea proiectului;
- planul de comunicare;
- planificarea activitatilor, timpul de desfasurare si resursele implicate (inclusiv grafic Gantt din care sa rezulte relationarea activitatilor la un grad de detaliu suficient pentru a demonstra satisfacerea cerintelor caietului de sarcini);
- planul de livrare, instalare si implementare (detalierea activitatilor, rezultate asteptate – livrabile, documente rezultate si jaloane de proiect – milestones);
- planul de instruire;
- modalitatea de tratare a schimbarilor in cadrul proiectului (in limitele Caietului de Sarcini). Se va prezenta descrierea procedurii de management al schimbarilor precum si formularele care vor fi utilizate in cadrul acestui proces pe durata proiectului;
- planul de acceptanta – se va prezenta planul impartit pe etape precum si formularele aferente receptiilor/acceptantelor partiale si receptiei/acceptantei finale;
- planul de risc pentru fazele proiectului.

Serviciile PM vor fi oferite de personalul specializat in PM al Ofertantului. Ofertantii vor include in prezentarea echipei de proiect personalul PM propus. Managerul de proiect de la furnizor trebuie sa fie certificat de catre o organizatie recunoscuta pe plan international conform fisei de date a achizitiei.
In cadrul activitatilor generale de management de proiect, sunt stabilite modalitatile de organizare si coordonare a resurselor umane implicate in realizarea activitatilor proiectului.
Activitati generale de management de proiect vor consta in cel putin:

- planificarea activitatilor;
- coordonarea si administrarea activitatilor tehnice;
- coordonarea si administrarea echipelor de proiect;
- definirea si implementarea planului de comunicare in cadrul proiectului;
- revizuirea si administrarea modificarilor proiectului;
- organizarea proiectului prin stabilirea rolurilor si cadrului de comunicare, monitorizare si raportare;
- pregatirea si intretinerea planul de proiect in care sunt inregistrate activitatile, sarcinile, termenele de executie si estimarile asupra desfasurarii proiectului;
- organizarea si conducerea intalnirilor periodice cu echipa de proiect cu scopul de a reanaliza starea proiectului;
- pregatirea rapoartelor periodice; din aceste rapoarte va rezulta progresul activitatilor, eventualele intarzieri, motivele intarzierilor, riscurile aferente si metode sau actiuni de redresare;

Furnizorul va avea o abordare metodologica asupra intregului proces de implementare si va descrie modul in care va urmari derularea proiectului. Din punct de vedere al metodologiei ofertantul:
- va declara ce metodologie de dezvoltare a sistemelor informatice foloseste. Este obligatorie folosirea unei metodologii recunoscute pe plan international.
- va declara ce metodologie de management de proiect foloseste. Este obligatorie folosirea unei metodologii recunoscute pe plan international.
- va face o prezentare a metodologiilor folosite in proiect.

3.1.2 SERVICIILE SOLICITATE DE CONSULTANTA SI ASISTENTA

- Planificarea si coordonarea activitatilor proiectului prin folosirea unor tehnici si instrumente moderne de planificare
- Servicii de consultanta si asistenta pentru elaborarea cererilor de rambursare, a rapoartelor de progres si a altor documente solicitate de catre Autoritatea de Management
- Servicii de consultanta si asistenta privind gestionarea contractelor cu toti furnizorii implicati in proiect
- Monitorizarea si evaluarea implementarii proiectului

3.1.2.1 PLANIFICAREA SI COORDONAREA ACTIVITATILOR PROIECTULUI

Coordonarea activitatilor din cadrul proiectului – presupune ca pe intreaga perioada de implementare a proiectului, firma responsabila de realizarea managementului de proiect, sa coordoneze desfasurarea tuturor activitatilor, astfel incat sa fie evitate intarizierile ce pot aparea in diferitele faze ale proiectului, sa se respecte bugetul stabilit pentru proiect cat si alocarea corespunzatoare a resursele umane implicate in derulare.

- Ofertantul va fi responsabil pentru formarea unei Echipe de Proiect si pentru organizarea unui Birou de Proiect si va face in oferta sa tehnica propuneri concrete in acest sens.
- Ofertantul este responsabil pentru cunoasterea amanuntita a informatiilor existente in contractul de finantare si anexele acestuia, cat si in Manualul de implementare al proiectelor ce se deruleaza prin intermediul PO DCA, de catre expertii echipei de proiect.
- Ofertantul va elabora Planul de proiect care va oferi o privire de ansamblu asupra intregului proiect si va constitui referinta fata de care va fi controlata intreaga evolutie ulterioara a proiectului, in cadrul fiecarei etape. In cadrul Planului de Proiect se vor identifica livrabilele principale, necesarul de resurse impreuna cu fisele de post, totalitatea costurilor si punctele principale de control in cadrul proiectului, cum ar fi limitele de etape.

3.1.2.2 MANAGEMENTUL CONTRACTULUI DE FINANTARE

Mentinerea contactului permanent cu Managerul de proiect, prin implementarea cel putin a urmatoarelor subactivitati:

- Intocmirea **cererilor de rambursare** a cheltuielilor si vizarea acestora de catre responsabilul financiar si managerul de proiect. Ofertantul elaboreaza cererile de rambursare pe care le va inainta Beneficiarului, avand in vedere faptul ca numai Beneficiarul este responsabilul direct, conform prevederilor din Contractul de finantare care urmeaza a fi incheiat cu AMPODCA. De asemenea ofertantul asigura verificarea cheltuielilor pentru a asigura un control al acestora, in vederea evitarii oricaror iregularitati in utilizarea fondurilor europene;
- Realizarea efectiva a **verificarii documentelor de plata** depuse in cadrul contractelor de prestare de servicii si furnizare de produse, intocmirea efectiva a tuturor documentelor aferente managementului financiar al contractelor care se vor implementa in cadrul proiectului;
- Realizarea **raspunsurilor** la eventualele solicitari de clarificari – Furnizorul elaboreaza raspunsurile la solicitarile de clarificari pe care le va inainta Beneficiarului, avand in vedere faptul ca numai Beneficiarul este responsabilul direct, conform prevederilor din Contractul de finantare care urmeaza a fi incheiat cu AMPODCA.;
- Asigurarea de suport pentru elaborarea tuturor **raportarilor** solicitate de Autoritatea de Management a PODCA. Ofertantul asigura elaborarea rapoartelor de progres solicitate de AM PODCA.
- Asigurarea de suport pentru rezolvarea tuturor aspectelor administrative ale Contractului de finantare, inclusiv eventualele **modificari/notificari/acte aditionale** ale contractului de finantare datorate modificarilor de buget, termene, calendar de implementare, calendar de rambursare etc.

3.1.2.3 Asigurarea managementului contractelor din cadrul proiectului

- Acordarea de sprijin metodologic pentru derularea, monitorizarea si urmarirea contractelor de servicii si furnizare care sa respecte atat legislatia in vigoare, cat si prevederile contractelor de servicii si furnizare de produse, Contractului de Finantare si a altor documente relevante
- Sprijinirea efectiva a celorlalte entitati responsabile in atingerea obiectivelor proiecelor in elaborarea urmatoarelor documente: identificarea riscurilor in privinta activitatii economico-financiare a A.C. si intocmirea planului de actiune pentru managementul acestor riscuri si elaborarea previziunilor privind fluxurile de plati si a graficului de rambursare astfel incat sa fie respectate conditiile impuse in Contractul de Finantare

3.1.3 Monitorizarea, evaluarea si raportarea tuturor activitatilor derulate in cadrul proiectului

Monitorizarea implementarii proiectului conform planului de lucru, bugetului si rezultatelor asteptate:

- Realizarea de analize periodice lunare cu privire la starea implementarii proiectului;
- Verificarea si ajustarea alocarii resurselor financiare si umane potrivite, coroborate cu graficul de realizare a activitatilor;
- Verificarea realizarii fiecarei subactivitati si activitati in parte si acordarea acceptantelor partiale;
- Colectarea, inregistrarea si raportarea trimestriala a informatiilor utile in raport cu evolutia proiectului;
- Initierea si participarea la toate intalnirile de lucru;
- Evaluarea permanenta, realizata pe parcursul duratei proiectului va fi axata pe urmatoarele aspecte: incadrarea in timpul alocat; incadrarea in buget; stadiul realizarilor; efectele implementarii proiectului pentru institutie; cooperarea in randul membrilor echipei de proiect;
- Monitorizarea financiara care va urmari utilizarea corecta a fondurilor, modul de efectuare a platilor, incadrarea in prevederile capitolelor bugetare de cheltuieli ale proiectului. Se va urmari permanent eficienta cheltuielilor realizate.

3.1.3 Cerinte pentru raportare

Ofertantul va intocmi rapoarte pe intreaga perioada de derulare a contractului. Rapoartele intocmite vor acoperi toate activitatile Proiectului si vor puncta toate rezultatele obtinute de catre Ofertant.
Pe parcursul implementarii contractului, Prestatorul trebuie sa elaboreze cel putin urmatoarele tipuri de rapoarte:
Raport Initial. Prestatorul va furniza catre Beneficiar un Raport preliminar care va cuprinde aprecierea privind situatia existenta, propuneri si recomandari, planificarea activitatilor si organizarea echipei sale, problemele critice identificate si principalele masuri care se impun pentru rezolvarea acestora, precum si informatiile necesare referitoare la strategia si planul de actiune al dezvoltarii proiectului. Acest raport va detalia actiunile necesare realizarii activitatilor din contract, precizand lista detaliata a livrabilelor aferente fiecarei actiuni si termenele de livrare, ce vor fi monitorizate de Autoritatea Contractanta. Termenul de predare va fi de 1 luna de la incheierea contractului.
Rapoarte lunare. Aceste rapoarte vor prezenta asigurarea ca activitatile se deruleaza conform planului de proiect din punct de vedere al incadrarii in timp, al incadrarii in buget, al realizarilor si al implicarii echipei de proiect in activitatile proiectului.
Rapoarte la sfarsitul fiecarei activitati parcurse. Aceste rapoarte vor prezenta activitatile desfasurate in activitatea respectiva, obiectivele realizate comparativ cu cele planificate, rezultatele obtinute in comparatie cu cele propuse, stadiul realizarii indicatorilor in comparatie cu cei propusi, resursele implicate in comparatie cu cele propuse, probleme identificate la nivelul fiecarei activitati, modificari esentiale fata de ceea ce s-a stabilit initial pentru acea activitate, operate sau previzionate la nivelul proiectului, recomandari pentru etapele urmatoare in vederea preintampinarii eventualelor deficiente la momentul raportarii, etc.
Rapoarte trimestriale. Aceste rapoarte vor prezenta principalele progrese ale perioadei raportate, dificultatile intampinate, abaterile de la planul activitatii si consumul de resurse. Beneficiarul poate sa solicite Prestatorului sa transmita rapoarte de progres intermediare privind anumite aspecte specifice identificate de reprezentantii sai.
Raport final. Raportul final se va transmite de catre Prestator catre Beneficiar la finalizarea activitatilor de consultanta prevazute in contractul de servicii. El trebuie sa descrie intregul proces de implementare a proiectului, care va inlesni evaluarea rezultatelor obtinute atat in termeni calitativi, cat si cantitativi. Raportul va include de asemenea, o evaluare a succesului proiectului.
Rapoartele trebuie elaborate in conformitate cu cerintele stipulate in instructiunile emise de catre finantator.

3.2 CERINTE PRIVIND IMPLEMENTAREA SISTEMULUI INFORMATIC

Ofertantii trebuie sa prezinte in detaliu metodologia de dezvoltare software care va fi adoptata pentru dezvoltarea sistemului informatic. Procedurile trebuie sa acopere cel putin urmatoarele aspecte:

- Sistemul de Management al Riscului ;
- Sistemul de Management al Calitatii ;
- Tehnici de colaborare si comunicare ;
- Abordarea proceselor interne de dezvoltare;
- Definirea si implementarea parametrilor de evaluare a ciclului de viata al proiectului de dezvoltare;
- Documente de livrat, formatele acestora precum si responsabilitatile privind livrabilele si acceptanta, atat din punct de vedere al Ofertantului cat si al Autoritatii Contractante.

Implementarea sistemului informatic trebuie sa se desfasoare intr-un mod organizat, astfel incat sa se asigure monitorizarea si controlul activitatilor pe toata durata proiectului. Etapele implementarii trebuie sa fie bine definite, marcate cu puncte de verificare, livrari si livrabile.
Implementarea sistemului va contine etapele de mai jos:

- Analiza si proiectare;
- Instalare , configurare si dezvoltare in cadrul componentelor sistemului;
- Instruire utilizatori;
- Testare functionala si integrata;

- Garantie si suport post-productie.

Ofertantii trebuie sa detalieze informatiile corespunzatoare modului de evaluare si acceptanta pentru livrarea proiectului. Ofertantii trebuie sa prezinte un plan detaliat de implementare a proiectului, in care sa tina cont de urmatoarele cerinte specifice etapelor de implementare:

3.2.1 ANALIZA SI PROIECTARE

Analiza proiectului va fi realizata pe fiecare componenta a sistemului, cu echipe specializate in domeniile respective atat din partea Furnizorului cat si a Autoritatii Contractante.
Furnizorul va pune la dispozitie chestionarele pe baza carora se vor desfasura interviurile cu angajatii Autoritatii Contractante si va elabora documentul de analiza, care va cuprinde cel putin urmatoarele categorii de informatii:

- Definitivarea structurii de date ce fac obiectul sistemului informatic integrat ;
- Definirea fluxurilor de lucru pentru fiecare categorie de utilizator in parte ;
- Specificatii de design (style guide);
- Estimarea volumului de informatie si a resurselor tehnice necesare functionarii sistemului informatic integrat ;
- Specificatii de raportare ;
- Specificatii de interfatare cu alte aplicatii/sisteme ale Autoritatii Contractante.

Autoritatea Contractanta va pune la dispozitia Furnizorului toate datele necesare configurarii optime a sistemului informatic integrat, precum:

- infrastructura existenta la momentul respectiv ;
- lista cu aplicatiile/sistemele utilizate ;
- alte date necesare configurarii sistemului informatic integrat, cum ar fi restrictii sau calendarul disponibilitatii resurselor alocate pe proiect din partea Autoritatii Contractante.

Pe baza documentului de analiza se va elabora de catre specialistii Furnizorului documentul de specficatii tehnice, pe baza caruia intreg sistemul va fi proiectat din punct de vedere tehnic.
Odata livrata analiza, prin cereri de schimbare, se pot face amendamente la procesele descrise, astfel incat sa raspunda cererilor ulterioare ale Autoritatii Contractante.
Cererile de schimbare vor genera modificari ale documentului initial de analiza. Aceste schimbari vor fi bine documentate si evidentiate astfel incat documentul de analiza sa ramana o imagine fidela a sistemului informatic integrat care se implementeaza.

Ofertantii trebuie sa descrie in detaliu metodologia dupa care vor derula activitatile de analiza si proiectare si sa prezinte impreuna cu oferta procedurile si instructiunile de lucru de analiza si proiectare implementate in cadrul propriei organizatii.

Ofertantii trebuie sa descrie instrumentele pe care le vor utiliza astfel incat sa poata asigura:

- colectarea si evidenta cerintelor
- acoperirea integrala a tematicii proiectului
- evidenta modificarilor cerintelor
- trasabilitatea cerintelor pornind de la obiectivele proiectului pana la specificatiile tehnice

Ofertantii trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapelor de analiza si proiectare. Descrierea trebuie sa contina cel putin urmatoarele informatii:

- formularul/formularele care va fi utilizate pentru fiecare livrabil
- descrierea continutului fiecarui livrabil
- modul in care va fi interpretat continutul livrabilelor

3.2.2 INSTALARE, CONFIGURARE SI DEZVOLTARE IN CADRUL COMPONENTELOR SISTEMULUI

Etapa de instalare si configurare a functionalitatilor specifice sau a adaptarii functionalitatilor platformelor de suport a sistemului informatic integrat, precum si dezvoltarile necesare in cadrul componentelor acestuia, trebuie sa se faca pe o perioada suficienta si sa cuprinda un numar suficient de resurse, astfel incat sa asigure rezolvarea tuturor cerintelor din caietul de sarcini si urmarind specificatiile din documentul de analiza.

3.2.3 INSTRUIRE UTILIZATORI

Etapa de instruire a utilizatorilor trebuie sa se incadreze in partea finala a implementarii sistemului e-VIZA, sa aiba o durata suficienta pentru insusirea de catre utilizatori a tuturor cunostintelor necesare privind sistemul si sa vizeze un numar suficient de instructori specializati.
Ofertantii vor livra un plan de instruire si de asemenea vor livra materialele necesare instruirii atat in format electronic, cat si in format tiparit. Instruirea se va realiza in limba Romana.

3.2.4 TESTARE FUNCTIONALA SI INTEGRATA

Furnizorul trebuie sa prezinte documentatia procedurilor de testare folosite in cadrul organizatiei sale, astfel incat sa dovedeasca capacitatea de asigurare a calitatii sistemului livrat, pe criterii stabilite de comun acord, ulterior analizei.
Pentru a asigura o buna desfasurare a procesului de testare, Furnizorul va realiza in urma analizei un plan de teste functionale pentru sistemul propus, precum si un plan de testare integrata a componentelor acestuia. Se va urmari cu precadere testarea functionalitatilor stabilite de comun acord cu Autoritatea Contractanta in cadrul etapei de analiza si proiectare.
Ofertantul trebuie sa descrie in detaliu metodologia dupa care vor derula activitatile de testare interna si vor demonstra integrarea acestor proceduri cu procedurile de analiza si proiectare.
Ofertantul trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapei de testare interna.

3.2.5 DEPLOYMENT

Oferta trebuie sa cuprinda serviciile de deployment a echipamentelor hardware la sediile consulare ale Autoritatii Contractante indicate in Anexa 1.
Pentru asigurarea unei bune desfasurari a procesului de deployment, Furnizorul va realiza in urma analizei un plan de deployment optim care sa tina cont de distantele fizice intre locatii, echipamentele de livrat la fiecare locatie, instalarea si punerea in functiune a echipamentelor la aceste locatii, personalul local care va fi instruit privind operatiunile (minimale) de utilizare a acestor echipamente, etc. Acest plan va fi prezentat Autoritatii Contractanta in cadrul etapei de analiza si supus aprobarii acesteia.

3.2.6 GARANTIE SI SUPORTUL POST-PRODUCTIE

Furnizorul va prezenta detaliat in cadrul ofertei procedurile si metodele pe care le va utiliza pe durata perioadei de garantie si suport post-productie pentru solutiile software oferite. Pentru detalii privind perioadele de acordare a garantiei si suportului post-productie a se vedea prezentul document la cap. 3.4 – «Cerinte privind garantia si suportul post-productie».

- descrierea procedurilor aplicabile si a fluxurilor de lucru aferente;
- roluri si responsabilitati privind activitatile specifice de mentenanta si garantie;
- formulare utilizate;
- instrumente utilizate.

3.2.7 MANAGEMENTUL PROIECTULUI

Furnizorul va prezenta in cadrul ofertei metodologia de management de proiect pe care o va utiliza in implementarea proiectului.
Ofertantul trebuie sa prezinte intr-un capitol separat propria intelegere a proiectului si a serviciilor pe care trebuie sa le presteze. Acest capitol va include atat descrierea la nivel inalt a activitatilor, modalitatea in care aceste activitati vor fi duse la indeplinire si livrabilele produse in urma activitatii.
Ofertantul trebuie sa prezinte metodologia de proiect pe care o va folosi in desfasurarea intregii activitati de implementare a proiectului. Metodologia trebuie sa fie bazata pe metodologiile standard folosite in proiecte IT de mare anvergura. Aceasta metodologie trebuie sa acopere cel putin procedurile de lucru pe care ofertantul le va utiliza in timpul implementarii, modul in care isi va organiza echipa de implementare (numar de specialisti, sarcina fiecarui membru al echipei, pregatirea profesionala).

3.2.7.1 PLANUL PRELIMINAR DE PROIECT

In figura de mai jos este prezentat planul preliminar de proiect (estimativ).

	An de implementare 1												**An de implementare 2**		
Activitate Luna	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**
1. Managementul de proiect															
2. Activitatea de promovare si publicitate aferenta proiectului															
2.1 Organizare conferinta lansare proiect															
2.2 Editare, tiparire si distribuire materiale de informare															
2.3 Difuzare comunicate de presa															
2.4 Organizare conferinta finalizare proiect															
3. Dezvoltarea si implementarea solutiei informatice															
4.1 Analiza in vederea identificarii specificatiilor tehnice															
4.2 Proiectarea arhitecturii hardware si software necesare pentru implementarea portalului															
4.3 Instalarea si configurarea infrastructurii hardware-software															

necesara proiectului															
4.4 Dezvoltarea efectiva a componentelor portalului															
4.5 Testarea functionalitatii portalului si asistenta utilizatorilor pe perioada lansarii.															
4.6 Punerea in functiune a portalului.															
5.Instruirea personalului serviciului vize din cadrul MAE															

In cadrul ofertei, Ofertantul va prezenta un plan detaliat de implementare a sistemului, ce va extinde planul preliminar de proiect. Acest plan va fi evaluat din punct de vedere al indeplinirii sarcinilor necesare implementarii sistemului in conformitate cu cerintele specifice din prezentul Caiet de Sarcini. Planul detaliat va fi intretinut de Ofertantul castigator pe parcursul proiectului si va tine seama de toate constrangerile impuse de proiect precum si de punctele de referinta ale acestuia.

3.3 CERINTE PRIVIND INSTRUIREA

Oferta trebuie sa cuprinda servicii de instruire a personalului desemnat din cadrul Autoritatii Contractante in vederea utilizarii si administrarii sistemului e-VIZA.
Ofertantii vor livra un plan de instruire si de asemenea vor livra materialele necesare instruirii atat in format electronic, cat si in format tiparit. Instruirea se va realiza exclusiv in limba romana.
Se estimeaza necesitatea instruirii in sali de curs de catre instructori specializati sau prin intermediul unui sistem tip eLearning a unui numar de 20 utilizatori cheie, 500 de utilizatori finali, precum si a 4 administratori de sistem. Perioada de instruire in sali de curs este de minim 5 zile , respectiv minim 4 ore (nu mai mult de 8 ore/zi) iar realizarea instruirii se va efectua in perioada finala a implementarii sistemului e-VIZA. Atat salile de curs necesare instruirii cat si echipamentele necesare vor fi puse la dispozitie de catre Autoritatea Contractanta.

3.3.2 COMPONENTA ELEARNING

In plus fata de instruirea in sali de curs sustinuta de instructori specializati, ofertele trebuie sa includa si servicii de tip eLearning, mai precis sa puna la dispozitia Autoritatii Contractante o platforma specializata de eLearning si continutul necesar realizarii instruirii personalului desemnat. Categoriile de utilizatori ai platformei de eLearning vor fi:

- Personalul beneficiar cu rol de utilizator cheie al sistemului ;
- Personalul beneficiar cu rol de utilizator final al sistemului ;
- Personalul beneficiar cu rol de administrator al sistemului ;

Se estimeaza necesitatea instruirii unui numar total de aproximativ 300 de utilizatori ai sistemului informatic in cadrul platformei de eLearning. Numarul si structura exacta a utilizatorilor ce urmeaza a fi instruiti fie in sali de curs de catre instructori specializati, fie prin intermediul sistemului tip eLearning, urmeaza a fi stabilita in faza de analiza a proiectului.

3.3.3 CERINTE PRIVIND CONTINUTUL ELECTRONIC EDUCATIONAL

Se cere furnizarea de continut electronic educational pentru instruirea personalului privind utilizarea si exploatarea sistemului informatic integrat. Furnizorul va trebui sa asigure respectarea urmatoarelor cerinte minime si obligatorii:

- Ofertantul trebuie sa:
  - Precizeze componenta echipei de proiectare a continutului, care trebuie sa cuprinda specialisti in tipul de aplicatii informatice pentru care trebuie realizate cursuri
  - Demonstreze experienta in construirea de cursuri pentru aplicatii informatice ;
- Continutul electronic trebuie sa fie adecvat utilizarii in mai multe scenarii, astfel :
  - pentru angajatii noi sau care folosesc pentru prima oara aplicatiile informatice vizate, continutul va servi ca un curs care ii initiaza;
  - pentru angajatii deja familiarizati cu aplicatiile, continutul va servi ca ajutor la cerere, pentru a explica activitati sau procese specifice.
- Cerinte functionale :
  - Cursantul va avea la dispozitie indexul cursului, care va contine scenariile de utilizare pentru aplicatia vizata, cu taskuri si subtaskuri
  - Continutul educational trebuie sa cuprinda:
    - Prezentarea fiecarui modul din cadrul portalului si a scenariilor uzuale in cadrul acestuia. Se vor prezenta scenarii adaptate pe rolurile existente in cadrul portalului
    - Ocazii de a testa intr-un mediu sigur cele mai importante elemente din scenariile de mai sus
    - Continutul trebuie sa aiba o structura modulara si sa permita navigarea intre module, existand mai multe cai de parcurgere (indicate sau la alegere
  - Fiecare curs trebuie sa expuna scenariile de utilizare a aplicatilor informatice sub forma de simulare a aplicatiei si teste.
  - Cursantul va fi ghidat in curs si in functie de calea de invatare prescrisa de autorul cursului. Pentru definirea cailor de parcurgere a materialului se vor folosi facilitatile de organizare, secventare si navigare oferite de SCORM 2004
- Standarde :
  - Cursurile trebuie sa fie compatibile cu standardul SCORM 2004. Astfel, cursurile trebuie sa functioneze pe orice platforma de eLearning compatibila cu standardul SCORM 2004, fara alte modificari sau ajustari
  - Conformitatea cu SCORM 2004 trebuie demonstrata prin testarea cu SCORM 2004 Conformance Test Suite (www.adlnet.gov)
- Livrarea continutului :
  - Continutul trebuie furnizat sub forma de arhiva conforma cu standardul SCORM 2004

3.3.4 CERINTE FUNCTIONALE ALE PLATFORMEI DE ELEARNING

- Modularitate:
  - Platforma de eLearning trebuie sa permita desfasurarea de sesiuni de instruire de tip asincron si desfasurarea de sesiuni de testare de cunostinte. In acest sens se cere ca platforma sa fie modulara, modulele de instruire asincron si testare putand functiona separat sau impreuna.
- Planificarea sesiunilor de instruire / testare:
  - Platforma trebuie sa permita crearea de sesiuni de instruire / testare, pentru care sa se poata stabili urmatorii parametri:
    - materialul de studiat (acesta trebuie sa poata fi ales din continutul deja existent in platforma, sau sa fie importat in momentul planificarii) / structura testului
    - perioada de valabilitate a sesiunii de instruire / testare

        - conditiile de inscriere a cursantilor, inclusiv modalitati de a conditiona inscrierea acestora de aparententa la un grup si / sau aprobarea unei anumite persoane desemnate
- Instruire de tip asincron:
    - Platforma trebuie sa permita cursantilor sa acceseze materialele de curs in orice moment, de cate ori si pentru cat timp doresc
    - Ghidarea cursantului prin continut trebuie sa se faca in functie de rezultatele acestuia si de metoda didactica gandita de autorul cursului
- Crearea testelor:
    - Platforma de eLearning trebuie sa ofere functionalitatea de creare de teste cu intrebari preluate aleator din bancuri de intrebari organizate in functie de anumite criterii considerate relevante
- Rapoarte si statistici:
    - Se cere ca platforma de eLearning sa ofere rapoarte si statistici atat pentru sesiunile de instruire cat si pentru sesiunile de testare. Aceste rapoarte trebuie sa includa informatii despre:
        - statistici pe utilizator referitoare la starea activitatilor sale de invatare (timpul de invatare, accesarea cursului)
        - rapoarte de progres pentru fiecare activitate de invatare in parte
        - activitatile terminate, abandonate si neincepute
        - rapoarte individuale si pe grupuri de utilizatori privind rezultatele la teste
    - Platforma trebuie sa permita crearea de rapoarte customizate
- Import de cursuri SCORM 2004:
    - Platforma treabuie sa permita importul cursurilor create conform standardului SCORM 2004

3.3.5 SPECIFICATII TEHNICE PRIVIND PLATFORMA DE ELEARNING

- Platforma sa suporte utilizatori din domeniu (iar datele utilizatorilor trebuie sa fie preluate/actualizate dintr-un LDAP)
- Platforma trebuie sa fie conforma cu standardul SCORM 2004.

3.3.6 TUTORIALE PENTRU UTILIZAREA SISTEMULUI INFORMATIC INTEGRAT

In vederea incurajarii utilizarii aplicatiilor de care personalul desemnat de catre institutia beneficiara, furnizorul va realiza 3 tutoriale de utilizare a acestora pentru fiecare grupa de utilizatori in parte (administratori, utilizatori cheie si utilizatori finali). Aceste tutoriale trebuie sa acopere urmatoarele aspecte:

- O prezentare generala a sistemului e-VIZA, a functionalitatilor acestuia si a meniurilor principale
- Cele mai uzuale scenarii de utilizare
- Un ghid care sa contina informatii despre cum se va reactiona in anumite situatii intalnite in cadrul aplicatiei (de exemplu care sunt pasii care trebuie urmati in cazul aparitiei unei erori)
- Tutorialele trebuie sa fie prezentate intr-un format multimedia interactiv si trebuie sa contina cel putin urmatoarele elemente:
    - Text
    - Imagini
    - Filme animate
    - Simulare interactiva aplicatie software
    - Elemente cu rol de evaluare si fixare a cunostintelor
- Tutorialele trebuie sa poata fi parcurse in mod individual (in ritm propriu, fara a necesita prezenta unui trainer) Tutorialele trebuie sa aiba o structura modulara si sa permita navigarea intre module, existand mai multe cai de parcurgere (indicate sau la alegere)
- Tutorialele trebuie sa permita reutilizabilitatea elementelor

- Tutorialele trebuie sa aiba Index - lista titlurilor obiectelor de invatare intr-un mod asemanator cuprinsului unei carti. Titlurile sunt prezentate sub forma de link, astfel incat la click pe acest link sa se treaca direct la obiectul de invatare respectiv
- Tutorialele trebuie sa cuprinda functionalitati de Glosar: prezinta o lista de termeni si definitiile acestora si de asemenea sa ofere posibilitatea de a cauta cuvintele din lista
- Tutorialele se vor realiza in limba romana

3.4 CERINTE PRIVIND GARANTIA SI ASISTENTA POST-IMPLEMENTARE

3.4.1 GARANTIE SOFTWARE PENTRU PRODUSELE NON COTS

Perioada de garantie pentru toate dezvoltarile din cadul componentelor software oferite trebuie sa fie de 36 de luni de la data de acceptanta provizorie a sistemului informatic.
Serviciile de garantie oferite vor include minim urmatoarele:

- Diagnosticarea, izolarea si remedierea defectelor software semnalate de catre Autoritatea Contractanta
- Asistenta cu instalarea de actualizari si noi versiuni de programe puse la dispozitie de catre producatorii de software tip COTS (Sistem de Operare, Sistem Relational de Baze de Date, Componenta de Portal , etc.) care vor putea fi aplicate fara sa afecteze functionarea sistemului sau sa necesite noi dezvoltari ale componentelor sistemului
- Asistenta acordata Autoritatii Contractante pentru aplicarea corectiilor ca urmare a remedierii defectelor semnalate

Garantia privind dezvoltarea software din cadrul proiectului trebuie sa fie disponibila in toate zilele lucratoare 24x7) si trebuie sa garanteze remedierea defectelor software semnalate de Autoritatea Contractanta conform urmatorului tabel de gravitate (SLA):

Nivel de gravitate	Descriere	Reactie initiala a Ofertantului Castigator (ore)	Timp total de solutionare a defectului software (zile lucratoare)
1	Defect major, sistemul nu este functional	1	1
2	Defect mediu, unele functii sau componente ale sistemului nu sunt functionale	4	2
3	Defect minor, unele functii sau componente ale sistemului sunt afectate dar functionale	8	4

Ofertantii vor descrie in oferte planul detaliat privind garantia pentru dezvoltarea software asigurata in cadrul proiectului.

3.4.2 GARANTIE HARDWARE

Perioada de garantie pentru toate produsele hardware oferite trebuie sa fie de 36 de luni de la semnarea acceptantei provizorii de catre Autoritatea Contractanta.
Garantia pentru componentele hardware din cadrul proiectului, oferita la fata locului trebuie sa fie disponibila in toate zilele lucratoare (24x7). Ofertantul castigator va trebui sa se prezinte la fata locului pentru constatarea defectiunii in maxim 4 ore de la semnalarea acesteia de catre Beneficiar, diagnosticarea defectiunii se va face in maxim 8 ore de la constatarea acesteia, iar inlocuirea sau repararea componentelor hardware defecte se va face in decurs de 10 zile calendaristice de la diagnosticarea defectiunii, daca defectiunea nu aduce cu sine nefunctionarea sistemului, caz in care se va realiza in maxim 4 ore.

Ofertantii vor descrie in oferte planul detaliat privind garantia hardware asigurata in cadrul proiectului.
In cazul echipamentelor instalate in posturile consulare (din strainatate), garantia va fi asigurata in tara (in Romania) in locatia centrala, dar costurile aferente transporturilor echipamentelor de la / la oficiile consulare vor fi in sarcina ofertantului castigator.
In cazul defectarii enitatilor de stocare (HDD-uri), acestea nu se vor returna furnizorului ci vor fi distruse de catre beneficiar.

3.4.3 ASISTENTA POST-IMPLEMENTARE

Se solicita servicii de suport post-productie pentru componentele software ale sistemului pentru o perioada de 12 luni de la trecerea in productie a sistemului informatic. Serviciile vor fi disponibile telefonic in toate zilele lucratoare (24/7), prin posta electronica sau printr-un sistem tip help-desk. De asemenea, pentru a asigura o buna functionare a sistemului informatic, ofertantul va asigura pe durata suportului post-productie, prezenta unei echipe de specialisti la sediul Autoritatii Contractante, daca va fi cazul. Ofertantii vor descrie detaliat in oferta tehnica modul in care vor asigura serviciile de suport post-productie pentru sistemul informatic.

3.5 CERINTE PRIVIND ASIGURAREA CALITATII

Testarea sistemului trebuie sa verifice ca sistemul informatic integrat ce se va implementa este functional in intregime si toate componentele functioneaza conform specificatiilor de implementare.
Scenariile de testare vor fi intocmite impreuna cu reprezentantii desemnati ai Autoritatii Contractante. Testele standard de punere in functiune se vor efectua in prezenta reprezentantilor Autoritatii Contractante, si constau in identificarea si verificarea cantitativa si calitativa a componentelor.
Ofertantul trebuie sa prezinte procedura de testare si acceptanta pe care o propune spre folosire in cadrul prezentului proiect. Aceasta procedura are statutul de recomandare, Autoritatea Contractanta putand solicita modificarea acesteia in cazul in care se dovedeste necesar.
Teste preliminare:

- Beneficiarul va realiza impreuna cu reprezentanti ai Furnizorului teste asupra tuturor componentelor livrate (hardware si software) in conformitate cu instructiunile de instalare si folosire. Criteriul de succes il reprezinta trecerea cu succes a tuturor testelor si verificarilor recomandate de producator. Dupa instalarea cu succes a tuturor echipamentelor hardware si software si dupa testele preliminare, se va semna un certificat de instalare.

Teste operationale:

- Beneficiarul (asistat de catre Furnizorului) va realiza toate testele pe intregul sistem si pe componentele acestuia in conformitate cu Planul de Teste realizat de Furnizor si agreat de Beneficiar.
- Planul de testare va cuprinde cel putin urmatoarele tipuri de teste:
    - Testare unitara – se verifica in intregime logica individuala a fiecarei componente, se verifica respectarea cerintelor functionale evidentiate in documentele de Analiza si Proiectare. Criteriu de succes – componenta trece toate testele functionale.
    - Testarea sistemului integrat – se verifica faptul ca fiecare interfata intre componente functioneaza corect din punct de vedere al consistentei datelor, al constrangerilor de timp, al validarilor de date si al gestiunii erorilor. Criteriul de succes – Toate grupurile de componente testate trec toate testele de interfatare.
    - Testarea de stres – se verifica faptul ca toate componentele sistemului si sistemul ca un intreg sunt capabile sa gestioneze cantitatile cerute de date si sa raspunda numarului cerut de utilizatori cu timpii de raspuns mentionati. Se vor defini limitele din punct de vedere al volumului de date, al numarului de utilizatori si al numarului de evenimente dupa care nivelul de raspuns se deterioreaza. Criteriul de succes: sistemul ca intreg este capabil sa serveasca numarul cerut de utilizatori si sa raspunda la cantitatea ceruta de date cu timpi acceptabili de raspuns. Sistemul este capabil sa gestioneze varfurile prestabilite pentru numar de utilizatori

si volum de date cu scaderi acceptabile ale timpului de raspuns. In situatiile in care sistemul se blocheaza nu se pierd date critice, unde este cazul operatiile sunt efectuate tranzactional.

- Planul de testare de nivel inalt va fi prezentat odata cu oferta. Planul detaliat de testare, insotit de scenariile de testare, va fi realizat de catre Furnizor si aprobat de Beneficiar dupa etapa de Proiectare.

4. CERINTE PRIVIND SERVICIILE DE INFORMARE SI PUBLICITATE ALE PROIECTULUI

Activitatea de informare si publicitate a proiectului are scopul de a asigura vizibilitatea si promovarea proiectului.
Materialele publicitare vor respecta indicatiile tehnice mentionate in Manualul de Identitate Vizuala pentru PODCA.
Serviciile si produsele solicitate prin prezentul Caiet de sarcini, aferente Activitatii de informare si publicitate sunt:

A. Servicii pentru organizare conferinta lansare proiect si finalizare proiect
B. Editare, tiparire si distribuire materiale de informare
C. Difuzare comunicate de presa - publicitate in mass-media (elaborare, productie si difuzare)

In ansamblul lor, aceste activitati vor constitui elementele unei campanii de informare si publicitate bine coordonate, avand ca obiectiv general informarea corecta si pe cat posibil de completa, a publicului larg si a potentialilor beneficiari.
In scopul unei bune coordonari a proiectului, operatorul economic va asigura coordonarea si cadrul logic al activitatilor prin:
- numirea unor coordonatori de echipa cu experienta in domeniu, pentru fiecare tip de activitate;
- numirea unui manager de proiect, care va asigura coordonarea echipelor si va fi responsabil pentru intreaga campanie de informare si publicitate;
Beneficiarul, avand suportul consultantului, va implementa masurile de informare si publicitate la nivelul proiectului. Masurile de informare si publicitate nu vor fi continue dar vor fi asigurate pe intreaga perioada de implementare a proiectului. In cadrul activitatilor de informare si publicitate, se vor realiza si vor fi furnizate materiale informative si promotionale necesare derularii etapelor proiectului si a conferintelor de informare.

4.1 SERVICII PENTRU ORGANIZARE CONFERINTA LANSARE PROIECT SI FINALIZARE PROIECT

In primele doua luni de implementare a proiectului, se va stabili derularea unei conferinte dedicata lansarii proiectului, la care vor fi invitati reprezentanti ai AMPODCA, reprezentanti ai institutiilor si autoritatilor relevante prin activitatea desfasurata fata de obiectivele proiectului, cat si reprezentati ai societatii civile si cetateni, avand in vedere ca sunt direct vizati de efectele benefice ale realizarii acestui proiect.
In cadrul conferintei de lansare se vor sustine discursuri de prezentare a proiectului si a modului in care proiectul va aduce beneficii in randul grupului tinta. De asemenea, vor fi invitati si reprezentantii AMPODCA sa sustina discursuri/prezentari referitoare la oportunitatile oferite prin intermediul PODCA.
La finalul proiectului, va fi organizata o conferinta de prezentare a rezultatelor obtinute pe parcursul proiectului, precum si a metodelor prin care echipa propune continuarea / multiplicarea acestor rezultate.
Conferintele vor avea o durata estimativa de 4-5 ore si se vor desfasura la o locatie din Bucuresti pusa la dispozitie de catre Beneficiar. Sala va avea capacitatea de a gazdui cel putin 50 de persoane si va fi dotata cu instalatie de sonorizare (microfon fix si 2 microfoane mobile), ecran de proiectie de mari dimensiuni, video proiector.
Lista persoanelor si a reprezentantilor institutiilor/ organizatiilor ce urmeaza a fi invitate, pe baza carora operatorul economic va elabora lista finala a invitatilor, va fi avizata si dupa caz, completata de catre

Autoritatea Contractanta. De asemenea, lista institutiilor mass-media care vor fi invitate, va fi realizata de catre operatorul economic in colaborare cu Autoritatea Contractanta.
Operatorul economic va transmite prin fax (cu cel putin 2 saptamani inainte de fiecare eveniment) invitatiile personalizate catre potentialii beneficiari si institutiile/ autoritatile/ organizatiile sau actorii locali (in functie de tipul conferintei si in baza listei invitatilor definitivata anterior impreuna cu Autoritatea Contractanta).
Dupa ce va realizeaza follow-up-ul si va obtine confirmarile, prestatorul va intocmi *tabelul participantilor* - un tabel nominal cu institutiile/ organizatiile si firmele care au decis sa trimita reprezentanti la eveniment si datele personale ale celor care au confirmat participarea.
Numarul de participanti estimati a lua parte la o conferinta este de 50 de persoane.
In etapa de pregatire a evenimentelor, operatorul economic va avea intalniri de informare si colaborare cu Beneficiarul, ori de cate ori va fi necesar, pentru punerea la punct a tuturor detaliilor
Conferintele vor fi anuntate in mass media prin intermediul unui comunicat de presa cu cel putin o saptamana inainte de data programata pentru derularea conferintelor. Pentru aceste evenimente, operatorul va pregati un *comunicat de presa* (care va fi agreat din timp cu AC, multiplicat si diseminat in timpul evenimentului). pentru a asigura o promovare/diseminare eficienta a proiectului
Prestatorul va asigura servicii complete de catering pe durata conferintei si va fi responsabil de toate aspectele legate de organizarea pauzelor.
Serviciile de catering vor contine :

- pentru pauza de pranz: gustari reci si calde, patiserie, desert, cafea si racoritoare
- pentru pauza de cafea: cafea, sucuri, apa gazoasa si plata

4.2 EDITARE, TIPARIRE SI DISTRIBUIRE MATERIALE DE INFORMARE

Operatorul economic va realiza conceptia, executia grafica si productia materialelor de informare conform specificatiilor tehnice detaliate mai jos. Livrarea materialelor se va face la sediul beneficiarului iar costurile de transport vor fi suportate de catre prestator.
Materialele se vor realiza numai dupa primirea acceptului (bunului de tipar) din partea beneficiarului.
Etapele privind realizarea materialelor de informare

- Realizare machete materiale publicitare: conceptie grafica si editare
- Printare si inscriptionare materiale promotionale machetate

Se vor executa urmatoarele materiale de informare:
Caracteristicile tehnice ale produselor sunt prezentate in urmatoarul tabel:

Nr. Crt.	Item	Caracteristici tehnice	Cantitate
1	Autocolante	Format: 50 x 90 mm Suport: hartie autocolanta Tipar: policromie fata	444 buc
2	Banner "Panou informativ"	Descriere: coperta + 4 pag Format deschis: A3 Format inchis: A4 Suport coperta si interior: hartie dublu cratat mata de 250 g/mp Tipar coperta si interior: policromie fata/verso Finisare: capsare	1 buc
3	Brosura	Dimensiune A5, nr. pagini aprox.10, policromie copertile 1 si 4, policromie pagini interioare, creatie machete	500 buc
4	Agenda	Descriere: coperti + 60 file Format file: A5 Coperta: mucava de 2 mm pe care se casereaza hartie dublu cratat mata de 150 g/mp pe ambele fete la coperta , policromie fata, plastifiat mat	500 buc

		File: offset satinat de 80g Tipar file: o culoare fata/verso (grafica identica) Finisare :spira metalica neagra	
5	Pix	Descriere: din plastic, culoare alba Imprimare: o culoare la o pozitie	500 buc
6	Afis	Format: 47 x 67 cm Suport: hartie dublu cratat mata de 150 g/mp Tipar: 4+0	500 buc

Brosurile utilizate pe parcursul implementarii proiectului si pentru pentru conferinta de lansare si finala a proiectului, vor trebui sa indeplineasca urmatoarele cerinte:

- Elaborate in limba romana, intr-un stil accesibil, cu reprezentari grafice unde este cazul.
- Color, calitate a hartiei si grafica buna

Cuprins:

- Sa cuprinda in mod obligatoriu elementele de identitate vizuala ale proiectului;
- Cuvant inainte echipa de proiect/manager
- Sa cuprinda date despre proiect: scop general, obiective, activitati, durata de implementare, rezultate asteptate, impactul asteptat; aceste informatii vor fi puse la dispozitia Prestatorului de catre Beneficiar, iar Prestatorul le va prelucra si le va sintetiza astfel incat sa respecte formatul;
- Sa cuprinda mesaje clare referitoare la: dezvoltarea durabila / mediu si egalitatea de sanse;
- Sa cuprinda date de contact ale echipei de proiect;
- Sa cuprinda date referitoare la Beneficiar si la PODCA;
- Sa cuprinda o detaliere a principalelor activitati din proiect;
- Sa cuprinda date referitoare la rezultatele urmarite prin activitatile proiectului;

Beneficiarul va aproba forma finala a materialelor informative elaborate de prestator, in colaborare cu echipa de management a proiectului.
Ofertantii vor prezenta in oferta tehnica toate caracteristicile si specificatiile tehnice pentru produsele ofertate, astfel incat sa poata demonstra conformitatea acestora cu specificatiile solicitate in caietul de sarcini.

Ofertantii au obligatia sa respecte in totalitate specificatiile tehnice prevazute in prezentul caiet de sarcini.
Prestatorul se va asigura ca in elaborarea materialelor va fi respectata legislatia privind copywriting-ul, toate documentele elaborate in proiect devenind proprietatea exclusiva a beneficiarului.
Toate materialele elaborate in cadrul proiectului vor avea o imagine vizuala si grafica armonizata, astfel incat sa fie asigurat conceptul unitar al proiectului.

4.3 DIFUZARE COMUNICATE DE PRESA - PUBLICITATE IN MASS-MEDIA (ELABORARE, PRODUCTIE SI DIFUZARE)

Pe parcursul derularii proiectului prestatorul va asigura elaborarea si difuzarea a 2 comunicate de presa pentru a asigura diseminarea rezultatelor proiectului in randul grupului tinta, si a tuturor celor interesati de stadiul si evolutia proiectului.
Comunicatele de presa se vor difuza pe diferite canale mass-media, atat in presa scrisa (grupuri de discutii, site-ul oficial al proiectului, etc) cat si in cadrul evenimentelor si conferintelor.

5. ALTE MENTIUNI

Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu

usurinta a tipului de produs si nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse, aceste specificatii vor fi considerate ca avand mentiunea sau echivalent.
Caietul de sarcini face parte integranta din documentatia pentru atribuirea contractului si constituie ansamblul cerintelor pe baza carora se elaboreaza de catre fiecare ofertant propunerea tehnica. Caietul de sarcini contine, in mod obligatoriu, specificatii tehnice. Toate cerintele exprimate in Caietul de sarcini sunt minime si obligatorii.
Ofertele care nu satisfac in totalitate cerintele caietului de sarcini vor fi declarate neconforme si vor fi respinse.