Caiet de Sarcini

Achizitia publica a unei baze de date legislative si a serviciilor si echipamentelor necesare implementarii acesteia

Proiectul Implementarea portalului N-Lex

Str. Apolodor nr. 17, sector 5, 050741
Bucureşti, România
www.just.ro

Cuprins

1. Informatii generale

1.1. Autoritatea Contractanta

Ministerul Justitiei (MJ) este organul de specialitate al administratiei publice centrale, cu personalitate juridica, in subordinea Guvernului, care contribuie la buna functionare a sistemului judiciar si la asigurarea conditiilor infaptuirii justitiei ca serviciu public, apararea ordinii de drept si a drepturilor si libertatilor cetatenesti.

1.2. Descrierea Proiectului

Denumirea Proiectului: Implementarea portalului N-Lex (cod SMIS 32913)
Proiectul este cofinantat din Fondul Social European, prin Programul Operational „Dezvoltarea Capacitatii Administrative" (PODCA)

Axa prioritara 2 – Imbunatatirea calitatii si eficientei furnizarii serviciilor publice, cu accentul pus pe procesul de descentralizare
Domeniul de interventie 2 – Imbunatatirea calitatii si eficientei furnizarii serviciilor
Operatiunea: Folosirea mecanismelor electronice, de exemplu, portaluri internet si baze de date.

Scopul proiectului „Implementarea portalului N-Lex" este de a rezolva o problema majora cu care se confrunta, la momentul actual, societatea romaneasca: accesul liber la legislatie – element esential pentru crearea unui mediu adecvat desfasurarii raporturilor juridice de orice tip.

Astfel, in prezent, nu exista o modalitate de accesare gratuita a legislatiei nationale, in forma actualizata si consolidata, de altfel o conditie esentiala pentru asigurarea cunoasterii si respectarii legii de catre fiecare individ.

In consecinta, a fost identificata necesitatea crearii unui sistem informational legislativ care sa permita accesul rapid si neingradit, al oricarei persoane interesate, la legislatia in forma actualizata, pentru a se elimina astfel ambiguitatile rezultate din inflatia si instabilitatea normativa la nivel national, facilitandu-se identificarea si aplicarea actelor normative.

Avand in vedere cele mentionate, acest proiect vine sa raspunda problemei identificate, prin dezvoltarea unei aplicatii electronice de legislatie care va permite si va facilita accesul gratuit al tuturor celor interesati la aceasta baza de date legislativa, ce va contine forma consolidata si actualizata a actelor normative si fisa acestora. De asemenea, pentru asigurarea stabilitatii si acuratetei informatiilor furnizate, aceasta baza de date va fi actualizata periodic, in functie de modificarile legislative survenite.

Prin urmare, acest proiect, din perspectiva nationala, va contribui la o mai buna cunoastere a legislatiei atat de catre publicul larg, cat si de alte entitati (institutii publice, specialisti in drept, societati comerciale, universitati etc.), contribuind, totodata, la ameliorarea securitatii si certitudinii juridice a informatiilor si datelor furnizate.

In ceea ce priveste dimensiunea europeana a proiectului, mentionam ca la nivelul Uniunii Europene (UE), la initiativa Grupului de informatica juridica a Consiliului UE – JURINFO (actualmente Grupul de lucru E-Law), in vederea identificarii unei solutii electronice viabile pentru statele membre, care sa asigure accesul la legislatie, Oficiul pentru Publicatii al UE, in colaborare cu statele membre, a pus in practica, in anul 2006, proiectul european N-Lex. Prin portalul N-Lex se acorda acces gratuit la legislatiile nationale ale statelor membre, portalul fiind conceput pe baza unei tehnologii de comunicare interne, ce permite accesarea directa a bazelor de date legislative nationale, rezultatele cautarilor venind direct de la sursa.

Daca in faza initiala a proiectului european, portalul N-Lex oferea acces la bazele legislative nationale ale doar patru state membre, in momentul de fata numarul acestora a ajuns la 23, Romania nefacand inca parte din acest proiect european.

Astfel, acest proiect va raspunde, de asemenea, cerintelor existente la nivel european in ceea ce priveste accesul la legislatie, conform obligatiilor asumate de Romania in calitate de stat membru al UE, inclusiv în ceea ce priveşte interconectarea aplicației legislative naționale cu portalul N-Lex.

1.3. Obiectivul Proiectului

Obiectivul proiectul este imbunatatirea calitatii si eficientei serviciilor furnizate catre cetateni si alinierea la standardele europene.

1.4. Scop

Scopul proiectului este dezvoltarea unei aplicatii electronice de legislatie ce va permite accesul in forma gratuita al cetatenilor si al altor entitati la o baza de date legislativa nationala si interconectarea aplicatiei electronice de legislatie (a bazei de date legislative) cu portalul european de legislatie N-Lex.

1.5. Obiectul achizitiei

Obiectivul general al prezentului contract este achizitionarea unei baze de date nationale legislative care sa cuprinda fisa actelor normative si forma actualizata a actelor normative, dezvoltarea unei aplicații electronice care să permită accesul neîngrădit la baza națională legislativă, implementarea acesteia din urmă in aplicatia software dezvoltata şi interconectarea cu portalul N-Lex, precum şi instruirea personalului de specialitate IT din cadrul Ministerului Justiției cu privire la administrarea noii aplicații electronice.

In cadrul proiectului vor fi furnizate si echipamentele hardware, de comunicatii si licente software necesare implementarii cu succes a solutiei informatice.

2. Sistemul N-LEX

2.1. Utilizatorii

Proiectul isi propune sa prezinte intr-un mod organizat, structurat si unificat legislatia romaneasca, actualizată la zi.

Beneficiarii proiectului informatic se impart in mai multe categorii:

- Angajati din cadrul Ministerul Justitiei si al institutiilor subordonate precum și al Curtilor de Apel, Tribunalelor, Judecatoriilor etc. care se vor conecta la portalul solutiei si vor avea un acces privilegiat in functie de rolul pe care il detin, consumatori de continut sau editori;

- Angajati ai altor institutii publice, nesubordonate Ministerului Justitiei, care se vor conecta la portalul solutiei prin intermediul retelei STS si vor avea acces la portalul intern al solutiei;

- Publicul larg – persoane fizice si juridice interesate care vor accesa continutul sistemului prin intermediul portalului legislativ si vor putea consulta documente legislative emise de autoritatile romanesti.

- Sisteme informatice – aplicatii informatice la nivel european care se vor interconecta cu sistemul pentru a extrage informatii din portalul legislativ.

In functie de aceste categorii, sistemul va oferi informatii si servicii electronice catre urmatoarele categorii de utilizatori:

- **Utilizatori interni editori** – sunt persoane din cadrul Ministerului Justitiei, cu drepturi de creare de continut, care vor accesa sistemul din intranet si vor mentine la zi baza de date legislativa, publicand documente nou aparute si invalidandu-le pe cele abrogate; de asemenea vor avea drepturi pentru aplicarea de pachete de actualizare continut, specifice bazei de date legislativă.

- **Utilizatori interni administratori aplicatie** – sunt persoane din cadrul Ministerului Justitiei care vor accesa sistemul din intranet pentru a monitoriza sistemul si a realiza actiuni de mentenanta.

- **Utilizatori interni neautentificati** - sunt persoane din cadrul institutiilor subordonate Ministerului Justitiei, al instanțelor judecătorești si al celorlalte instituții publice, care vor accesa sistemul din intranet si vor avea acces la portalul legislativ.

- **Utilizatori externi neautentificati** – sunt persoane fizice si juridice care vor accesa sistemul din internet si vor putea consulta legislatia romaneasca publicata in sistem.

- **Consumatori de servicii web** - aplicatii informatice care vor accesa sistemul din internet intr-un mod securizat si vor extrage informatia prin intermediul unor servicii web pe care sistemul dezvoltat le va publica.

2.2. Cerintele generale ale sistemului

Ofertantul trebuie sa raspunda punctual la toate cerintele cuprinse in prezentul Caiet de Sarcini si sa detalieze in propunerea sa tehnica modurile si mijloacele prin care solutia ofertata indeplineste aceste cerinte, astfel incat comisia de evaluare sa aiba posibilitatea evaluarii acesteia in mod cat mai informat. In cazul in care solutia ofertata, detaliata in Oferta Tehnica, nu ofera informatii complete, prin detalierea raspunsului la cerinte, sau nu indeplineste cerintele exprimate in Documentatia de Atribuire, comisia de evaluare poate sa declare solutia ca fiind necorespunzatoare.

Informatiile din propunerea tehnica vor fi prezentate astfel incat sa fie posibila identificarea cu usurinta a corespondentei cu specificatiile tehnice minime din Caietul de Sarcini. Ofertele care nu vor include informatiile relevante sau care nu raspund corect si complet tuturor acestor cerinte vor fi respinse ca neconforme.
Oferta tehnica va include prezentarea solutiei oferite, cu detalii privind arhitectura hardware si software, serviciile aferente, tehnologiile folosite si solutiile tehnice propuse pentru cerintele definite in Caietul de Sarcini.
Pe de alta parte, oferta tehnica va contine raspunsul punct cu punct la cerintele din caietul de sarcini. Raspunsul negativ sau lipsa raspunsului la oricare din cerintele minimale din Caietul de Sarcini va duce la respingerea ofertei ca neconforma.
Un simplu raspuns de confirmare din partea Ofertantului cu privire la respectarea cerintelor din Caietul de Sarcini, fara precizarea exacta a modalitatii de indeplinire, nu este acceptat. Se vor prezenta dovezi concrete in sprijinul afirmatiilor din oferta cu detalii tehnice, imagini si link-uri de pe site-ul producatorului, acolo unde este cazul.
Sistemul trebuie construit pe o platforma tehnologica avansata, in jurul conceptului de portal informational pentru a asigura un punct unic de acces la functionalitati si avand urmatoarele caracteristici:

- Interfata utilizator de tip WEB;
- Acces la toate functionalitatile din interfata (configuratie de tip portal);
- Administrare unica pentru toate componentele;
- Securitate integrata;
- Sa fie parametrizabil intr-un grad care sa elimine, pe cat posibil, scrierea de programe si crearea de tabele specifice client;
- Actualizarea informatiilor in sistem sa aiba loc in timp real si sa permita si descarcari de date intre diferite locatii;
- Verificarea automata a datelor introduse, pentru limitarea la maximum a posibilitatii de a introduce date eronate sau neverosimile sau de a opera functii/functionalitati gresite;
- In cazul aparitiei unor erori, sa permita trimiterea automata catre persoanele desemnate pentru interventii a erorii detaliate in vederea remedierii acesteia;
- Sa permita definirea campurilor de date obligatorii si optionale, precum si a regulilor de validare a datelor completate in aceste campuri;
- Sa existe un sistem de validare a introducerii datelor. Aplicatiile vor asigura calitatea datelor introduse, prin proceduri de validare (prin definirea campurilor obligatorii, a formatului acceptat pentru anumite campuri, a unor valori sau plaje de valori posibile pentru anumite campuri etc.);
- Sistemul trebuie sa aiba interfata utilizator in limba romana;

- Interfata-utilizator trebuie sa prezinte coerenta din punctul de vedere al elementelor de design (structura, fonturi, culori, meniuri, etc.) la nivelul intregului sistem;
- Interfata trebuie sa ofere cel puțin aceleasi functionalitati cu cele existente pe portalul european N-Lex si sa permita interogarea folosind conectori construiti pe modelul acestora.

Pentru implementarea si functionarea portalului legislativ este necesar ca infrastructura de comunicatii sa fie de inalta performanta, fiabila, scalabila si compatibila cu tehnologiile folosite in aplicatii. Se solicita ca aplicatia implementata sa asigure:

- **Modularitate** - Arhitectura sistemului va fi modulara putand fi usor extinsa cu noi functionalitati fara a perturba componentele existente si fara a necesita reorganizarea datelor existente in sistem, necesitand un efort de integrare minim. Conceptele de modularitate se vor mentine si pentru arhitectura fizica a aplicatiei. In functie de modificarile legislative la nivel national sau european, beneficiarul poate considera necesara adaugarea de noi componente la sistemul informatic integrat sau poate chiar noi aplicatii sau sisteme care necesita parte sau totala integrare la aplicatia curenta. Ofertantii vor realiza o solutie hardware care sa ofere posibilitatea extinderii si cu alte componente arhitecturale hardware.

- **Scalabilitate** - Sistemul trebuie sa permita scalarea pe orizontala si pe verticala fara a fi necesara rescrierea aplicatiilor. Din punct de vedere hardware sistemul trebuie sa permita:
  - Adaugarea de servere noi in clustere fara a modifica serverele existente
  - Adaugarea de resurse noi pe un singur server fara a modifica aplicatia;
- **Accesul simultan a mai multor utilizatori** – sistemul trebuie sa permita accesul utilizatorilor simultan la aceleasi resurse logice (documente), software (interfete web), hardware (servere).
- **Caracter deschis, interoperabilitate** - Sistemul informatic propus trebuie sa permita integrarea cu alte sisteme informatice nationale sau internationale (cel putin sistemul european N-LEX).

Avand in vedere numarul foarte mare estimat de utilizatori trebuie analizata situatia pe cele doua paliere:

- minister, institutii publice
- public

In ambele situatii Ofertantii trebuie sa ofere solutii concrete care sa vizeze reducerea acestui trafic:

- tinand cont de calitatea retelei internet
- numarul mare de accesanti
- marimea documentelor care urmeaza sa fie descarcate

2.3. Cerinte de disponibilitate si performanta

Solutia va asigura un mare grad de disponibilitate a aplicatiilor. Acest lucru se obtine prin oferirea de redundanta la nivelul:

- serverelor (prin folosirea de echipamente cu surse redundante si cu capacitati hot-plug, prin folosirea de hard-diskuri interne in configuratie RAID cu capacitati hot-plug);
- folosirea de arhitecturi de tip cluster pentru componentele sistemului (serverul de aplicatii si serverul de baza de date); arhitectura de tip cluster asigura disponibilitatea aplicatiilor ce ruleaza pe nodurile clusterelor si asigura practic disponibilitatea aplicatiilor pentru utilizatorii acestora chiar in cazul in care unul din nodurile (serverele) din cluster nu mai poate deservi, serviciile sale fiind preluate de celelalt nod fara un down-time notabil pentru utilizatori pana la repunerea in functie a serverului respectiv; clusterele vor fi capabile sa asigure „load balancing" si „fail-over" pentru partea de portal si extranet, respectiv „fail-over" pentru partea de Intranet;
- folosirea de storage centralizat de tip SAN (Storage Area Network) cu conexiune de tip Fiber Channel; conexiunea serverelor la storage-ul centralizat se va face in mod redundant;
- echipamentele de retea (switch-urile trebuie sa fie in perechi de 2 echipamente pentru asigurarea redundantei pentru a oferi o inalta disponibilitate a comunicatiei in reteaua locala a Data Center-ului in care sunt interconectate toate serverele ce gazduiesc aplicatiile tuturor sistemelor);
- echipamentele de asigurare a securitatii comunicatiilor trebuie sa fie intr-o configuratie cluster pentru redundanta pentru a evita ca acestea la randul lor sa poata fi un potential Single Point Of Failure intre utilizatorii sistemelor si acestea.

Solutia trebuie sa asigure redundanta tuturor componentelor principale de infrastructura software si hardware (inclusiv componente critice ale echipamentelor de calcul), in vederea asigurarii continuitatii furnizarii serviciilor.

Solutia trebuie sa asigure disponibilitate ridicata 24x7 pentru toate componentele sistemului cu suport pentru topologii de clustering de tip activ-activ.

Solutia trebuie sa permita stoparea temporara a unui nod pentru mentenanta si suport, sistemul in acest timp fiind disponibil pentru activitati normale (tehnologie cluster);

Sa asigure mecanisme de tip load balancing pentru balansarea dinamica a incarcarii sistemului intre resursele hardware si software instalate;

Scalabilitatea sistemului, pe fiecare nivel (baza de date, nivel prezentare, etc), sa fie garantata prin capabilitati de adaugare, in orice moment, de noi resurse hardware si software fara a impune stoparea temporara a serviciilor dezvoltate;

Pentru interogarile de cautare se solicita un timp de raspuns de maxim pentru 25 de utilizatori simultani:

- 2 secunde pentru cautarile in titlu
- 10 secunde pentru cautarile in textul documentelor

2.4. 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.
La nivel hardware, sistemul va fi protejat prin intermediul unor dispozitive de tip firewall care vor realiza filtrarea traficului catre si dinspre sistem.
La nivel software, sistemul va indeplini anumite cerinte din punct de vedere al securitatii, cum ar fi autentificarea unica a anumitor categorii de utilizatori si autorizarea acestora in sistem utilizand mecanisme specifice prin intermediul rolurilor si privilegiilor.
Utilizatorii vor avea acces numai la aplicatiile si informatiile pentru care au drepturi.
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.
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 de tip editor de continut nu va avea acces la baza de date decat prin intermediul aplicatiei. Acesta va putea vizualiza, modifica sau sterge doar acele date pentru care are drepturi acordate prin atributiile de serviciu.
Solutia trebuie sa realizeze impunerea politicilor de securitate intr-un mod uniform si centralizat, prin care se restrictioneaza cine la ce are acces, cand si de unde, si reprezinta componenta fundamentala a solutiei de securitate.
O astfel de componenta centralizata asigura faptul ca politicile sunt uniform si consistent aplicate pentru toate sistemele, furnizand cel putin urmatoarele functionalitati, dar nerestrictionat la acestea:

Autentificare: validarea credentialelor utilizatorilor. Accesul in aplicatie interna pentru editarea de continut se va realiza in urma unui proces de autentificare al utilizatorilor. Autentificare se va realiza prin recunoasterea de catre sistem a unei perechi de identificatori “nume utilizator/parola”, pereche definita anterior in sistem de catre personal calificat.

Autorizare: restrictionarea accesului utilizatorului numai la resursele la care trebuie sa aiba acces, conform rolului si responsabilitatilor acelui utilizator. Solutia trebuie sa permita aplicarea lor intr-un mod centralizat, dintr-un singur loc pentru toate resursele organizatiei.
Va permite utilizatorului sa citeasca, modifice si sa actualizeze informatiile aferente profilului propriu pe oricare dintre resursele pe care le poate folosi.
Sistemul sa permita delegarea drepturilor de acces indiferent de utilizator si rolul sau in sistem pe anumite perioade definite.
Sa suporte un mod flexibil si unitar pentru gestiunea drepturilor si politicilor de acces ale utilizatorilor la toate resursele sistemului integrat (aplicatii, module, categorii de informatie) prin definire, modificare, stergere, explorare.

Securizarea datelor

Sistemul va cuprinde si un mecanism de salvare si recuperare a datelor, care sa poata fi folosit in caz de nevoie. Din punct de vedere al securitatii datelor si a aplicatiei solutia trebuie sa permita:

- salvarea/restaurarea si arhivarea/dezarhivarea datelor in regim de lucru online.
- sa pemita salvarea totala si/sau partiala a bazei de date.
- sa permita efectuarea de backup automat intr-o forma unitara, centralizata si usor de administrat.
- sa permita efectuarea de backup numai pentru fisierele care au suferit schimbari de la ultimul backup si pentru fisierele nou create.

Instalarea patch-urilor disponibile pentru diferitele componente ale sistemului informatic se va face centralizat doar la nivelul serverelor respective (de aplicatii, de baze de date, etc.) fara a afecta functionarea corecta a acestuia.

Utilizatorul final va avea instalat doar un web browser prin care se vor accesa modulele solutiei software corespunzatoare drepturilor atribuite.

Utilizatorul final nu va avea acces pe baza de date decat prin intermediul aplicatiilor specifice Sistemului Informatic si in concordanta cu drepturile acordate.

Solutia trebuie sa asigure prin licentele oferite functionalitati de cluster la nivel de servere de web, aplicatii si baze de date.

Arhitectura solutiei software trebuie sa fie o arhitectura pe “N-tier”, din care nu pot lipsi urmatoarele componente:

a) Client web
b) Server de aplicatii
c) Baza de date

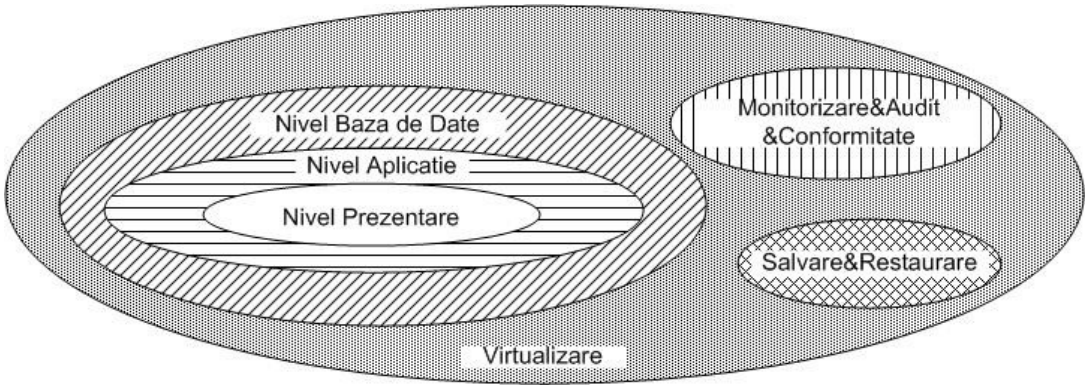
2.5. Arhitectura logica si functionala

Arhitectura Sistemului Informatic Integrat trebuie sa fie:

- **Modulara** – componente cu roluri si caracteristici/proprietati bine definite
- **Deschisa** - pot fi adaugate componente, proprietati noi). Modulele, (componentele) solutiei au caracteristici generale, adaptabile in functie de cerintele clientului.
- **Multi nivel** – arhitectura client - server, separata pe mai multe straturi

La nivel logic aplicatia de baza va fi organizata pe 3 niveluri functionale de baza la care se adauga 3 zone auxiliare de infrastructura si aplicatii:

- **Nivel Baza de date** - stocheaza si ofera informatii cu privire la documente legislative in format structurat.
- **Nivel Aplicatie Logica** – implementeaza functionalitatile de administrare a bazei de date legislative in tot ceea ce priveste managementul documentelor, introducerea de documente nou-aparute, marcarea documentelor expirate sau a portiunilor din documente expirate, marcarea relatiilor dintre documente, etc. De asemenea la acest nivel se realizeaza si administrarea utilizatorilor, a rolurilor si a drepturilor de acces.
- **Nivel Prezentare** - la acest nivel se realizeaza publicarea documentelor stocate la nivelul aplicatiei catre utilizatori, pe diferite canale de comunicatii (portal, servicii web)
- **Zona de Virtualizare** – cu rol in optimizarea infrastructurii tehnologice
- **Zona de Monitorizare, Audit si Conformitate –** cu rol in obtinerea de informatii cu privire la utilizarea aplicatiei si la modificarile suferite de sistemul informatic
- **Zona de Salvare si Restaurare –** cu rol in securizarea bazei de date legislative, precum si a configuratiei aplicatiei.



1.1.1.Cerinte nivel baza de date

Accesul la acest nivel se va realiza numai prin intermediul nivelului aplicatiei logice pentru modificarea continutului si prin nivelul de prezentare pentru extragerea de informatii legislative, utilizandu-se functionalitatile zonei de acces si securitate.

Continutul bazelor de date se refera la toate structurile logice care asigura cunoasterea si aplicarea corecta a legislatiei. Fara a limita structurarea informatiei, ele trebuie sa fie reprezentate de urmatoarele categorii:

a) baza de date legislativa, din decembrie 1989 pana in prezent (continutul Monitorului Oficial partea I si I bis);
b) baza de date legislativa anterioara decembrie 1989, continand principalele acte normative din acea perioada (abrogate sau partial in aplicare) si sunt utilizate in procedurile judiciare actuale sau in procesul de elaborare a actelor normative (de ex: actele normative in temeiul carora s-au operat exproprieri);
c) baza de date cuprinzand actualizarea fisei actelor normative (evidentierea modificarilor, completarilor, abrogarilor, aprobarilor si republicarilor actelor normative, a actelor normative subsecvente si a actelor normative conexe);
d) completarea actelor normative importante cu modificarile publicate de la ultima republicare in Monitorul Oficial; redarea acestei forme neoficiale, cu evidentierea diferitelor modificari intervenite si precizarea, la fiecare modificare, a actului normativ care modifica/completeaza.

Textul actelor normative trebuie sa fie redat cu diacritice, conform normelor de scriere la data emiterii, sa nu contina cuvinte gresite/omise, repetate, sau cu greseli de ortografie. Actualizarea bazelor de date mentionate anterior se va realiza in functie de importanta actelor publicate si urgenta cunoasterii noilor reglementari, fara a se depasi un interval de zile stabilit in faza de analiza dupa cum urmeaza:

a) *actualizarea legislatiei* se realizeaza prin preluarea in forma electronica integral a continutului *Monitorului Oficial partea I si I bis* in program. In program vor fi de asemenea publicate actele normative relevante in forma lor actualizata (neoficial, nerepublicate in M.Of.);

b) *actualizarea fisei actelor normative* se realizeaza prin evidentierea modificarilor, completarilor, *abrogarilor, aprobarilor si republicarilor actelor normative, a actelor normative subsecvente si a actelor normative conexe.*

Realizarea fiselor actelor normative va tine seama de toate modificarile, completarile, abrogarile, aprobarile si republicarile acestora. Criteriul de verificare a modului de realizare este raportarea la Repertoriul Legislativ publicat sub indrumarea Consiliului Legislativ

Baza de date trebuie sa poata raspunde interogarilor cu privire la continutul legislativ. Criteriile de cautare trebuie sa produca rezultate relevante pentru utilizatori, sa ofere liste de rezultate acceptabile si posibil de verificat (cat mai scurte). Pentru cresterea acuratetei rezultatelor este necesar ca textele sa contina diacritice. Daca prin criteriile simple rezultatele sunt implicit relevante, in cazul utilizarii criteriilor combinate relevanta este marcata de acuratetea criteriilor de cautare in:

- textul unui document
- textul tuturor documentelor

De asemenea cautarile vor permite utilizarea descriptorilor generici „?" si „*" cu respectarea cerintelor anterioare, caracterul "?" inlocuind orice caracter alfa-numeric, iar caracterul "*" inlocuind un grup de caractere alfa-numerice.

Actele legislative stocate la nivelul de baza de date trebuie sa fie:

- **redactate cu diacritice** (pentru a se asigura usurinta lecturii, acuratetea rezultatelor cautarilor de termeni/expresii si conform normei de prezentare a actelor comunitare redactate in romana si publicate pe siteurile **N-Lex**, **eur-lex**);
- sa aiba cuprins (pentru a usura orientarea in text , conform redactarii pe siteurile N-Lex, eur-lex) si posibilitatea de returnare a unei subsectiuni logice din document;
- sa nu aiba cuvinte omise, gresite, repetate, propozitii sau fraze trunchiate cu exceptia acelora in care eroarea apartine sursei oficiale MO/BO;
- fiecare act legislativ trebuie sa fie identificabil printr-un identificator alfa-numeric, care sa contina in el informatii cu privire la numarul documentului, tipul documentului, data publicarii / data semnarii documentului.

1.1.2.Cerinte nivel aplicatie logica

Accesul la acest nivel se realizeaza in functie de rolurile si privilegiile fiecarui utilizator.

Rolul acestui nivel este de a modela cerintele de aplicatie ale sistemului:

- Sistemul trebuie sa fie extensibil pentru a permite adaugarea de noi functionalitati si schimbari fara a fi necesara reproiectarea completa a acestuia;
- Sa asigure confidentialitatea, securitatea informatiilor si monitorizarea accesului la date printr-un sistem de drepturi si parole de acces la nivel de: utilizator, functie, modul, operatiune;
- Sa fie parametrizabil intr-un grad care sa elimine, pe cat posibil, scrierea de programe si crearea de tabele specifice client;

- Solutia trebuie sa ofere facilitati de introducere a actelor normative;
- Solutia trebuie sa ofere facilitati de modificare a actelor normative introduse deja in sistem;
- Solutia trebuie sa ofere facilitati de retragere sau marcare ca invalide a actelor normative care sunt abrogate;
- Solutia trebuie sa ofere facilitati de marcare a legaturilor dintre actele normative la nivel de document, cat si la nivel de continut de document (articol, alineat, paragraf, etc.);
- Solutia trebuie sa ofere functionalitati avansate de cautare atit pentru cererile trimise din portal cat si pentru cererile primite prin intermediul conectorilor;
- Solutia trebuie sa ofere facilitati de definire si administrare a utilizatorilor de tip administratori de aplicatie si editori;
- Solutia va oferi mecanisme de autentificare si autorizare a utilizatorilor.

1.1.3.Cerinte nivel prezentare

Acest nivel are rolul de a prezenta informatiile din formatul intern al aplicatiei si bazei de date, intr-un format accesibil utilizatorului final si prezinta urmatoarele functionalitati:

- Functionalitati de regasire si prezentare a informatiilor publice in portal
- Functionalitati de furnizare servicii online (servicii web)
- Functionalitati de autentificare a utilizatorilor pe baza mecanismelor aflate la nivel logic

Datorita existentei mai multor tipuri de utilizatori, nivelul de prezentare va oferi facilitati diferite, in functie de tipul utilizatorilor. Pentru utilizatorii umani, interni si externi, va exista un portal de publicare a continutului. Pentru utilizatorii consumatori de servicii electronice, nivelul de prezentare va face publice servicii de interogare si servicii de publicare al continutului informatiilor cu caracter legislativ stocate la nivelul bazelor de date. Toate datele prezentate utilizatorilor vor trebui sa respecte specificațiile „open-data” referitoare la formatul datelor pentru libera re-utilizare.

Atat pentru portal, cat si pentru conectori se va avea in vedere indeplinirea urmatoarelor cerinte functionale:

- Posibilitate de cautare simpla dupa urmatoarele criterii:

- Cuvant/cuvinte din titlul documentului: Rezultatele cautarii vor contine numai acele documente in al caror titlu se regaseste expresia sau cuvantul exact introdus;

- Cuvinte/Grup de cuvinte din textul documentului cu o semnificatie logica: Rezultatele cautarii vor contine numai acele documente in al caror text se regaseste grupul de cuvinte cu semnificatia logica. Grupul de cuvinte poate fi scris exact sau lasate libere formele de exprimare. Grupul de cuvinte sa poata fi introdus in unul sau mai multe campuri. Aplicatia va permite operatori de tipul “si” / ”sau” pentru a parametriza cautarea pentru cuvintele introduse;

- Tipul documentului: Rezultatele cautarii vor contine numai acele documente care fac parte dintr-o anumita categorie de documente selectate;

- Numarul documentului: Rezultatele cautarii vor contine numai acele documente referite prin an si numarul documentului (ex. 2009-11, returneaza toate documentele aparute in anul 2009 si au numarul 11, indiferent de tipul documentului lege, ordonanta, hotarire, etc.);

- Data publicarii documentului legislativ;

- Data emiterii documentului legislativ;

- Publicat in (sursa publicarii) se va mentiona sursa (curent va fi MO), dar prin completarea bazei pot aparea si alte surse (BO din perioada 1947-1989 sau alte publicatii);

- Acte in vigoare la o anumita data.

Criteriile de cautare trebuie sa produca rezultate relevante pentru utilizatori, sa ofere liste de rezultate acceptabile si posibil de verificat (cat mai scurte). Pentru cresterea acuratetei rezultatelor este necesar ca textele sa contina diacritice.

Listele de acte trebuie sa prezinte direct minim urmatoarele categorii de informatii:

- **de identificare** - titlul, numarul, data emiterii / publicarii, emitentul;
- **de evaluare -** numarul de acte din lista, starea fiecarui act, data intrarii lor in vigoare.

La pozitionarea pe un act din baza, aplicatia va afisa si urmatoarele informatii:

- actul in ultima sa forma (cu toate modificarile la zi), daca nu s-a cerut la o alta data, cu posibilitatea de a avea la dispozitie trecerea la forma de la o alta data;

- cuprinsul actului;
- formatul in timp al unui articol care a suferit modificari, cu indicarea actului modificator;
- corelatia cu alte acte;
- legaturi cu actele comunitare (inclusiv cele de armonizare);
- toate formele consolidate corespunzatoare actelor modificatoare si data lor de intrare in vigoare.

La nivel de prezentare, se va urmari existenta unei interfete de cautare a actelor normative care sa urmeze standardul oferit de interfata N-LEX, ca in figura urmatoare:

La nivelul portalului intern vor fi publicate anumite functionalitati de la nivelul aplicatie logica, in ceea ce priveste managementul bazei de date legislative:

- Introducerea actelor legislative
- Modificarea actelor legislative
- Retragerea sau invalidarea actelor legislative
- Marcarea legaturilor dintre actele normative la nivel de document, cat si la nivel de continut de document (articol, alineat, paragraf, etc.)

Pentru consumatorii de servicii electronice, nivelul de prezentare va oferi functionalitati de interconectare sub forma unui conector disponibil in format XML/SOAP.

Urmatoarele functionalitati vor fi disponibile:

- Interogarea bazei de documente legislative dupa urmatoarele criterii, luate individual sau combinate:
    - cautare de cuvinte/grupuri de cuvinte, cu semnificatie logica in:

      a) Continutul din titlulul documentului legislativ

      b) Continut din corpul documentului legislativ
    - Tipul documentului legislativ
    - Numarul documentului Legislativ
    - Data publicarii documentului legislativ
    - Data emiterii documentului legislativ
    - Starea documentului (activ sau inactiv la o data)
    - emitent
- Obtinerea listei de documente legislative in urma unei cautari
- Obtinerea unui document in urma unei interogari punctuale
- Descrierea serviciilor web ce trebuie implementate se regasesc in „N-Lex – Ghidul dezvoltatorului ver. 1.2” ce va fi pus la dispozitie in cadrul fazei de analiza

Pentru optimizarea transferului de informatii, nivelul prezentare va oferi suport pentru compresia datelor.

1.1.4.Cerinte zona virtualizare

Virtualizarea a cunoscut in ultima vreme o crestere spectaculoasa datorita capacitatii sale de a reduce costurile de achizitie si mentenanta a infrastructurii tehnice. Zona de virtualizare va realiza separarea logica a masinilor fizice in masini virtuale, care vor fi dedicate diferitelor nivele functionale.

Zona de virtualizare va asigura optimizarea utilizarii capacitatii de calcul a serverelor si va oferi instrumente de administrare a infrastructurii virtuale implementate in cadrul proiectului.

1.1.5.Cerinte zona de salvare si recuperare

Datele/informatiile sunt in prezent un element comun pentru orice companie. Informatiile in format electronic se aduna in interiorul companiilor in cantitati din ce in ce mai mari in fiecare an. Acest lucru a condus intr-un mod evident la presiuni din ce in ce mai mai mari asupra departamentelor IT, crescand responsabilitatile cu privire la stocarea si siguranta acestora. Astfel, principalele actiuni asupra informatiilor, in afara de utilizarea cat mai eficienta a acestora, sunt backup-ul si arhivarea datelor.

Zona de salvare si recuperare va oferi mecanisme de salvare si recuperare a componentelor de baza din cadrul arhitecturii logice si functionale. Datorita cerintelor standardizate pentru salvarea datelor si a aplicatiilor, aceasta zona va fi acoperita de un produs dedicat, pe care ofertantul il va include in oferta tehnica. Functionalitatile acestei zone sunt acoperite in capitolul corespunzator din arhitectura tehnica.

1.1.6.Cerinte zona de monitorizare, audit si conformitate

Zona de monitorizare si audit va oferi informatii cu privire la :

- Utilizarea aplicatiei de catre utilizatorii publici prin intermediul portalului
- Auditul si conformitea actiunilor realizate de utilizatorii administratori cu pivire la a configuratiile sistemelor din solutie

Este imperativ ca toata activitatea de monitorizare si management sa se faca dintr-un singur punct de control. Numai in acest mod se vor putea anticipa probleme de performanta, sau discontinuitate a serviciului. Se va oferi un canal rapid de comunicatie intre zona de business si echipele de infrastructura, aplicatii si baze de date. Un astfel de sistem ne va permite sa identificam exact zona din care provine o problema si sa reducem considerabil timpii de diagnostic si rezolvare a problemelor.

O astfel de solutie trebuie sa ofere o vedere de ansamblu a tuturor componentelor de la end-user la baza de date, de la service-level la infrastructura pentru a identifica si rezolva orice incident ce poate afecta activitatea.

Solutia trebuie sa ne sprijine sa intelegem performanta experientei reale a utilizatorului final in utilizarea aplicatiilor web-based, astfel incat sa putem optimiza performanta, imbunatati capacitatea si diagnostica rapid problemele. Dorim sa depasim limitarile solutiilor de monitorizare care urmaresc doar scenarii predefinite sau ale aplicatiilor desktop-based care urmaresc numai un anumit subset de utilizatori, si sa ne concentram pe urmarirea activitatii tuturor utilizatorilor, in timp real, permanent.

Din punct de vedere functional, se considera urmatoarele cerinte minime si obligatorii pentru atingerea scopului mentionat:

Implementare rapida – se doreste evitarea interferentei pe care un analizor de trafic ar aduce-o in fluxurile de date ale aplicatiilor; de aceea, solutia trebuie sa permita instalarea analizorului pe un port de monitorizare pasiva, in fata serverelor web sau de aplicatii, insa in spatele firewall-ului pentru a putea fi protejat corespunzator. Din aceasta perspectiva, sistemul ar putea sa “vada” fiecare pachet inainte de a ajunge la server si imediat dupa ce a iesit, fara a interfera cu traficul normal.

Performanta ridicata si impact redus – solutia nu trebuie sa produca nici un fel de impact asupra infrastructurii de retea sau a aplicatiilor. Se doreste evitarea instalarii de agenti software sau programe, marcarea continutului web sau generarea de trafic de retea aditional. Sistemul trebuie sa poata incepe monitorizarea, inregistrarea si analiza traficului utilizator imediat dupa instalare si configurare, fara a necesita arhitecturi suplimentare

Vizualizarea completa a infrastructurii web – sistemul trebuie sa fie capabil sa examineze lantul livrarii de servicii din perspective variate, inclusiv utilizator final, server web, locatia utilizatorului, situl web, pagina web, o succesiune de mai mult pagini, sau nivele ale aplicatiei

Rapoarte si grafice personalizabile – sistemul trebuie sa dispuna de o interfata grafica usor de personalizat, destinata sa evidentieze cauza-radacina a problemei de performanta pe care o experimenteaza un utilizator. De asemenea, trebuie sa fie capabil sa asigure accesul facil la un set cuprinzator de metrici de performanta pentru fiecare componenta a lantului de service delivery. Definirea de rapoarte personalizate, suplimentare care sa asigure corelarea si analiza masuratorilor pentru resurse specifice ale infrastructurii web, ori maparea lor pe functionalitati specifice de business, reprezinta o capacitate functionala de mare importanta.

Alerte in timp real – sistemul trebuie sa dispuna de functionalitati de alertare care sa permita administratorilor si detinatorilor de aplicatii sa impuna SLA-uri. Alertele trebuie sa poata fi definite pentru servere, pagini, situri specifice, ori alte resurse monitorizate, inclusiv tranzactii utilizator si erori de continut.

Vizualizarea sitului web prin ochii utilizatorului final – dorim ca solutia agreata sa fie capabila sa reproduca sesiunea de lucru a utilizatorului final, exact asa cum este afisata in browser-ul acestuia. Justificam aceasta cerinta prin prisma faptului ca data fiind multitudinea de browsere, configuratii ale terminalelor utilizator si elemente afisabile in paginile web, exista foarte multe situatii in care operatorii help desk raporteaza o problema de navigare, problema care nu este detectata de administratorii de aplicatii si a carei sursa nu poate fi identificata. Este esential sa putem reproduce sesiunea exacta a utilizatorului final, astfel incat sa putem identifica exact configuratia utilizata si momentul in care s-a produs eroarea.

Oferirea unei vizibilitati reale echipei de administrare – Erorile de aplicatie intr-un site web de productie sunt dificil de urmarit, atat din perspectiva timpului cat si si din cea a alocarii de resurse. Avem nevoie sa putem avea vizibilitate asupra disponibilitatii reale a siturilor web, sa putem vedea ce s-a intamplat cu adevarat si sa putem determina exact unde cade responsibilitatea si sa diagnosticam sursa problemei.

Oferirea unei vizibilitati totale asupra siturilor web – a monitoriza o singura dimensiune a disponibilitatii aplicatiilor web si a neglija layer-ul de interactiune zilnica intre utilizatorii finali si aplicatii reprezinta o problema critica. Este necesara furnizarea de capacitati de “instant replay” care sa permita vizualizarea comportamentului utilizatorilor finali, precum si raspunsul exact al aplicatiilor

La nivel de audit si conformitate a sistemului informatic pentru a securiza solutia legislativa impotriva incercarilor de a o utiliza altfel decat a fost stabilit prin acest proiect, este nevoie de implementarea unei solutii de securitate prin care se va realiza automatizarea colectarii logurilor din organizatie, cu un sistem de alertare si monitorizare, precum si obtinerea unei platforme de investigatie pentru cresterea nivelului de securitate si evitarea expunerii datelor sensibile la riscuri. Solutia trebuie sa ne ajute la conformitatea cu regulile de securitate prin colectarea si stocarea securizata a logurilor, raportarea si alertarea evenimentelor provenite din sisteme eterogene.

Solutia de audit si conformitate va trebui sa sprjine autoritatea contractanta in atingerea conformitatii regulamentare astfel:

1. Sa existe o evaluare permanenta a securitatii si conformitatii produselor la nivel de furnizor, prin raportarea la categoriile de securitate specificate in US NIST 800-53:
    a. Evaluarea completa de securitate
    b. Dezvoltarea de cod si modele arhitecturale care sa acopere operatiunile de securitate comune
    c. Pregatirea si supervizarea dezvoltatorilor pentru constientizarea permanenta a problemelor de securitate a codului
    d. Evaluarea permanenta a vulnerabilitatilor in componentele terte utilizate de solutia agreata; aceasta procedura presupune ca eventualele corectii de securitate sa fie aplicate in timp util
    e. Semnarea software-ului in cod digital pentru a preveni intruziunea
    f. Evaluarea metodelor de criptare a datelor in fluxurile operationale
    g. Indeplinirea de catre furnizor a standardelor de securitate si conformitate prevazute ca obligatorii prin lege
2. Furnizorul solutiei sa aiba implementate acele controale de securitate si conformitate care sa asigure indeplinirea cerintelor ISO 27001
3. Sa fie asigurate functionalitatile necesare pentru:
    a. Implementarea sabloanelor de software si hardware autorizate a rula in mediul informatic
    b. Mentenanta, monitorizarea si analiza de loguri de audit in integralitatea lor
    c. Controlul utilizarii privilegiilor administrative
    d. Monitorizarea si controlul conturilor inactive
    e. Protejarea importiva furtului de date
    f. Reactia la incidentele de securitate

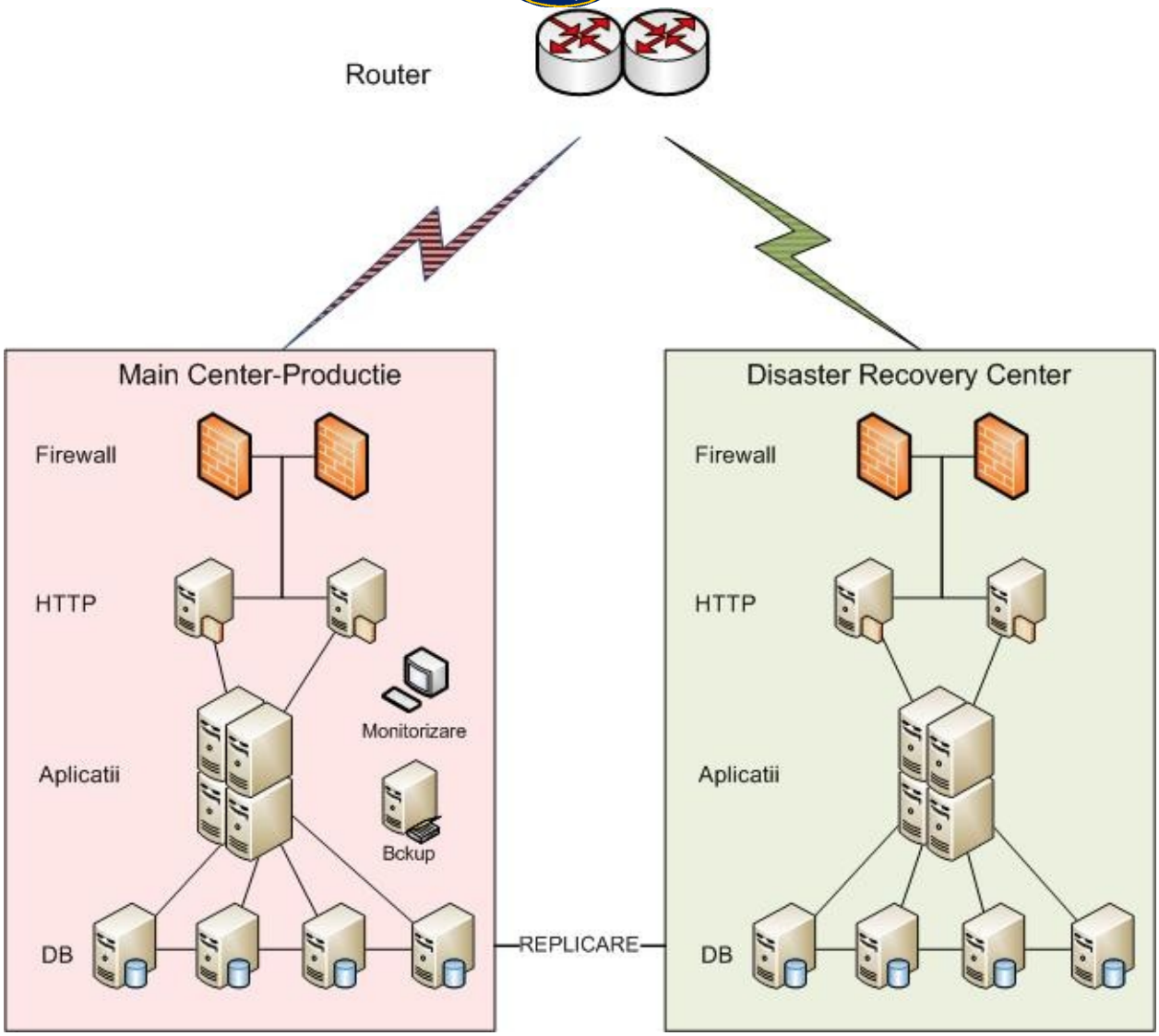
2.6. Arhitectura tehnica

Pentru asigurarea cerintelor functionale si prezentate anterior, sistemul va trebui sa includa cel putin componentele:

- Sistem de comunicatii cu urmatoarele echipamente
    - Echipamente de retea tip firewall
    - Echipamente de retea tip switch
    - Echipamente de retea tip router

- Sistem de stocare de tip Storage Area Network (SAN)
    - Echipamente de comunicatii tip SAN switch
    - Echipamente de stocare date SAN
- Echipamente de calcul fizice capabile sa sustina urmatoarele servere virtualizate:
    - Serevere virtuale sistem de gestiune a bazelor de date
    - Servere virtuale pentru portal
    - Servere virtuale pentru publicarea de conectori pentru sisteme externe (N-LEX)
    - Servere virtuale web – de tip reverse proxy cu posibilitate de balansare
    - Server virtual pentru salvare si restaurare
    - Server virtual pentru monitorizare
- Biblioteca de benzi pentru salvarea datelor
- Sursa neintreruptibila de curent
- Cabinet si accesorii pentru echipamente

Infrastructura hardware trebuie sa fie instalata intr-o locatie principala (Main Center) care va gazdui toate componentele hardware necesare pentru rularea in bune conditii a aplicatiilor descrise mai sus. Pentru a asigura un grad mare de disponibilitate al sistemului, anumite componente vor fi instalate in arhitectura redundanta activ-activ la nivel de conexiuni, servere de aplicatii si servere de baza de date.
Pentru a asigura serviciul in caz de evenimente neprevazute (caderi de curent, calamitati naturale,etc.), infrastructura hardware din Main Center va fi duplicata si instalata intr-o locatie secundara (Disaster Recovery Center), unde va fi configurata pentru a putea fi utilizata in cazul in care activitatea in locatia principala este afectata.



In continuare se va descrie arhitetura tehnica a locatiei principale (Main Center).

Datorita numarului mare de utilizatori ce se estimeaza ca vor accesa sistemul si a diversitatii utilizatorilor (interni, externi, conectori), se va avea in vedere separarea accesului utilizatorilor interni, fata de cei externi si de conectori.

Utilizatorii interni si externi vor fi redirectionati in functie de categorie interni/externi catre instante separate.

Pentru a avea acces zona de administrare a bazei de date legislative, utilizatorii interni se vor autentifica in aplicatie.

Se va utiliza virtualizarea sistemelor fizice si se vor asigura cel putin urmatoarele resurse de procesare active si complet licentiate din punct de vedere software (suplimentarul poate fi considerat rezerva hardware pentru scalare verticala):

- 4 x Serevere virtuale sistem de gestiune a bazelor de date
  - Min. 4 core
  - Min. 32 GB RAM

- 2 x Servere virtuale pentru portal
  - Min. 4 core
  - Min. 16 GB RAM
- 2 x Servere virtuale pentru publicarea de conectori pentru sisteme externe (N-LEX)
  - Min. 2 core
  - Min. 32 GB RAM
- 2 x Servere virtuale – de tip web reverse proxy
  - Min. 2 core
  - Min. 16 GB RAM
- 1 x Server virtual – monitorizare solutie
  - Min. 2 core
  - Min. 8 GB RAM
- 1 x Server virtual – solutie backup &recovery
  - Min. 2 core
  - Min. 8 GB RAM

Locatia secundara (Disaster Recovery Center) va replica functionalitatile de baza ale sistemului fara componenta de monitorizare si cea de backup si recovery. Se va utiliza virtualizarea sistemelor fizice si se vor asigura cel putin urmatoarele resurse de procesare active si complet licentiate din punct de vedere software (suplimentarul poate fi considerat rezerva hardware pentru scalare verticala):

- 4 x Serevere virtuale sistem de gestiune a bazelor de date
  - Min. 4 core
  - Min. 32 GB RAM
- 2 x Servere virtuale pentru portal
  - Min. 4 core
  - Min. 16 GB RAM
- 2 x Servere virtuale pentru publicarea de conectori pentru sisteme externe (N-LEX)
  - Min. 2 core
  - Min. 32 GB RAM
- 2 x Servere virtuale – de tip web reverse proxy
  - Min. 2 core
  - Min. 16 GB RAM

1.1.7. Infrastructura Software necesara

1.1.7.1. Cerinte tehnice pentru virtualizare

Pentru folosirea optima a serverelor dedicate aplicatiilor se solicita o solutie de virtualizare ce trebuie sa indeplineasca urmatoarele cerinte:

- posibilitatea de a migra masinile virtuale pornite pe alte servere in cazul intreruperilor planificate, fara intreruperi;
- pornirea automata a unei masini virtuale pe un alt server in cazul aparitiei de intreruperi neplanificate ale serverului sau masinii virtuale;
- posibilitatea de conversie a sistemelor de operare Linux, Windows care ruleaza pe servere fizice in masini virtuale;
- posibilitatea de a folosi ca sisteme virtuale Linux, Windows;
- posibilitatea de clonare, suspendare temporara a activitatii si mutarea masinilor virtuale pe alte servere.

Sistemul trebuie sa asigure managementul centralizat al serverelor dedicate hostingului de masini virtuale. Prin aceasta solutie se doreste atat managementul integrat al sistemului de operare al serverelor gazda, cat si integrarea cu sistemul de monitorizare al masinilor virtuale.

Cerinte generale privind Solutia pentru managementul serverelor de masini virtuale

- Optimizarea administrarii si a timpului de raspuns pentru incidente;
- Automatizarea activitatilor IT si eliminarea sarcinilor repetitive, mari consumatoare de timp;
- Posibilitatea delegarii drepturilor administrative si de provizionare, simplificand actiunile echipei IT;
- Evidenta stricta a masinilor virtuale folosite in intreaga infrastructura;
- Plasarea inteligenta a masinilor virtuale, folosindu-se astfel resursele hardware la maxim, micsorand consumul de energie electrica.

Cerinte Minime Obligatorii:

- Managementul centralizat al tuturor masinilor virtuale si gazdelor fizice din cadrul solutiei;
- Monitorizarea starii de sanatate si utilizare la nivel de gazde fizice si masini virtuale;
- Conversia serverelor fizice in servere virtuale;
- Instalarea update-urilor automat pentru gazdele de masini virtuale;

- Plasarea inteligenta a masinilor virtuale pe gazdele fizice in functie de necesarul resurselor hardware;
- In cazul adaugarii de hardware nou, sistemul va oferi instalarea automata a sistemului de operare al gazdei fizice, instalarea rolurilor si dependintelor necesare si adaugarea acestuia in clusterul de masini virtuale corespunzator;
- Portal cu sabloane de masini virtuale pentru mediile de test;
- Posibilitatea crearii de masini virtuale avand roluri deja instalate si configurate in functie de sablonul corespunzator;
- Posibilitatea de a crea sabloane de inlantuiri de masini virtuale. Astfel se pot crea in mod automat servicii cu anumite dependinte: de exemplu se poate crea o masina virtuala care are instalat deja software-ul necesar pentru a oferi servicii de baze de date si o alta masina care ofera servicii de tip front-end;
- Posibilitatea delegarii drepturilor de administrare si provizionare a masinilor virtuale;
- Solutia trebuie sa permita instalarea unei console de management separat de serverul de administrare;
- Integrarea facila cu infrastuctura existenta de autentificare, sistemele de management si monitorizare;
- Monitorizare proactiva a masinilor virtuale, gazdelor fizice precum si a aplicatiilor ce ruleaza in masinile virtuale prin integrarea cu sistemul de monitorizare al serverelor;
- Consolidare a serverelor si conversia serverelor fizice in servere virtuale fara intreruperea accesului utilizatorilor la acestea si fara costuri aditionale;
- Simplificarea managementului serverelor, a back-up-ului si restaurarii in caz de dezastru;
- Suport pentru definirea de servicii cu aplicatii multi-tier de tip „one tier”, „two-tier” etc.;
- Suport pentru deploymentul de aplicatii virtuale pe servere;
- Suport pentru instalarea consolei in arhitectura clusterizabila pentru asigurarea redundantei.

Sistemul va oferi management pentru intreaga gama de clustere de gazde de masini virtuale. Software-ul trebuie sa fie de tip Enterprise si sa asigure accesul la versiuni noi de produs pentru o perioada de minim 3 ani.

1.1.7.2.Cerinte tehnice sistem de operare

Cerinte generale:

- Solutia trebuie sa fie de tip Enterprise si sa asigure urmatoarele caracteristici tehnice. Solutia trebuie sa se integreze cu infrastructura IT a Ministerului Justitiei.
- Solutia trebuie sa ofere suport pentru 4 TB RAM pentru sisteme 64-bit Suport pentru procesoare multi-core (minim 64 de procesoare)
- Solutia trebuie sa ofere suport pentru adaugare sau inlocuire de memorie fizica sau procesoare in regim online
- Solutia trebuie sa ofere suport pentru clustering cu minim 16 noduri
- Suport pentru virtualizare cu posibilitatea de alocare a minim 64 de procesoare virtuale per masina virtuala si 2048 de procesoare virtuale

Cerinte functionale:

- Sa permita mutarea elementelor interactive din faza configurarii in faza ulterioara instalarii, eliminand interactiunea administratorului la instalarea sistemului de operare;
- sa ofere o interfata unica pentru configurarea si monitorizarea serverului, cu programe de tip expert pentru optimizarea sarcinilor comune de administrare a serverului.
- sa ofere un shell, optional cu linie de comanda si limbaj de script, ce ajuta administratorii sa automatizeze sarcinile de rutina de administrare a sistemului pe mai multe servere.
- sa ofere instrumente de diagnosticare puternice, care ofera vizibilitate permanenta asupra mediului serverului, fizic si virtual, pentru a identifica si rezolva rapid problemele care apar.
- sa permita administrarea serverului si replicare a datelor optimizate pentru control imbunatatit al serverelor din locatii de la distanta
- sa permita instalari minimale, in care sunt instalate numai rolurile si caracteristicile necesare, minimizand nevoile de intretinere si reducand zonele de atac de pe server.
- Sa contina Internet Protocol versiunea 6 (IPv6), iar nodurile de clustere de la locatii dispersate geografic sa nu mai fie necesar sa se gaseasca intr-o subretea cu acelasi IP sau sa fie configurate cu retele locale virtuale (VLAN) complicate.

- sa ofere mecanisme de balansare si sa includa suport pentru mai multe adrese IP dedicate, care permit gazduirea mai multor aplicatii in acelasi cluster.
- Sa ofere un mecanism ce asigura ca reteaua si sistemele nu sunt compromise de calculatoare virusate, izoland si/sau depanand calculatoarele care nu se conformeaza politicilor de securitate care au fost stabilite.
- sa ofere un mecanism de protectie impotriva aplicatiilor periculoase;
- sa ofere flexibilitate criptografica crescuta, suportand algoritmi de criptare standard si definiti de utilizator, permitand crearea, stocarea si preluarea mai facila a cheilor criptografice.

Cerinte de virtualizare:

- sa permita virtualizarea rolurilor de server sub forma de masini virtuale (VM) separate care ruleaza pe aceeasi masina fizica, fara a fi necesara achizitia de software de la terti.
- sa se poata implementa mai multe sisteme de operare – Windows, Linux si altele – in paralel pe un singur server
- Sa ofere clustering-ul gazdelor sau al masinilor virtuale care ruleaza pe gazde si backup-ul masinilor virtuale in timp ce acestea ruleaza
- Sa permita programelor accesate de la distanta sa fie deschise cu un singur clic si sa fie utilizate ca si cum ar rula pe calculatorul utilizatorului final.

Solutia sistem de operare trebuie sa beneficieze de update-uri de securitate, patchuri pentru o perioada de minim 3 ani. Solutia ofertata trebuie sa fie COTS, de ultima generatie si sa beneficieze de suport direct de la producator pentru un interval de minim 1 an

1.1.7.3.Cerinte tehnice baze de date

Componenta de Baze de Date va indeplini (minim) urmatoarele cerinte tehnice:

- Sa fie un sistem de gestiune a bazelor de date de tip relational;
- Sa permita folosirea a peste 64Gb memorie.
- Serverul sa permita folosirea a minim 16 core-uri
- Solutia trebuie sa ofere posibilitatea efectuarii backup-ului in multiple fisiere simultan pentru a putea efectua operatia pe discuri diferite in paralel.
- Solutia trebuie sa ofere posibilitatea de a crea, modifica, sterge index-ul concurent cu activitatile utilizatorilor
- Solutia trebuie sa ofere posibilitatea de a crea un snapshot al bazei de date

- Solutia trebuie sa ofere posibilitatea de a crea index secundar la nivel de coloane care sa comprime si sa stocheze datele in memorie pentru access rapid la datele din Data Warehouse
- Solutia trebuie sa ofere posibilitatea de a procesa sute de milioane de linii in mai putin de o secunda pentru access rapid la rapoarte
- Solutia trebuie sa ofere posibilitatea de afisare a rapoartelor intr-un mod interactiv, astfel incat utilizatorii sa poata urmari evolutia in timp a anumitor evenimente, sa poata efectua filtrari asupra datelor prezentate
- Solutia trebuie sa ofere unelte pentru gestionare facila a obiectelor bazelor de date:
    - Unelte pentru administrarea bazelor de date si a proceselor uzuale care se executa asupra bazelor de date precum si al rapoartelor
    - Posibilitatea de definire si gestionare a obiectelor bazei de date (tabele, indecsi, proceduri stocate, triggere) direct din instrumentele folosite de dezvoltatori pentru scrierea aplicatiilor
    - Posibilitatea de a oferi compresia datelor folosind suport UCS-2 Unicode
    - Loc central care ofera posibilitatea administrarii entitatilor de date si ierarhiilor din multiple baze de date cu posibilitatea versionarii
    - Interogare si analiza ad-hoc si self-service a datelor: facilitati de interogare a datelor disparate in momentul solicitarii rapoartelor.

- Sa aiba suport Unicode UTF-8 sau echivalent;
- Sa permita minimizarea conflictelor de acces la date si garantarea simultaneitatii accesului la date;
- Sa ofere suport pentru diverse tipuri de date, cum ar fi date multimedia sau structuri de date de tip XML;
- Sa ofere suport pentru modelare a structurilor de date de tip arbore: metode incorporate pentru crearea si operarea pe noduri ierarhice;
- Sa ofere suport pentru stocarea datelor binare mari, precum documente si imagini, ca parte integranta a bazei de date, pastrand in acelasi timp consecventa tranzactionala;

- Sa ofere suport pentru cautare complexa la nivel de text, folosind indecsi specializati; efectuarea rapida a cautarilor in acest tip de date
- Sa ofere suport pentru crearea de tabele cu mai mult de 900 de coloane.
- Sa ofere 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).
- Sa ofere suport pentru proceduri stocate si trigger-i;
- Sa permita restrictionarea accesului la nivelul obiectelor bazei de date;
- Sa permita importul si exportul de date in formate acceptate de alte sisteme de gestiune a bazelor de date (cel putin Oracle, SQLServer, DB2, MySQL);
- Sa permita conectarea cu alte sisteme de gestiune a bazelor de date pentru schimb de date bidirectional;
- Sa suporte diverse tipuri de indexare.
- Solutia trebuie sa ofere suport scalabil si sigur pentru baze de date, incluzand instrumente integrate de raportare si analiza.
- Solutia trebuie sa ofere raportare consolidata si managementul depozitelor de date;
- Solutia trebuie sa ofere unelte pentru administrarea bazelor de date si a proceselor uzuale care se executa asupra bazelor de date precum si al rapoartelor;
- Solutia trebuie sa ofere facilitati pentru monitorizarea tranzactiilor;
- Sa ofere suport pentru criptarea transparenta a datelor, a fisierelor de date si a fisierelor jurnal fara sa fie necesara modificarea aplicatiei. 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.
- Sa ofere suport pentru 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.

- Sa ofere posibilitate de a filtra evenimentele auditate; posibilitatea de a customiza operatia de audit in functie de evenimentele din baza de date
- Sa ofere posibilitate de adaugare online a resurselor de memorie la masinile fizice care gazduiesc bazele de date, pentru scalarea la cerere a acestora.
- Sa ofere posibilitatea de colectare a 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
- Sa ofere 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
- Sa ofere suport pentru tehnologii de tip data mirorring
- Solutia trebuie sa ofere posibilitatea de a rula in configuratii de disponibilitate ridicata activ-activ/activ-pasiv
- Solutia trebuie sa benefieze de update-uri de securitate, patchuri pentru o perioada de minim 3 ani. Solutia ofertata trebuie sa fie COTS, de ultima generatie si sa beneficieze de suport direct de la producator pentru un interval de minim 1 an.

1.1.7.4.Cerinte tehnice portal si server de aplicatii

Componenta de Portal si Server de Aplicatii va indeplini (minim) urmatoarele cerinte tehnice:

- Sa ofere suport pentru tehnologii si standarde deschise;
- Sa includa o interfata web standardizata, simpla si intuitiva;
- Sa utilizeze tehnologii bazate pe Web 2.0 si AJAX pentru cresterea uzabilitatii - imbunatatirea experientei utilizatorilor;
- Sa ofere acces catre toate resursele prezente in cadrul portalului printr-o singura autentificare, la deschiderea sesiunii;
- Sa ofere un grad ridicat de securitate a sistemului, care sa garanteze confidentialitatea si securitatea datelor utilizatorilor pentru accesul neautorizat atat dinafara cat si din interiorul sistemului;

- Sa includa mecanisme de grupare a serverelor in clustere atat in topologii de tip activ-activ cat si activ-pasiv;
- Sa includa mecanisme de scalare a sistemului pe orizontala (Scale Out) si verticala (Scale Up);
- Sa ofere suport pentru servicii web;
- Sa asigure disponibilitate permanenta 24x7 a serviciilor on-line oferite prin intermediul portalului;
- Sa ofere suport pentru conectarea la multiple sisteme de gestiune a bazelor de date relationale (SGBDR);
- Partajarea conexiunilor de date (Connection Pooling) sa fie integrata cu mecanismele de clustering si detectare a defectelor, implementate la nivelul bazelor de date;
- Sa permita stoparea temporara a unui nod din cluster pentru mentenanta si suport, sistemul in acest timp fiind disponibil pentru activitati normale;
- Sa ofere suport pentru protectie impotriva supraincarcarii serverului de aplicatii utilizand optiuni de configurare a resurselor software pentru cazurile in care serverul nu mai poate accepta noi cereri de procesare, capacitatea maxima a sistemului fiind atinsa;
- Sa contina un design modular si optiuni de instalare ce permit numai instalarea caracteristicilor strict necesare, reducand zonele de atac si simplificand administrarea actualizarilor.
- Sa permita copierea setarilor site-urilor Web pe mai multe servere Web, fara a fi necesara configurare suplimentara.
- Sa contina administrarea integritatii serverului Web, alaturi de instrumentele complexe de diagnosticare si depanare ce permit vizibilitatea si urmarirea cererilor care ruleaza pe serverul Web.
- Sa permita izolarea pachetelor de aplicatii, sa mentina site-urile si aplicatiile izolate, crescand securitatea si stabilitatea.
- Sa ofere un model de extensibilitate flexibil ce permite personalizarea, cum ar fi adaugarea de module noi utilizand cod nativ sau administrat.

1.1.7.5.Cerinte tehnice server web

Serverul web va reprezenta punctul unic de acces pentru utilizatorii umani interni si externi ai sistemului. In functie de tipul utilizatorului si domeniul din care provine, acesta va fi redirectionat catre portalul intern sau cel extern al aplicatiei.

Pachetul software trebuie sa ofere urmatoarele capabilitati:

- Rescrierea adreselor URL si capabilitati de tip server proxy si reverse proxy
- Rularea paginilor dinamice
- Balansare a incarcarii
- Suport pentru protocolul HTTP 1.1 (RFC 2616, 0)
- Suport pentru protocolul HTTPS (RFC 2818)
- Suport pentru compresia continutului static si dinamic
- Suport pentru realizarea de cache la acest nivel

1.1.7.6.Cerinte tehnice pentru monitorizare, audit si conformitate

Solutia trebuie sa ofere o imagine globala a intregului sistem informatic pentru a detecta proactiv, diagnostica si rezolva orice problema de performanta si disponibilitate in ordinea prioritatii dictate de business.

Din punct de vedere al monitorizarii serviciilor web solutia trebuie sa fie capabila sa adune intr-o singura consola masuratori care sa permita:

- Din perspectiva serviciului oferit sa se vada modul in care performanta si disponibilitatea modulelor componente afecteaza businessul prin urmarirea timpilor de raspuns la nivel de serviciu
- Din perspectiva utilizatorului final sa se vada cum acesta interactioneaza cu aplicatiile si cum acestea raspund nevoilor sale prin masurarea timpilor de raspuns de tip “end-to-end”, adica exact la nivelul utilizatorului final
- Din perspectiva tehnica sa se vada modul in care fiecare componenta contribuie la performanta sistemelor, incluzand baze de date si infrastructura fizica si virtuala din background. Acest lucru trebuie realizat prin masurarea parametrilor de stare ai sistemelor (servere de prezentare, servere de aplicatii, servere de baze de date, sisteme de operare, storage, retea si infrastructura fizica, sau virtuala). Aceste masuratori trebuie facute prin agenti specializati.
- Sa permita vizualizarea dependintelor intre servicii si legaturile intre servicii si componentele sistemelor. Aceste dependinte trebuie sa poata fi customizate in interfata de configurare a sistemului
- Sa aiba o singura consola pentru a vizualiza intregul sistem (aplicatii, baze de date, infrastructura)
- Consola trebuie sa fie web, fara instalare de plugin-uri si sa fie suportata minim de Internet Explorer, Mozila, Google Chrome, Opera si Safari
- Sa permita crearea de panouri custom cu acces bazat pe roluri

- Sa permita autentificarea integrata cu sisteme LDAP versiunea 3, dar cel putin cu urmatoarele: Active Directory, Sun Java Systems Directory Server, OpenLDAP, Novell eDirectory, cu posibilitatea maparii utilizatorilor si a grupurilor din LDAP pe utilizatori si roluri din sistemul de monitorizare
- Sa dispuna de un mecanism de alertare bazat pe reguli.
- Sa dispuna pentru fiecare tehnologie monitorizata de un set de reguli standard care sa poata fi customizate. De asemenea sa permita crearea de reguli noi
- Sa dispuna de un mecanism avansat de notificare si de actiuni la aparitia unei alerte. Sa poata face alertare pe mail catre recipienti alesi in mod dinamic in functie de sistemele afectate, de serviciile de business din care fac parte respectivele sisteme, de perioada din zi (de exemplu alarmele care vin noapte sa fie trimise catre persoana care este de serviciu)
- Sa permita executarea de scripturi automate la aparitia alarmelor (de exemplu sa poata elimina automat un proces care consuma 99% CPU si nu nu face parte din procesele aplicatiei)
- Sa permita trimiterea unui trap SNMP la aparitia alarmelor

La nivelul monitorizarii utilizarii aplicatiei web solutia trebuie sa permita:

- Inregistrarea cererilor end-to-end si a timpilor de retea — Inregistrarea tuturor cererilor si raspunsurilor in aplicatiile Web. Informatia trebuie culeasa inaintea serverelor Web prin mecanisme de captura de trafic fara instalarea de pachete in serverele Web.
- Sa poata captura tranzactii reale, sau sa reproduca tranzactii simulate — Sa poata genera tranzactii simulate pentru testarea perfomantei si disponibilitatii aplicatiilor
- Sa poata analiza sesiuni individuale de activitate ale utilizatorilor pentru masurarea performantei aplicatiilor web. Sa captureze si sa stocheze sesiuni de lucru utilizator reali, sa reproduca sesiunea capturata din perspectiva utilizatorului final
- Sa poata monitoriza si alerta cand anumite pagini sunt apelate si sa poata reproduce sesiunile derulate pe paginile monitorizate
- Sa dispuna de capacitatea de a cauta sesiuni efectuate dupa cuvinte cheie din acestea
- Calcularea de SLA-uri pe baza performantei — Formarea unor referinte cu privire la timpii de acces si alertarea utilizatorilor cand aceste valori sunt depasite.

- Masuratori detaliate geografic — Monitorizarea timpilor de raspuns defalcat pe locatii geografice, sau alte grupari logice.

- Performanta servererlor Web si de aplicatie — Monitorizarea serverelor Web si de aplicatie pentru metrici referitoare la configuratia acestora: CPU, numar de servicii, numar de accese.

- Inspectare si analiza de continut — Vizualizarea informatiei exacte afisate in browser-ul utilizatorului final.

- Posibilitatea de a tria tranzactiile — Captura si cautare in datele reale ale utilizatorilor pentru a putea vedea ce anume au facut utilizatorii si ce a raspuns sistemul. Posibilitatea de inspectare detaliata a detaliilor tehnice ale modului de interactiune intre utilizator si aplicatie.

- Replay de sesiune si tranzactie — Posibilitatea de a reproduce exact activitatea unei sesiuni, sau a unei tranzactii individuale. Posibilitatea de a gasi sesiunile si tranzactiile pe baza filtrarii dupa cuvinte cheie. Mecanismul de reply trebuie sa parcuga pas cu pas paginile vizitate de utilizatori. La fiecare pagina trebuie sa se vada modul in care utilizatorul a interactionat: ce campuri a completat, ce optiuni a ales, ce link, sau buton a apasat pentru a merge la pasul urmator

- Reproducerea problemelor pentru Help-Desk — Posibilitatea de a asambla cu un singur click si de a trimite catre help-desk detaliile unei sesiuni care a dat eroare

- Activitatea utilizatorilor trebuie capturata fara impact asupra serverelor – Metoda solicitata de captura a sesiunilor utilizatorilor este network sniffing. Doar in acest mod se poate asigura impact zero asupra serverelor web. Metoda de sniffing trebuie sa suporte minim protocoalele: HTTP/HTTPS, TCP, RDP (TCP), SOAP (HTTP).

Auditul de securitate va asigura automatizarea colectarii log-urilor din entitatile fizice si virtuale, va include un modul de alertare operationala in timp real si va furniza o platforma de investigatii care sa asigure un nivel de securitate optim prin evaluarea proactiva a riscurilor, furnizarea de rapoarte istorice pe orice perioada de timp si mentinerea unui control activ, permanent.

Pentru a rezolva cerintele de conformitate definite in cadrul organizatiei, solutia agreata trebuie sa poata indeplini trei sarcini esentiale:

1. Setarea unui standard de baza al conformitatii si securitatii organizationale:
2. Urmarirea activitatii utilizator
3. Alertarea asupra violarilor de securitate potentiale

Solutia trebuie sa constituie un real suport pentru organizatie in vederea auditului sistemului informatic. Pe baza suportului de produs si a informatiilor furnizate de acesta, responsabilii de securitate vor trebui sa poata:

- Colecta date din mediul auditat si seta un standard de baza
- Efectua modificarile necesare pentru a acoperi minimul de cerinte de securitate, care ar putea include delegare granulara de drepturi si segregare de responsabilitati
- Urmari activitatea zilnica a utilizatorilor
- Asigura stocarea pe termen lung a tuturor datelor colectate
- Pregatirea procedurilor de remediere, in caz de alertare asupra unor posibile devieri de la standard

Solutia trebuie sa dispuna de urmatoarele capacitati:

- Sa furnizeze mecanisme de configurare wizard-based care sa asigure conformitatea cu specificatiile de securitate
- Sa furnizeze management de evenimente mapat pe multiple site-uri si echipamente
- Sa permita colectarea logurilor de retea, de securitate, ale infrastructurii de virtualizare si de performanta a infrastructurii IT&C de pe toate platformele, cu sau fara agenti:
    - UNIX / Linux
    - Windows Server
    - Infrastructuri HyperV si VMWare
    - Echipamente de retea cu capacitati syslog
    - Alte echipamente cu capacitati syslog
    - Baze de date Oracle si MS SQL
    - Aplicatii personalizate
    - Loguri de evenimente diverse in format text
- Sa permita crearea facila de template-uri pentru includerea in procesul de monitorizare si centralizare a log-urilor non-standard
- Sa furnizeze un mecanism de incredere care sa garanteze integritatea si securitatea log-urilor pe parcursul colectarii si transportului
- Sa furnizeze un mecanism de protectie a datelor stocate. Aceste log-uri nu trebuie sa poata fi alterate de nimeni
- Sa asigure normalizarea log-urilor provenite din surse diverse, aducandu-le la un numitor comun fara pierdere de informatii
- Sa furnizeze un mecanism propriu de failover pentru componentele critice

- Sa asigure un impact minim asupra sistemelor monitorizate. Colectarea trebuie sa poata fi efectuata cu sau fara agenti. Alertarea trebuie implementata pentru toate platformele, independent de natura lor. Monitorizarea in timp real si alertarea vor fi de asemenea furnizate pentru sistemele pe care nu se pot instala agenti (servere critice UNIX/Linux, routere, alte echipamente de retea cu capacitati de management)
- Sa dispuna de console de management, MC sau web-based
- Sa se integreze cu Active Directory si sa permita granularizarea de roluri bazat pe Active Directory
- Sa dispuna de un mecanism de raportare istorica, investigationala. Mecanismul trebuie sa asigure o incarcare minima pe serverele de baze de date.
- Sa aiba o arhitectura modulara; sa permita distribuirea modulelor astfel incat sa poata raspunde unor scenarii variate de implementare si sa scaleze unor cerinte variate. De asemenea, scalabilitatea va asigura ca implementarea initiala poate fi extinsa facil, fara reconfigurarea platformei

Solutia agreata va indeplini toate cerintele functionale care sa asigure auditul complet de securitate si conformitate in cadrul organizatiei, indeplinid sarcinile operationale necesare cu un minim de efort din partea personalului dedicat:

- Sa furnizeze colectare securizata a log-urilor de evenimente. Securitatea trebuie aplicata la sursa, la destinatie si la transport.
- Sa pastreze online cat mai multe date posibil; sa asigure stocarea flexibila a pana la 5 ani de evenimente. Log-urile de evenimente vor fi arhivate si comprimate. Mecanismul de compresie cel mai eficient pentru datele online va avea un avantaj major.
- Sa furnizeze o consola de raportare inteligenta. Sa dispuna de un set semnificativ de rapoarte preconfigurate, dar sa permita totodata crearea facila de rapoarte noi. Aceste rapoarte sa poata fi redistribuite si exportate in formatele standard (PDF, XLS, TXT, CSV)
- Sa furnizeze un modul de alertare configurabil. Alertele vor fi predefinite sau definite in cadrul implementarii, si vor trebui sa poata fi mapate pe diverse scenarii; de asemenea, sa poata fi definite alerte pe evenimente corelate
- Sa furnizeze suport pentru conformitate; sa dispuna de mecanisme de raspuns la regulamentele interne si externe, prin monitorizarea accesului la sistemele critice si detectarea activitatii neobisnuite
- Sa furnizeze automatizare completa a proceselor de colectare si normalizare de evenimente
- Sa monitorizeze activitatea utilizatorilor; sa colecteze si sa coreleze utilizatori si administratori si sa alerteze automat atunci cand intervin activitati anormale

- Sa asigure integritatea log-urilor. Sa poata utiliza zone tampon pe sursele monitorizate, unde evenimentele sa fie duplicate la generare, astfel incat sa se eveite posibilitatea de interventie umana asupra surselor de log-uri.
- Sa asigure redundanta functionala
- Sa furnizeze un mecanism de criptare si comprimare a datelor stocate, pentru un timp de retentie nedefinit. Sa garanteze ca o data stocate, log-urile nu mai pot fi alterate in nici un mod.
- Sa furnizeze capacitati de analiza a anomaliilor; sa simplifice tendintele activitatii de sistem si sa detecteze incidentele de securitate.
- Sa permita customizarea colectarii si raportarii, pe baza de wizard-uri de configurare
- Sa permita managementul centralizat al agentilor (instalarea si dezinstalarea automata si manuala a agentilor)

Intrucat colectarea, normalizarea si corelarea datelor sunt critice pentru succesul unui audit performant si eficient, urmatoarele cerinte sunt minime si obligatorii:

- Sa se poata colecta cantitati mari de date folosind o arhitectura scalabila
- Evenimentele sa fie stocate intr-o structura alta decat baza de date, pentru a minimiza cerintele de stocare si pentru a permite stocarea datelor pentru cel putin 3 ani. Aceste log-uri trebuie sa poata fi accesate in orice moment si importate selectiv intr-o baza de date pentru necesitati de raportare, analiza si investigatii
- Evenimentele sa poata fi importate din arhive intr-o baza de date dedicata, pentru necesitati de raportare programata si analize investigationale; importul sa poata fi granularizat in functie de necesitati, inclusiv prin mecanisme automate, pentru a minimiza volumul de date asupra carora se vor genera rapoarte
- Sa permita accesul rapid la evenimentele stocate, cu costuri minime de spatiu si fara a implica echipamente lente cum ar fi benzile de backup
- Sa fie posibila filtrarea, arhivarea si criptarea log-urilor la sursa, pentru a minimiza impactul asupra retelei si asigura securitatea datelor
- Sa se poata derula cautari in evenimentele arhivate si sa se poata raporta pe baza unor criterii date
- Sistemul centralizat de colectare de log-uri sa fie integrat in solutie
- Sa existe posibilitatea de granularizare detaliata a colectarii

Analiza evenimentelor si raportarea regulata vor furniza echipei de securitate sumarizari detaliate si vizualizari ale activitatii din mediul informatic. Aceste informatii sunt necesare pentru a:

- Dovedi conformitatea regulamentara catre auditori
- Asigura asupra conformitatii utilizatorilor cu politicile de securitate interne

- Urmari activitatea administrativa
- Asista activitatea biroului de statistica din cadrul Ministerului Justitiei, in sensul determinarii accesului preponderent al utilizatorilor la anumite legi spre deosebire de altele

Toate rapoartele vor trebui sa ofere o compilatie completa si relevanta de date. Solutia agreata trebuie:

- Sa filtreze evenimentele colectate pentru a prezenta spre raportare numai acele evenimente necesare in rapoartele produse
- Sa optimizeze storage-ul pentru analize de date
- Sa furnizeze rapoarte predefinite, specifice problemelor; acestea sa fie prezentate in sursa deschisa pentru a putea fi customizate de personalul intern
- Sa furnizeze rapoarte conforme specificului autoritatii contractante, care sa poata fi dezvoltate intern cu un minim de efort prin modificarea rapoartelor predefinite sau programarea de noi rapoarte intr-o interfata prietenoasa
- Sa dispuna de posibilitatea customizarii rapoartelor, bazata pe o tehnologie standard de industrie
- Sa distribuie rapoartele catre destinatiile necesare: export in formatele comune TXT, CSV, XLS, PDF, DOC, HTML, prin salvare pe disc sau expediere e-mail
- Sa poata fi usor de generat si distribuit, in baza unei programari si bazat pe continut

Pentru relevanta raportarilor, sistemul de corelare a evenimentelor si raportare trebuie:

- Sa asigure agregarea si afisarea contului utilizator in toate rapoartele, inclusiv in rapoartele generate din evenimente in care acesta nu este continut (de exemplu, evenimente care contin numai adresa IP a statiei de lucru)
- Sa coreleze evenimente din surse situate geografic diferit sau din fusuri orare diferite

In vederea derularii de analize investigationale, este cerinta obligatorie ca solutia agreata sa furnizeze un portal care sa unifice toate sursele de date (evenimente de platforma, modificari de politici globale etc.) in rapoarte consolidate care sa reflecte nivelul de securitate si conformitate al sistemului

Solutia va prezenta in portalul de analiza investigationala toate rapoartele predefinite sortate dupa tehnologie. De asemenea, solutia va oferi seturi de rapoarte predefinite dupa standardul si specificatia de conformitate din standarde acoperite de:

- ISO27001
- SOX

- JSOX
- COSO
- HIPAA
- PCI

Remedierea posibilelor violari de securitate si devieri de la conformitate pot fi posibile numai cu suportul unui mecanism de alertare inteligent, predefinit si complet customizabil.

Solutia trebuie sa dispuna de un mecanism de alertare asupra evenimentelor sensibile de securitate, cu posibilitatea de a crea noi alerte in baza unor politici flexibile. Noi reguli de alertare vor putea fi definite in baza unor criterii singulare, corelate sau de excludere, inclusiv:

- Eveniment singular – cand un singur eveniment indica situatia care necesita remediere
- Evenimente corelate – cand trebuie detectata o situatie specifica, definita in termeni de evenimente care survin in aproximativ acelasi timp
- Cumul de evenimente – cand trebuie detectata o situatie in care actiuni similare se deruleaza intr-o succesiune rapida
- Lipsa unui eveniment – cand se asteapta evenimente specifice intr-un anumit interval de timp sau intr-o anumita situatie data, dar acest sau aceste evenimente nu mai au loc
- Lipsa unui eveniment corelat – cand trebuie urmarite situatii sau procese in care actiunile subsecvente nu mai au loc
- Reguli particularizate – cand se doreste detectarea unei situatii care nu poate fi definita prin celelalte modele de reguli

Solutia trebuie sa permita monitorizarea in timp real a sistemelor UNIX/Linux si echipamentelor de retea, fara a avea nevoie de agenti distribuiti; de asemenea, sa permita monitorizarea in timp real a sistemelor Windows.

Sistemul de monitorizare in timp real va dispune de functionalitati de confirmare si notificare. Sistemul va avea capacitatea sa notifice imediat administratorii asupra activitatilor de frauda si sa genereze actiuni automate (dezactivarea contului utilizator compromis, anularea modificarilor frauduloase de permisiuni etc.), si va contine o lista predefinita de alerte pentru a facilita implementarea de politici de securitate:

- Modificarea unui cont computer
- Crearea unui cont computer
- Stergerea unui cont computer
- Autentificare utilizator reusita
- Autentificare utilizator esuata (cont blocat)

- Crearea unui cont utilizator
- Stergerea unui cont utilizator
- Deblocarea unui cont utilizator
- Membru adaugat unui grup
- Membru sters dintr-un grup
- Crearea unui nou grup
- Stergerea unui grup
- Modificarea politicii globale de audit
- Modificarea politicii de domeniu
- Oprirea auditului
- Adaugarea de drepturi administrative pentru un utilizator sau un grup
- Stergerea drepturilor administrative pentru un utilizator sau grup
- Adaugarea unui membru intr-un grup administrativ
- Incercarea de a modifica parola unui cont administrativ
- Autentificarea reusita in afara programului de lucru
- Evenimente multiple de acces interzis
- Evenimente multiple de autentificare esuata
- Tentative multiple de a modifica o parola
- Evenimente de autentificare reusita dupa un numar de autentificari nereusite
- Stergerea unui log de audit
- Salvarea unui log de audit

1.1.7.7.Cerinte tehnice pentru salvare si recuperare

Solutia de backup trebuie sa asigure usurinta in instalare si configurare prin utilizarea unor asistenti dedicati procesului (wizard).
De asemenea, utilizarea produsului trebuie sa se faca de catre operatorii nostri printr-o integrata grafica intuitiva. Pentru job-uri customizate, administratorul trebuie sa se poata interfata la CLI (command line interface).
Aplicatia va trebui sa suporte toate modelele de backup/restaurare (full, incremental, differential) precum si o functie de consolidare a backup-urilor incrementale.
Solutia trebuie sa aiba o arhitectura modulara care sa asigure dezvoltarea acesteia in timp prin adaugarea unor diverse componente. Acestea trebuie sa se integreze cu usurinta astfel incat rezultatul sa fie extinderea functionalitatii.
De asemenea, estimand o crestere abrupta a datelor pe care trebuie sa le protejam, solutia va trebui sa permita un grad inalt de scalabilitate.

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

- licentiere standard pe server, clienti, device-uri, module etc.
- licentiere volumetrica a datelor care vor fi protejate.

Solutia trebuie sa aiba disponibili agenti si module specializate pentru interfatarea atat cu mediul virtual cat si cu mediul fizic. Avand in vedere platformele disponibile cat si pe cele pe care le avem in vedere pentru dezvoltarile ulterioare, aplicatia trebuie sa suporte platforme eterogene (Windows, Unix, Linux, MacOS).

De asemenea, solutia de backup trebuie sa dispuna de suport la nivel de aplicatie (in special pentru Exchange, Sharepoint) sau baza de date (in special pentru Oracle, SQL server, MySQL).

Utilizatorul, in functie de drepturile de acces pe care le primeste, trebuie sa aiba la dispozitie un planificator (scheduler) avansat de task-uri de backup, restaurare sau raportare.

Securitatea si Controlul accesului utilizatorilor trebuie asigurat in mod nativ de catre solutia care va fi propusa.
Initial, volumul total al datelor care trebuie protejate este de aproximativ 1 TB.
Dorim ca solutia sa permita utilizarea librariilor de benzi si in acest scop se va prezenta o lista de compatibilitate.
De asemenea, pentru diminuarea ferestrelor de backup, aplicatia va pune la dispozitie solutii de backup disk-to-disk (VTL sau alta tehnologie).
Pentru diminuarea spatiului de stocare, solutia va dispune de mecanisme avansate si configurabile de compresie a datelor.
De asemenea, solutia propusa trebuie sa aiba disponibila o functie de eliminare a redundantei datelor (deduplicare). Functia de deduplicare trebuie sa fie de preferat in mod off-line (configurabil in afara ferestrei de backup) si la un nivel maxim al eficientei – bit/bloc variabil.
In scopul reducerii traficului de retea, solutia trebuie sa asigure scenarii de utilizare eficienta SAN si de interfatare cu Network Attached Storage precum si compatibilitate NDMP (Network Data Management Protocol). Utilizatorul trebuie sa aiba posibilitatea initierii unui proces de compresie a transportului datelor prin retea.

Avand in vedere existenta datelor cu caracter confidential care trebuie protejate, solutia de backup va trebui sa asigure criptarea anumitor job-uri selectabile de catre utilizator.

Solutia va avea in vedere optimizarea si micsorarea ferestelor de backup prin tehnici specifice de automatizare, planificare si executie a task-urilor necesare. Solutia trebuie sa asigure functii specifice de back-up pentru toate tipurile de informatii : date statice, date vitale si informatii critice.

Solutia trebuie sa genereze rapoarte cu privire la operatiunile de salvare / restaurare;

Pentru scenarii de disaster recovery, solutia de backup va dispune de module specializate de backup/restaurare Bare Metal a serverelor Linux sau Windows. Procesul

de backup trebuie sa se execute transparent pentru utilizator, fara a fi necesara oprirea serverelor (hot/live backup).

Se vor asigura module dedicate protectiei infrastructurii virtuale a companiei (VMWare si HyperV).

Furnizorul trebuie sa asigure urmatoarele activitati:

- Instalarea solutiei
- Configurarea solutiei pe baza cerintelor beneficiarului
- Transferul de cunostinte privind utilizarea si administrarea solutiei

Instalarea si configurarea trebuie facute de personal specializat, certificat de producator.

Transferul de cunostinte trebuie facut de instructori specializati, certificati de producator.

Documentatia componentei de salvare si recuperare va contine urmatoarele documente in limba romana:

- Ghidul personalizat de instalare
- Ghidul personalizat de configurare
- Ghidul personalizat de operare si administrare. Acest ghid va fi utilizat in cadrul sesiunilor de transfer de cunostinte

1.1.7.1.Cerinte tehnice pentru replicarea intre cele doua centre de date

In vederea asigurarii disponibilitatii si securitatii datelor gestionate de catre sistemul informatic legislativ, se doreste realizarea replicarii datelor (baze de date, aplicatii) intre cele doua centre de date (primar si secundar).

Componenta de replicare a datelor intre cele doua centre de date va fi utilizata de beneficiar pentru sincronizarea si replicarea inteligenta a depozitelor de date structurate sau nestructurate din organizatie, oferind protectie in caz de dezastru, prin asigurarea unor copii de date realizate in timp real cu impact minim de performanta asupra surselor de informatii / date.

Cerinte generale pentru replicare

Solutia de replicare aleasa intre cele doua centre de date va avea in vedere urmatoarele aspecte. Toate datele din centrul de date primar vor trebui sa fie replicate in centrul de date secundar folosind reteaua IP dintre cele 2 amplasamente, prin una din urmatoarele metode:

- replicare prin mecanisme native specifice pentru toate serverele de baze de date din sistem
- copiere/reinstalare pentru serverele cu date cu continut static si in cazuri exceptionale (aplicare de patch-uri etc.)

Banda maxima de comunicatii care va fi disponibila pentru replicarea datelor este de 100 Mb/s. Circuitele de comunicatii vor fi puse la dispozitie de beneficiar prin intermediul STS.

Timpul de replicare a datelor din centrul primar in centrul de disaster recovery trebuie sa fie de maxim 60 de minute.

Timpul de recuperare in caz de dezastru a activitatii in centrul de date secundar prin aplicarea procedurilor de recuperare in caz de dezastru trebuie sa fie de maxim 4 ore de la momentul declararii de catre personalul abilitat al Beneficiarului a indeplinirii conditiilor de declarare a dezastrului in centrul primar si de incepere a aplicarii procedurilor necesare pentru repornirea tuturor sistemelor si a serviciilor in centrul de date secundar.

1.1.8.Infrastructura Hardware necesara

Sistemul propus trebuie sa fie un mediu complet - furnizorul va livra infrastructura hardware necesara functionarii sistemului. Sistemul propus nu va afecta functionalitatile serviciilor existente.

Sistemele si echipamentele livrate trebuie sa fie noi, neutilizate si de ultima generatie. Ele trebuie sa asigure gradul solicitat de performanta, fiabilitate si flexibilitate fiind proiectate si destinate pentru aplicatii critice “enterprise level”.

Dispozitivele hardware trebuie sa fie astfel proiectate incat sa poata asigura scalarea sistemului in cazul cresterii nevoii de putere de calcul

Dispozitivele hardware trebuie sa fie compatibile cu caracteristicile retelei electrice din Romania astfel incat sa nu existe probleme la conectarea acestora la reteaua electrica.

Arhitectura solutiei propuse trebuie sa includa urmatoarele caracteristici generale de fiabilitate, disponibilitate si usurinta in efectuarea service-ului (Reliability Availability Serviceability- RAS) la nivel de servere sau sasiu:

- componente redundante in interiorul sistemului (surse de alimentare electrica).
- capabilitati de auto-testare si rezolvare a defectelor intermitente fara interventie umana
- dealocarea “online” si izolarea componentelor defecte ale sistemului (de exemplu discuri, ventilatoare, subsisteme de alimentare cu energie electrica, adaptoare PCI); in momentul reboot-ului componentele defecte vor fi deconfigurate
- diagnosticarea erorilor in timp real.
- capabilitati arhitecturale de prevenire a erorilor

Echipamentele care vor fi livrate si care compun solutia tehnica asigurand atat Main Center cat si Disaster Recovery Center constau in:

Numar	Descriere	Cantitate
1	Rack si accesorii (1 MC +1DRC)	2
2	Surse neintreruptibila de curent (3 MC+3DRC)	6
3	Sasiu Servere Blade(1 MC +1DRC)	2
3.1	Server Blade (4 MC +4DRC)	8

3.2	Switch SAN blade (2 MC +2DRC)	4
3.3	Switch Ethernet blade (2 MC+2DRC)	4
3.4	Dispozitiv stocare extern (1 MC+1DRC)	2
4	Unitate benzi de backup (1 MC)	1
5	Router (2 DRC)	2
6	Firewal(2 MC+2DRC)	4

Articol 1 – Rack si accesorii	
Cantitate	**2**
Descriere	**Rack si accesorii**
Rack	Ansamblu modular standard de 19 inchi, cu 42U disponibili pentru pozitionarea echipamentelor. 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 posibildin punct de vedere functional).
	Structura interna a rack-ului va facilita pozitionare cablurilor, pentru distribuirea echilibrata a bugetului de conexiuni, respectiv pentru a implementa o schema de asigurare a redundantei (la nivel de alimentare, interconectare SAN, LAN etc.) si evitarea conditiilor de tip single-point-of-failure.
Console	monitor TFT, de min. 17inch si suport pentru afisare de r ezolutii native 1280x1024; tastatura USB cu dispozitiv integrat de tip touch-pad; porturi de acces la consolele KVM si la porturile usb si video di n nodurile de procesare astfel incat toate nodurile de procesare sa fie deservite de monitorul si tastatura incluse in consola (nu mai putin de 4 porturi de acces KVM). Pliata, consola va ocupa un spatiu optim de 1U in rack.

Cabluri	Oferta va include toate cablurile de interconectare interna si externa a componentelor solutiei (alimentare cu energie electrica, conexiune LAN,conexiune SA etc.)

Articol 2– Surse neintreruptibile de curent	
Cantitate	**6**
Descriere	**Surse neintreruptibile de curent**
UPS	Se va implementa o structura eficienta de alimentare de tip UPS compusa dintr-o unitate discreta independenta de tip on-line, monofazata (1/1) de 5KVA. Aceasta structura trebuie sa ofere un timp de functionare in regim de avarie de minim 15 de minute la o incarcare preconizata de minim 50%. Arhitectura preconizata este de natura sa aiba cost si complexitate minime, precum si un nivel optim de disponibilitate operationala; 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. Unitatea UPS trebuie sa permita extinderea timpului de functionare in regim de avarie prin cel putin un modul discret de baterii, integrabil in structura fara necesitatea opririi alimentarii echipamentelor deservite. Componentele interne ale unitatilor UPS, inclusiv bateriile, vor fi de tip hot-swap si vor permite deservirea (inclusiv inlocuirea acestora) fara oprirea sarcinii. Unitatea UPS va include modul de management pentru monitorizare la distanta, inclusiv software de management si idicatori frontali pentru suprasarcina si nivel incarcare module de baterii.

Articol 3 – Sasiu Servere Blade	
Cantitate	**2**
Descriere	Sasiu cu suport pentru integrarea modulelor de procesare, a extensiilor de I/O ale acestora precum si a modulelor de management. Suport pentru minim 14 servere tip blade

Format	Design modular, maxim 9U, montabil in cabinet de 19” cu toate accesoriile necesare montarii incluse Sasiul trebuie configurat pentru instalarea de noduri de procesare de tip blade sau similare, optimizate pentru asigurarea densitatii si puterii de calcul necesare Pentru asigurarea puterii de calcul necesare si adaptarii la cerintele diverselor aplicatii, fiecare sasiu va suporta configurarea si echiparea cu module (noduri) de procesare de tip blade pe 64 biti, in arhitectura CISC x86 si/sau RISC/EPIC (sau derivate din EPIC). Sasiu montabil in cabinet sistem, cu suport pentru cel putin 14 module blade, cu posibilitatea intermixarii acestor module blade in sasiu in orice mod
Caracteristici de inalta disponibilitate	Midplane de inalta disponibilitate care suporta functii de tip hot-swap la nivel de server blade individual, module de interconectare LAN, module de management, surse de alimentare Sasiul va fi echipat cu toate componentele redundante, hot-plug / hot-swap si utilizabile in mod concurent, pentru alimentare si ventilare, management (inclusiv procesoare de serviciu / management).
Arhitectura I/O	Suport pentru minim opt module I/O interne pentru interconectare in tehnologie 1Gbps Gigabit Ethernet, 10 Gbps Ethernet, 8 Gbps Fibre Channel.
Surse de alimentare	Minim patru surse hot-swap, instalate intern in sasiu, redundante n+n, alimentare la 200-240 Vac. Sistemul va permite alimentarea concurenta a fiecarui modul sursa prin cel putin 2 componente (cai de alimentare) intermediare PDU sau similare. 2 module cu cate 2 surse de alimentare de minim 2800 W fiecare, hot-swap, instalate intern in sasiu, redundante n+n, alimentare la 200-240 Vac
Unitate Optica	Unitate optica DVD-RW interna, pe panoul frontal, accesibila de fiecare din serverele blade instalate in sasiu.
USB	Minim doua porturi USB pe panoul frontal pentru unitati media aditionale, accesibile de oricare dintre serverele blade instalate in sasiu.
Sistem de ventilatie	Baterii de ventilatoare tip hot-swap, redundante, instalate intern in sasiu

Module switch	Subsistemul va include componente discrete, implementate pentru configurare si operare independenta sau ca module in sasiul platformei de procesare - Atunci cand acestea se vor implementa independent, porturile de comunicatie individuale din fiecare modul de procesare de tip blade vor fi accesibile direct, din afara sasiului sub-sistemului de procesare, fara dispozitive intermediare de conectare, prin componenta neutra de tip pass-through. - Atunci cand acestea se vor implementa ca module in sasiul sub-sistemului de procesare, vor dispune de cel putin cate un port intern de conectare pentru fiecare modul de procesare blade pe care il deservesc.
Conectivitate "high speed" (10 Gbps)	Minim 2 module ce vor asigura conectivitate externa prin minim 10 x 10Gb porturi Ethernet fiecare, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2, echipate cu module de conectare SFP+ fiecare
Conectivitate Fibre Channel	Minim 2 module ce vor asigura conectivitate externa prin minim 6 x 8 Gbps porturi Fibre Channel
Management sistem	Suport pentru management de la distanta, redirectare interfata grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta pentru fiecare server blade, switch instalat, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer). Module de management centralizat pentru intregul sasiu, hot-swap, redundante 1+1, cu switch KVM incorporat pentru toate modulele de procesare de tip blade. - Suport pentru management de la distanta, redirectare interfata grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta pentru fiecare server blade, switch instalat, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer), integrare LDAP (Lightweight Directory Access Protocol). - Modulul de management trebuie sa dispuna de porturi USB pentru tastatura si mouse, port VGA pentru conectare la monitor, port RJ-45 pentru management. Modul de tip KVM inclus, rack-mountable 1-2U, format din: - monitor TFT, de min. 17” si suport pentru afisare de

	rezolutii native 1280x1024- tastatura USB cu dispozitiv integrat de tip touch-pad. Consola va avea porturi de acces si interconectare cu consolele KVM din componentele platformei de stocare: min. 8 x porturi locale KVM/Cat5 pentru acces local.

Articol 3.1 – Servere Blade	
Cantitate	**8**
Descriere	**NOD DE CALCUL – Server lamelar**
Arhitectura	Modul de procesare de tip blade, compatibil cu sasiul ofertat
Procesor	Procesor CISC x86 octo-core, la frecventa de minim 2,5 GHz, minim 20 MB L3 cache pentru fiecare procesor, suport pentru doua procesoare, doua procesoare instalate
Memorie interna	128 GB 1600MHz ECC DDR3, suport pentru ChipKill sau echivalent, respectiv pentru configurare in mod hot-spare si pentru memory mirroring; fiecare modul de procesare va putea scala la minim 512 GB RAM prin extindere ulterioara
Hard disk	Minim 2 x 146 GB SAS 15.000 rpm
Video	Controller video integrat cu memorie de minim 16MB
Interfete retea	Interfete de retea Dual 10 Gbps Ethernet integrate, suport pentru failover si load balancing, suport TCP/IP Offload Engine (TOE) Minim 4 x porturi 10 Gb Etherne
Interfata Fibre Channel	Minim 2 x porturi 8 Gbps HBA
Sloturi I/O	Minim 2 x PCI-Express 2 x porturi USB
Management de sistem	Procesor de management integrat, capabilitati de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local si la distanta -Suport pentru functii de diagnostic, reset, POST si auto-recuperare -Serverul va fi livrat impreuna cu aplicatia de management realizata de producatorul echipamentului, aplicatie ce trebuie sa asigure cel putin: inventarierea componentelor, monitorizarea starii de functionare, trimiterea de alerte prin e-mail
Conectivitate servere blade	Fiecare server blade trebuie sa dispuna de conectori redundanti pentru alimentare electrica, semnale I/O,

	management
Compatibilitate sisteme de operare	Sisteme de operare compatibile, certificate de producator: Microsoft Windows Server 2008 si 2012 Web/Standard/Enterprise, SUSE Linux Enterprise Server 11, Red Hat Enterprise 5 sau superior, VMware ESX 4.0 sau superior - licențe pentru sistemul de operare (8 servere) – vezi 2.6.1.2 - licențe baze de date per procesor (8 procesoare) – vezi 2.6.1.3

Articol 3.2 – Switch SAN blade	
Descriere	Switch Storage Area Network lamelar
Cantitate	**4**
Porturi	Minim 6 porturi externe 8 Gb Minim 16 porturi interne 8 Gb
Rata Transfer	Agregat 48 Gbps
Management	Serial RJ-45 USB HTTP, SNMP v1/v3, SSH; Auditing, Syslog;

Articol 3.3 – Switch Ethernet blade	
Descriere	Switch Ethernet lamelar
Cantitate	**4**
Porturi	Minim 10 porturi externe 10 GbE (scalabil pina la minim 12 porturi) Minim 14 porturi interne 10 GbE (scalabil pina la minim 36 porturi)
Rata Transfer	Minim 1Tbps
Protocoale	IPv6 management (full IPv6 support) 1,024 configurable VLANs (IEEE 802.1Q)

	IEEE 802.1ad IEEE 802.1w IEEE 802.1d IEEE 802.1s IEEE 802.1p QoS (metering, remarking, DSCP/CoS) BGP 4, RIPv1, RIPv2 OSPF v2 (RFC 2328) with ECMP, OSPF (RFC 3101) DHCP/BootP DHCP Relay (RFC 3046) 802.1p (Priority Queues), IEEE 802.3x Flow Control IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) & IGMP v3 Multicast Snooping, IGMP Filtering, IP Forwarding Jumbo Frame (12K) Static Routing
Management	RJ-45 USB SNMP V1, V2 and V3 HTTP Graphical User Interface CLI Telnet interface SSH Secure FTP NTP

Articol 3.4 – Dispozitiv stocare extern	
Cantitate	**2**
Descriere	Sistem de stocare date, "dual controller" Sistemul trebuie sa nu depaseasca dimensiune de 2U in configuratia ofertata.
Arhitectura	Sistem de stocare modular, care sa permita scalabilitatea performantei si capacitatii non-disruptiv. Nu se accepta solutie compusa din mai multe sisteme de stocare independente/distincte care cumulat sa indeplineasca cerintele de performanta (ex: numar de porturi, memorie cache, numar maxim de discuri, IOps, etc) Sistemul trebuie sa nu depaseasca dimensiune de 2U in configuratia ofertata. Sistemul trebuie sa permita upgrade-ul la un sistem

	superior fara a pierde datele aflate pe discurile deja existente. Migrarea trebuie sa se realizeze cu aceleasi discuri cu posibilitatea de a respecta aceeasi configuratie. Astfel echipamentul ofertat trebuie sa poata fi upgradat la sisteme de tip High end care dispun de cel putin 380 de discuri.
Tipuri RAID suportate	RAID 0, 1, 10, 5, 6, 50
Interfata catre host	4 porturi FC la o viteza de 8 GBps, Cu posibilitatea de schimbare a conectivitatii catre host la : 4 x iSCSI la viteza de 1 GBps sau 10 GBps 4 x SAS la viteza de 6 GBps Conectivitatea catre host trebuie sa se realizeze direct, prin intermediul solutiei de stocare ofertata. Nu sunt acceptate sisteme de virtualizare care sa permita un upgrade al nivelului de conectivitate la tehnologie ISCSI sau SAS.
Conectivitate back-end	SAS minim 2 porturi, viteza de 12GBps
Cache	Minim 8 GB memorie cache Sistemul ofertat trebuie sa dispuna de baterie pentru backup la nivelul controllerului pentru a nu avea pierderi in cazul unei intreruperi a alimentarii cu energie electrica sau din cauza altor factori.
Tipuri HDD suportate	SAS, NL-SAS si SSD cu posibilitatea de a fi mixate in interiorul aceluiasi sertar de expansiune cu posibilitatea de a fi mixate in interiorul aceluiasi sertar de expansiune. Sistemul propus trebuie sa poata integra discuri la urmatoarele viteze : 7200 rpm, 10000 rpm si 15000 rpm. Sistemul propus trebuie sa poata integra discuri cu dimensiunea de 2.5” cat si cu dimensiuni de 3.5”.
Discuri instalate	14 x 600 GB SAS, 10k rpm
Numar HDD instalabile	scalabil online pana la minim 95 discuri
Surse de	2 surse hot-plug care sa ofere redundanta

alimentare	
Software inclus in configuratia ofertata	Software pentru managementul sistemului de discuri de la acelasi producator cu unitatea de stocare. Documentatia pentru sistemul de management se va livra in sistem electronic pe unitate de tip DVD cat si hard copy in limba Romana. Suportul tehnic (atat electronic cat si hard copy) trebuie sa provina de la furnizorul echipamentului de stocare. Sistemul ofertat trebuie sa se livreze si cu urmatoarele aplicatii software: Aplicatie pentru multipath pentru cel putin 10 servere cu sistem de operare MS Windows Aplicatie pentru multipath pentru cel putin 10 servere cu sistem de operare Linux Aplicatie pentru multipath pentru cel putin 20 servere virtualizate cu aplicatia Vmware Aplicatie pentru multipath pentru cel putin 5 servere cu sistem de operare AIX Thin Provisioning Sistemul ofertat trebuie ofere posibilitatea adaugarii (cu un cost aditional) a urmatoarelor aplicatii software avand acealasi producator cu unitatea de stocare (se va descrie si functionalitatea aplicatiilor de mai jos): Aplicatie pentru monitorizarea performantei Aplicatie pentru realizarea de copii dinamice Aplicatie pentru replicarea datelor local Aplicatie pentru replicarea datelor la distanta Aplicatie care sa permita replicarea bazelor de date SQL Aplicatie care sa permita volume de tip WORM
Certificari sisteme de operare	Windows Server 2003/2008/2012, RHEL, SLES, Solaris, AIX, HP-UX, Vmware
Redundanta si disponibilitate	Module memorie cache, surse de alimentare, ventilatoare Sistemul trebuie sa permita upgrade-ul online pentru firmware-ul controllerelor si pentru cel al discurilor. Sistemul trebuie sa permita adaugarea online de noi cutii cu discur si de noi discuri
Garantie	3 ani cu timp de raspuns de 2 ore si timp de remediere

	de 24 ore.
Certificari	Sistemul va avea cel putin urmatoarele certificari (se vor prezenta documente care sa ateste aceste certificari) : UL, CSA, CE, FCC
Performanta	Sistemul ofertat trebuie sa asigure minim urmatoarele performante (nivelul de performanta trebuie sa fie indicat pe pagina web a producatorului unde este descris echipamentul sau in documentatia acestuia): Minim 270K IOPS Minim 4 GB/s throughput Minim 9400 IO/s pentru TPCC citire / scriere cu discuri la viteza de 10krpm Minim 40000 IO/s pentru citire random cu discuri de tip SSD

Articol 4 – Unitate de backup	
Cantitate	**1**
Descriere	Biblioteca de benzi
Caracteristici	- unitate de stocare rackabila cu inaltime de maxim 2U - capacitate de incarcare cu benzi magnetice de 24 sloturi - 2 unitati de citire/scriere benzi magnetice cu conectivitate Fibre Channel - Tipuri de unitati de citire/scriere suportate: LTO-4, LTO-5, LTO-6. - Unitatea de stocare va fi livrata cu 2 unitati LTO-5 - 1 licență necesară funcționării – vezi 2.6.1.7

Articol 5 – Router	
Cantitate	**2**
Descriere	Echipament Router comunicatii
Forma	Rack max 2U
Interfete	2 x 10/100/1000 Mpbs- RJ-45 1 x Serial 1 x USB
Memorie RAM	Minim 512MB

Management la distanta	SNMP RMON
Standarde	IEEE 802.3 IEEE 802.1Q IEEE 802.3af IEEE 802.3ah IEEE 802.1ah IEEE 802.1ag ANSI T1.101 ITU-T G.823 ITU-T G.824
Protocoale de rutare	OSPF IS-IS BGP EIGRP DVMRP PIM-SM IGMPv3 GRE PIM-SSM static IPv4 routing static IPv6 routing policy-based routing (PBR) MPLS Bidirectional Forwarding Detection (BFD) IPv4-to-IPv6 Multicast
Functionalitati	Suport SSL Firewall protection Suport VPN Suport MPLS Logare loguri Suport IPv6 Suport Dynamic Multipoint VPN Management orientat Web Services NetFlow

Articol 6 - Firewall	
Cantitate	**4**
Numar porturi	Minim 6

10/100/1000Base-T RJ45	
Firewall throughput	Minim 2.9 Gbps
VPN throughput	Minim 400 Mbps
Sesiuni concurente	Minim 1 milion
Conexiuni pe secunda	Minim 20.000
IPS throughput default/profil recomandat	Minim 2 Gbps / 0.3 Gbps
VLAN-uri suportate	Minim 1024
Spatiu de stocare	Minim 250 GB
Sisteme virtual suportate default /max	3/3
Suport pentru network address translation	Suport pentru NAT static sau ascuns cu functionalitate de adaugare de reguli in mod automat sau manual
Suport DHCP	Suport pentru adrese IP dinamice
Suport VLAN	minim 256 de VLAN-uri

3. Servicii si livrabile

Se doreste ca echipamentele si produsele software furnizate sa fie insotite de servicii de implementare si de project management de calitate, care sa garanteze atingerea cu succes a obiectivelor proiectului.

Furnizorul va presta toate serviciile necesare pentru implementarea solutiei in conformitate cu recomandarile producatorului si cerintele functionale si tehnologice prezentate in Caietul de sarcini, precum si rezultate in urma etapei de analiza a proiectului. Toate costurile asociate trebuie cuprinse in oferta financiara.

3.1. Servicii de furnizare continut baza de date legislativa si actualizare continut

Ofertantul va prezenta beneficiarului baza de date legislativa actualizata cu actele la zi, conform cu cerintele specificate in capitolul cerinte nivel baza de date.

Ofertantul va prezenta modul de organizare al bazei de date si metodologia de actualizare a continutului bazei de date (inclusiv structura pachetului de actualizare).

Achiziția bazei de date include şi serviciile aferente de actualizare a acesteia. Astfel, ofertantul va realiza, cu titlu gratuit, actualizarea continutului bazei de date legislative, pe perioada implementării proiectului şi pentru o perioada de 36 de luni (3 ani) calculate de la momentul acceptanței şi punerii în producție a aplicației legislative care permite interogarea bazei de date legislative.

Ofertantul va prezenta un plan pentru realizarea actualizarii periodice a bazei de date, astfel incat introducerea unui document nou sa nu se realizeze cu o intarziere mai mare de 3 zile de la data publicarii.

Pe parcursul perioadei de actualizare conform caietului de sarcini, Ofertantul va prezenta la sfarsitul fiecarei luni (in primele 5 zile lucratoare din luna urmatoare), rapoarte cu documentele nou introduse in luna respectiva.

Serviciile de furnizare continut baza de date legislativa si actualizare continut vor include in mod obligatoriu urmatoarele livrabile:

- Baza de date legislativa actualizata la zi
- Document cuprinzand designul bazei de date legislative (tabele, chei primare, chei referentiale)
- Document cu planul de actualizare a continutului bazei de date legislative
- Rapoarte lunare de actualizare a continutului bazei de date legislative

3.2. Servicii de achizitie echipamente, implementare infrastructura hardware si software de baza

Se va stabili configuratia echipamentelor conform specificatiilor tehnice din caietul de sarcini.

Livrarea echipamentelor la beneficiar se consemneaza prin notele de receptie si constatare pentru evidentierea conformitatii din punct de vedere cantitativ si fizic a celor livrate.

Se va asigura disponibilitatea echipamentelor in momentul in care acestea devin necesare . In aceasta etapa se va realiza si configurarea facilitatilor de disponibilitate ridicata si load balancing, precum si instalarea si configurarea produselor software de sistem (sisteme de operare, RDBMS, backup).

La finalizarea activitatilor de instalare, punere in functiune si configurare a echipamentelor, se incheie la beneficiar un proces-verbal de receptie calitativa in care

se consemneaza conformitatea din punct de vedere calitativ potrivit prevederilor contractuale in acest sens.
Livrarea echipamentelor hardware si a licentelor software standard va fi realizata de catre personalul Furnizorului si se va realiza in conformitate cu Graficul de proiect. Beneficiarul va asigura conditiile tehnice pentru desfasurarea in bune conditii a acestor activitati pe amplasamente.

Ofertantul va realiza instalarea echipamantelor hardware si de comunicatie si a sistemului informatic legislativ cu toate componentele sale in centrul de date al Beneficiarului. Personalul IT desemnat de beneficiar va asista la instalare si va fi instruit astfel ca pe viitor sa poata replica instalarea aplicatiei.

In aceasta etapa ofertantii vor include in mod obligatoriu urmatoarele livrabile:

- Planul de instalare si configurare infrastructura
- Echipamente hardware
- Licente software
- Realizare configuratie hardware si software de baza
- Document cuprinzand configuratia hardware conform cu cerintele tehnice de infrastructura si planul de implementare
- Document cuprinzand configurarea software-ului de baza conform cu cerintele de arhitectura tehnice si planul de implementare

3.3. Servicii de dezvoltare aplicatie software web

Acest grup de activitati cuprinde toate sarcinile specializate de construire a aplicatiei informatice pentru accesul neingradit la baza de date legislativa. In conformitate cu ciclul de viata standard al unui proiect de dezvoltare software, acestea cuprind activitati de analiza, proiectare, dezvoltare si configurare.

Ofertantii trebuie sa prezinte detaliat livrabilele care vor rezulta in urma prestarii serviciilor corespunzatoare etapelor de analiza si proiectare.

1.1.9. Analiza

In vederea implementarii sistemului, Ofertantul va trebui sa execute activitati de analiza, desfasurate in cadrul institutiei Beneficiarului, avand la baza cerintele operationale ale sistemului descrise modular in specificatiile tehnice.

Ofertantii trebuie sa descrie in detaliu metodologia dupa care vor derula activitatile de analiza
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.
- Analiza sistemului existent:
    - Va consta in analiza situatiei din momentul de fata din cadrul institutiei Beneficiarului prin sedinte de analiza, chestionare etc.; se vor identifica problemele pe care institutia doreste sa le rezolve prin realizarea acestui proiect.
    - Definirea cerintelor informationale specifice, impuse de solutia recomandata (identificarea utilizatorilor care au nevoie de informatie, unde, cand, in ce forma, ce continut.
    - Definirea scenariilor de utilizare a aplicatiilor

La baza acestei etape vor fi cerintele de arhitectura logica si operationala, precum si functionalitatile descrise in specificatiile tehnice din caietul de sarcini.

1.1.10.Proiectare

Utilizand documentele rezultate in etapa de analiza, ofertantul va realiza proiectul tehnic al aplicatiei informatice, care va oferi interfata de utilizare a bazei de date legislative.

Proiectul tehnic va cuprinde:

- Specificatii tehnice arhitectura
    - Arhitectura hardware si software
    - Disponibilitate
    - Performanta
- Specificatii design aplicatie:
    - Specificatii nivel baza de date
        - Interconectarea si utilizarea bazei de date legislative
    - Specificatii nivel aplicatie logica alcatuire modulara:
        - Organizare pe
            - Module
            - Obiecte
            - Proceduri
    - Specificatii nivel prezentare
        - Interfete http
        - Scenarii de utilizare

1.1.11.Dezvoltare/configurare si testare interna

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

Plecand de la prototipul functional aprobat in cadrul etapei anterioare si pe baza unor iteratii succesive de dezvoltare, se vor derula urmatoarele activitati:

1. Dezvoltarea componentelor de software.
2. Teste la nivelul codului sursa si la nivel de modul.
3. Documentarea scenariilor detaliate de testare.
4. Instalarea si configurarea domeniului de testare.

1.1.12. Punere in productie

Ofertantii trebuie sa prezinte planul care va fi utilizat la trecerea in productie a sistemului.

Serviciile de dezvoltare aplicatie software web vor include in mod obligatoriu urmatoarele livrabile:

- Raport de analiza cuprinzand:
  - Cerinte modificare design baza de date legislativa
  - Cerinte design aplicatie
  - Cerinte de business pentru interfetele http /web services
  - Cerinte pentru scenarii de utilizare ale aplicatiei
- Proiect tehnic
- Aplicatie software
  - Cod sursa
  - Fisiere binare(daca e cazul)
  - Fisiere de configuratie(daca e cazul)
  - Licenta aplicatie(daca e cazul)
- Raport de punere in productie

3.4. Servicii de asigurare a interconectarii bazei de date nationale cu sistemul european NLEX

In vederea implementarii sistemului, Ofertantul va trebui sa execute activitati de analiza a standardului de interconectare, avand la dispozitie documentul care stipuleaza modalitatea prin care portalul NLEX interactioneaza cu aplicatiile legislative nationale.
In urma analizei standardului, ofertantul va realiza implementarea conectorilor, testarea interna si punerea in productie a acestora.

Serviciile de dezvoltare aplicatie software web vor include in mod obligatoriu urmatoarele livrabile:

- Raport de analiza standard NLEX
- Codul sursa pentru conectori
- Raport de testare functionalitate conectori
- Raport de punere in productie conectori

3.5. Servicii de instruire

Ofertantul va asigura instruirea personalului de specialitate IT din cadrul Ministerului Justitiei in ceea ce priveste administrarea noului sistem informatic – conditie esentiala in vederea asigurarii mentinerii in functiune, in parametri optimi, a acestuia.

Vor fi instruiti cel putin 5 administratori de sistem.

Programul de instruire destinat administratorilor de sistem va contine minim urmatoarele aspecte:

- proiectarea si administrarea sistemului dezvoltat;
- administrarea bazelor de date componente ale sistemului;
- monitorizarea performantelor sistemului;
- asistenta utilizatorilor interni ai sistemului.

Administrarea sistemului

Instruirea se adreseaza administratorilor de sistem, administratorilor de baze de date, dezvoltatorilor care vor mentine solutia si va urmari furnizarea necesarului de cunostinte la nivelul specialistilor Ministerului Justitiei pentru mentinerea in productie a sistemului implementat.

Instruirea va conține atât un modul teoretic, cât şi unul practic, utilizându-se, ca material principal de instruire, sistemul efectiv dezvoltat. Instruirea se va finaliza prin examinarea cursanților (testare scrisă tip grilă sau întrebări cu răspuns liber) şi, în cazul în care cursanții întrunesc punctajul minim obligatoriu, formatorul le va elibera certificat de monitorizare şi administrare a sistemului dezvoltat în cadrul proiectului.

Obiectivele si caracteristicile acestei instruiri sunt:

Instruire	Obiective	Nr. Participanti	Nr. zile	Nr. Sesiuni
Administrarea sistemului informa	**Obiective:** - Intelegerea modulelor de administrare a sistemului - Asimilarea arhitecturii functionale si tehnice a	5	5	1

tic legislativ	sistemului; - Prezentarea componentei de dezvoltare continut digital; - Standarde de dezvoltare folosite la construirea sistemului; - Activitati specifice administrarii bazelor de date; - Dezvoltarea unei strategii eficiente de backup si recuperare.			

Serviciile de instruire vor include in mod obligatoriu urmatoarele livrabile:

- Manual de utilizare sistem
- Manual de administrare sistem

3.6. Servicii de garantie si suport tehnic

Pentru aplicatia furnizata se vor oferi servicii de garantie si suport tehnic de minim 12 luni (1 an) de garantie.

Pentru Baza de date legislativa se vor oferi, cu titlu gratuit, servicii de actualizare continut legislativ pe o perioada de 36 de luni (3 ani) ulterior acceptanței şi punerii în producție a aplicației legislative care permite interogarea bazei de date legislative, in conformitate cu cerintele precizate la punctul 3.1 din prezentul caiet de sarcini.

Pentru echipamentele hardware furnizate se vor oferi servicii de garantie pe o perioada de 36 de luni (3 ani).

Ofertantii vor asigura asistenta tehnica on-line sau on-site pentru rezolvarea defectelor de fabricatie ale produselor hardware.
De asemenea prin serviciul de suport se va oferi asistenta tehnica profesionala legata de instalarea si operarea licentelor software.
Ofertantii vor asigura personal disponibil pentru inregistrarea si rezolvarea problemelor aparute.

4. Organizare si metodologie

Oferta va detalia graficul propus al tuturor serviciilor aferente implementarii sistemului.

Ofertantul va propune metodologia de management al intregului proiect:

- Metodologia de implementare a proiectului
- Metodologia de actualizare a continutului
- Metodologia de implementare a programului de formare propus

Ofertantul trebuie sa descrie mecanismele care vor fi folosite pentru a asigura calitatea rezultatelor proiectului. Scopul controlului calitatii este sa asigure ca in cadrul proiectului sunt luate masurile necesare si ca toate mecanismele sunt folosite pentru a asigura calitatea proiectului pe parcursul implementarii lui, gestionand preventiv riscurile si problemele, si verificand rezultatele.

In cazul in care Ofertantul va subcontracta anumite faze sau livrabile ale proiectului, acesta trebuie sa prezinte subcontractorii respectivi si activitatile alocate acestora.

4.1.1.Durata proiectului si planul de realizare a proiectului

Implementarea proiectului trebuie finalizata până cu cel mult 10 zile anterior datei de expirare a contractului de finanțare încheiat cu AM PODCA, respectiv 01.10.2014.

Ofertantul va prezenta un plan detaliat de realizare a activitatilor pentru toate componentele sistemului, urmand ca acest plan sa fie aprobat in faza de analiza a sistemului.

*4.1.2.*Facilitati oferite de catre Autoritatea Contractanta

Autoritatea Contractanta va furniza ofertantului desemnat castigator toate informatiile si/sau documentele considerate necesare pentru buna executie a contractului, care vor putea fi oferite.

5. Cerinte privind personalul

Ofertantul trebuie sa demonstreze ca are la dispozitie personalul corespunzator pentru natura si dimensiunile acestui proiect, conform cerințelor documentației de atribuire.

Coordonator de proiect – minim 1 expert

Responsabilitati in cadrul proiectului:

- Coordoneaza echipa de experti cheie si experti non-cheie
- Gestioneaza din partea furnizorului aspectele legate de managementul proiectului (activitati de organizare a proiectului, planificare, executie, monitorizare, control si inchidere a proiectului)
- Mentinerea relatiei cu Beneficiarul ca punct principal de contact
- Urmarirea respectarii tuturor termenelor limita
- Rezolvarea diferitelor situatii in scopul evitarii situatiilor de criza
- Valideaza si furnizeaza catre Beneficiar livrabilele din cadrul proiectului
- Asigura implementarea metodologiei proiectului propuse prin oferta

Expert juridic senior – 1 expert

- Coordoneaza activitatile de actualizare continut legislativ
- Verificare baze de date legislative si asigurarea confomritatii acesteia
- Participa in etapa de analiza cu privire la aplicatia dezvoltata.

Expert juridic - 1 expert

Responsabilitati in cadrul proiectului:

- Verifica baze de date legislativa si asigura confomritatea acesteia
- Coordoneaza activitatile de actualizare continut legislativ
- Participa in etapa de analiza cu privire la aplicatia dezvoltata.

Arhitect de Solutie – minim 1 expert

Responsabilitati in cadrul proiectului:

- Participa la realizarea proiectarii sistemului
- Decide care este subsetul de specificatii adresat de fiecare produs din lista propusa de Furnizor
- Asigura conformitatea solutiei tehnice in vederea implementarii setului complet de specificatii ale proiectului
- Coordoneaza si supervizeaza dezvoltarea solutiei tehnice
- Participa la designul si proiectarea sistemului informatic legislativ.
- Identifica riscurile si problemele tehnice si a solutiilor de rezolvare
- Are rol in proiectarea sistemului si supervizarea implementarii, oferind expertiza tehnica.

Expert baze de date – minim 1 expert

Responsabilitati in cadrul proiectului:

- Proiecteaza, dezvolta si configureaza bazele de date in cadrul proiectului
- Optimizeaza functionarea bazelor de date in scopul maximizarii performantelor sistemelor
- Participa la designul bazei de date care va sustine continutul legislativ.
- Participa la faza de testare
- Asigura transferul de cunostinte catre personalul Beneficiarului

Specialist retelistica – minim 1 expert

Responsabilitati in cadrul proiectului:

- Instaleaza si configureaza echipamentele de retea in cadrul proiectului
- Asigura transferul de cunostinte catre personalul Beneficiarului

Specialist infrastructura servere lamelare – minim 1 expert

Responsabilitati in cadrul proiectului:

- Instaleaza si configureaza echipamentele server furnizate in cadrul proiectului
- Coordoneaza instalarea si configurarea serverlor lamelare in cele doua locatii.(MC+DRC)

- Optimizeaza functionarea echipamentelor furnizate in scopul maximizarii performantelor sistemelor
- Participa la faza de testare
- Colaboreaza cu expertul de stocare & backup
- Colaboreaza cu expertul de infrastructura stocare & backup pentru realizarea infrastructurii
- Asigura transferul de cunostinte catre personalul Beneficiarului

Specialist infrastructura stocare si recuperare – minim 1 expert

Responsabilitati in cadrul proiectului:

- Instaleaza si configureaza echipamentele de stocare furnizate in cadrul proiectului
- Configureaza solutia de salvare si recuperare date
- Realizeaza proceduri de salvare si restaurare in caz de dezastru
- Colaboreaza cu expertul pe infrastructura IT
- Asigura transferul de cunostinte catre personalul Beneficiarului

Specialist sisteme de operare si virtualizare – minim 1 expert

Responsabilitati in cadrul proiectului:

- Instaleaza si configureaza sistemele de operare si realizeaza configuratia virtualizata din cadrul proiectului
- Realizeaza configuratiile de inalta disponibilitate acolo unde se specifica in caietul de sarcini
- Asigura transferul de cunostinte catre personalul Beneficiarului

Dezvoltator software – minim 1 expert

Responsabilitati in cadrul proiectului:

- Dezvoltarea aplicatiei software care va interoga baza de date legislativa
- Testare unitara (interna)
- Suport acordat utilizatorilor cheie pentru testarea functionala
- Rezolvare disfunctionalitati (bug-uri)

Instructor – minim 1 expert

Responsabilitati in cadrul proiectului:

- Elaboreaza planul de instruire,
- Elaboreaza materialele de instruire,
- Organizeaza si furnizareza instruirea personalului
- Elaboreaza manualele de utilizare.

Analist de business – minim 1 expert

Responsabilitati in cadrul proiectului:

- Coordoneaza analiza şi evaluarea situației existente

- Raspunde de elaborarea documentului de analiză şi a specificațiilor funcționale ale sistemului informatic

Ofertantul va adopta toate masurile necesare pentru a asigura in mod continuu personalului salariat ori contractat echipamentele si suporturile necesare pentru indeplinirea in mod eficient a sarcinilor acestuia.
Ofertantul va prezenta o declaratie pe proprie raspundere din care sa rezulte ca la elaborarea ofertei a tinut cont de obligatiile referitoare la conditiile de munca si protectia muncii, in conformitate cu normele si reglementarile legale in vigoare.

6. Cerinte minime obligatorii sesiune demonstrativa

Ofertantii trebuie sa realizeze o demonstratie functionala a sistemului informatic, pe care o vor propune ca solutie in cadrul unei sesiuni speciale la sediul autoritatii contractante.
Ofertantul va realiza sesiunea demonstrativa utilizand echipamentul propriu.
Se solicita ca in cadrul sesiunii demonstrative sa fie prezentate cel putin urmatoarele functionalitati:

Nr. Crt.	Cerinta verificata	Modul de verificare
1.	Cautare in titlu	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de cuvinte/expresii care vor fi subiectul cautarii in titlu Pas 2) Se va realiza in aplicatie cate o cautare pentru fiecare cuvant/expresie Criteriu validare cu succes a cerintei: Rezultatul cautarilor trebuie sa intoarca documente relevante cu privire la cuvintele/expresiile subiect al cautarii
2.	Cautare in text	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de cuvinte/expresii care vor fi subiectul cautarii in text Pas 2) Se va realiza in aplicatie cate o cautare pentru fiecare cuvant/expresie Criteriu validare cu succes a cerintei: Rezultatul cautarilor trebuie sa intoarca documente relevante cu privire la cuvintele/expresiile subiect al cautarii
3.	Utilizarea diacriticelor in textele legislative	Pas 1) Se va evidentia in aplicatie numarul total de documente. Pas 2) Se va realiza in aplicatie o cautare in text dupa cuvantul „și” Pas 3) Se noteaza numarul de rezultate intoarse de cautare Criteriu validare cu succes a cerintei: Numarul de documente trebuie sa reprezinte 95% din numarul total de documente
4.	Lipsa de erori in text, altele decat cele ale emitentului oficial	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de cuvinte/expresii, care au probabilitate mare de a fi obiect al greselilor de ortografie Pas 2) Se vor efectua cautari in text pentru fiecare din cuvintele selectate Pas 3) in cazul in care vor exista rezultate la cautare, acestea se vor izola si se va evidentia faptul ca erorile provin din actul original al emitentului oficial. Criteriu validare cu succes a cerintei: Documentele cu erori trebuie sa provina din actele originale.
5.	Vizualizarea corecta a tabelelor in documentele legislative	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de documente legislative ulterioare anului 1989 care contin tabele in text

		Pas 2) Pentru fiecare document legislativ, ofertantul va prezenta textul Pas 3) Se vor consemna acele documente si tabele care contin defecte in formatare. Se considera defect in formatare tabel urmatoarele situatii: • Tabelul iese din formatul textului documentului • Tabelul prezinta elemente discordante de aranjare a coloanelor : ○ coloane fara cap de tabel ○ coloane suprapuse • Tabelul prezinta elemente discordante de formatare a celulelor: ○ celule care depasesc coloana din care fac parte ○ textul din celula depaseste capacitatea celulei Criteriu de validare cu succes: Documentele din lista propusa de autoritatea contractanta nu prezinta probleme de formatare la nivel de tabele
6.	Existenta cuprins pentru documente similare documentelor comunitare si posibilitate de vizualizare din aplicatie doar a cuprinsului	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de documente legislative ulterioare anului 1989. Pas 2) Pentru fiecare document legislativ, ofertantul va prezenta forma cuprins Criteriu validare cu succes a cerintei: Toata documentele trebuie sa prezinte cuprins.
7.	Posibilitatea de a vizualiza doar cuprinsul actului	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de documente legislative ulterioare anului 1989. Pas 2) Pentru fiecare document legislativ, ofertantul va prezenta in interfata modalitatea de a vizualiza doar cuprinsul actului Criteriu validare cu succes a cerintei: Toate documentele trebuie sa prezinte cuprins si posibilitate de vizualizare in aplicatie doar a cuprinsului.
8.	Existenta in documente a sectiunilor si posibilitatea de a vizualiza doar o anumita sectiune	Pas 1) Autoritatea contractanta va prezenta la inceputul sesiunii demonstrative o lista de documente legislative ulterioare anului 1989. Pas 2) Pentru fiecare document legislativ, ofertantul va prezenta forma cuprinsul si vizualizarea unei sectiuni pornind de la cuprins Criteriu validare cu succes a cerintei: Toata documentele trebuie sa prezinte cuprins si posibilitatea de navigare din cuprins catre o sectiune.
9	Existenta a minim 800 de	Pas1) Se vor realiza in aplicatie cautari dupa

	documente legislative publicate anterior anului 1989	data publicarii cu ani anteriori anului 1989 Pas 2) Se va insuma numarul documentelor rezultate la cautare Criteriu validare cu succes a cerintei: Numarul de documente trebuie sa depaseasca 800.

Mentiune:
Pentru toate aceste cerinte, ofertantul va depune o declaratie pe propria raspundere, care va fi verificata de comisie in perioada probei DEMO si care va face referire la:
- numar acte fara diacritice
- numar acte cu posibile erori in text si cauza aparitiei lor
- numar acte care contin tabele care pot ridica probleme la vizualizare
- timpul necesar real pentru remedierea situatiilor mentionate si atingerea obiectivelor stabilite.

7. Identitate vizuală, informare şi publicitate

Furnizorul trebuie să ia toate masurile necesare asigurării vizibilității finanțării nerambursabile în cadrul PODCA, în conformitate cu indicațiile tehnice menționate in Manualul de identitate vizuală PODCA (disponibil pe website-ul http://www.fonduriadministratie.ro).

În acest sens, Furnizorul, fără a se limita la acestea, va:

- eticheta cu elemente obligatorii de identitate vizuală (etichete autocolante care vor fi aplicate în locuri vizibile) mijloacele fixe achiziționate în cadrul proiectului (a se vedea instrucțiunile din manual);
- include însemnele de vizibilitate necesare, conform Manualului de identitate vizuală PODCA, pe site-ul(urile)/aplicațiile/materialele rezultat(e) din proiect;
- include pe materialele-suport pentru activitățile de training, inclusiv pe certificatele de orice tip, a elementelor obligatorii de identitate vizuală, precum şi a mesajelor speciale/logo-uri/sloganuri care să atragă atenția asupra importanței promovării dezvoltării durabile şi a asigurării egalității de şanse.