Caiet de Sarcini

Extindere SEAP prin trecerea la un sistem dinamic si oferirea facilitatii de interoperabilitate pentru utilizatorii sistemului

CUPRINS

1 Obiectivele proiectului

Obiectivul general al proiectului este să furnizeze servicii electronice instituțiilor din administrația publică prin modernizarea sistemului electronic de achiziții publice, crearea unor facilități în cadrul acestuia pentru asigurarea interoperabilității între sistemul de eProcurement cu întregul mediu de afaceri din România si eficientizarea activitaților interne ale CNMSI privind administrarea sitemului electronic de achiziiti publice.

Instituțiile care au anumite atribuții specifice în domeniul verificării şi controlului achizițiilor publice şi a fondurilor structurale vor beneficia de un sistem care va ajuta la o coordonare inter-instituțională a activității, iar pe de altă parte vor putea fi stabilite clar responsabilitățile la nivelul fiecărei instituții.

Proiectul va implementa un mediu virtual care va fi disponibil 24 de ore din 24, fiecare utilizator putând beneficia de serviciile expuse pe Internet atunci când consideră că este mai convenabil pentru el. Astfel sistemul se va orienta către necesitățile utilizatorului şi nu a furnizorului de servicii.

Proiectul va asigura cel mai înalt nivel de securitate al utilizatorilor prin folosirea certificatelor digitale la autentificarea în mediul virtual, criptarea comunicației şi semnarea documentelor din secțiunea privată a fiecărui utilizator. Totodată se va institui un mecanism de încredere pentru comunicarea inter-instituțională eficientă înregistrându-se economii de costuri operationale. Se va promova migrarea către un mod de lucru alternativ, mult mai eficient, ecologic (hârtiile vor fi eliminate) şi rapid prin intermediul Internetului.

Obiectivele specifice ale proiectului sunt :

1. Eficientizarea fluxurilor de de lucru prin implemetarea unui platforme de management documente si fluxuri de lucru.
2. Extinderea serviciilor oferite de catre sistemul electonic de achizitii publice.

Îndeplinirea acestor obiective se va putea urmări prin realizarea următoarelor rezultate:

1. Implementarea unei infrastructuri de magement a documentelor si fluxurilor de lucru
2. Extinderea servicilor oferite pe sistemul SEAP
3. Instruirea utilizatorilor din cadrul CNMSI pentru utilizarea şi mentenanța sistemului.

Implementarea proiectului va asigura implementarea principiilor proiectelor e-guvernare: accesibilitate, eficiență, eficacitate, democrație, inovativ şi neutru tehnologic,colaborativ, sigur şi scalabil. Acesta va asigura livrarea serviciilor electronice către cetățeni şi mediul de afaceri şi de asemenea va ajuta la integrarea departamentelor din primărie pentru finalizarea serviciilor electronice.

2 Cerinte privind solutia tehnica

2.1 Cerinte generale

Arhitectura sistemului informatic trebuie să asigure:

- Accesul facil al utilizatorilor la informatiile si operatiile ce le sunt puse la dispozitie
- Viteză mare de acces la informații şi posibilități avansate de regăsire a informației pentru maxim de claritate si relevanta
- Securitatea informațiilor şi a accesului la informații pe bază de drepturi şi parole
- Informatizarea sistemelor informaționale decizionale şi a proceselor existente;
- Implementarea de modele, algoritmi şi metode statistice, pentru alocarea optimă a resurselor
- Asigurarea unui management modern prin perfecționarea continuă a tehnicilor manageriale, având ca suport sistemul informațional şi informatic al instituției
- Transformarea software-ului dintr-un element de cost într-o achiziție strategică
- Eficientizarea activității şi utilizarea performantă a infrastructurii hardware

Acțiunile de modernizare şi restructurare informatică vizând arhitectura tehnică şi de aplicații a sistemului informatic propus trebuie să se încadreze în obiectivele specifice, şi să sprijine cerințele principale privind:

- posibilități de interfațare cu alte sisteme
- flexibilitate pentru adaptarea dinamică la cerințele care pot să apară
- asigurarea fiabilității şi a siguranței în exploatare
- optimizarea resurselor informatice existente
- securitatea datelor printr-un sistem de limitări ale accesului (bazat pe autorizări şi parole)
- să aibă încorporată o funcție de arhivare/dezarhivare a datelor
- să fie un sistem parametrizabil şi configurabil după cerințele specifice ale utilizatorului
- reducerea ciclului de răspuns la solicitări cu ajutorul informațiilor obținute în timp real
- reducerea costurilor cu imprimate, formulare, etc. aferente circuitului informațional
- comunicarea electronică cu alte institutii

Sistemul informatic va trebui să răspundă urmatarelor cerinte:

- **Flexibilitatea**, exemplificată prin capacitatea aplicației de a lucra cu reguli de tranzacționare stabilite sau modificabile de către utilizator
- **Modularitatea,** care implică dezvoltarea aplicației în jurul unui nucleu căruia i se pot adăuga module şi proceduri noi pentru un upgrade uşor, având o arhitectură deschisă care sa permită integrarea cu alte aplicații sau dezvoltarea ulterioară de noi funcții şi integrarea completă a acestora
- **Interfața modernă, intuitiva şi personalizabilă,** având sectiuni configurabile şi asigurând adaptarea la necesități de design practic, fiecare utilizator putându-şi particulariza aplicația pentru genul de muncă pe care îl efectuează
- **Modalitatea de căutare sa fie naturală, în timp real, senzitivă** şi să se facă după criterii de căutare definite de utilizator
- **Separarea logica a operațiilor între serverul de gestiune a bazei de date şi aplicația client,** prin realizarea operațiilor de calcul in cadrul aplicației de client şi folosirea serverului de baze de date pentru tranzacționare şi relaționare. În acest mod se separa logic operațiile efectuate între serverul de baze de date şi aplicația client.
- **Sa aibă nivel ridicat de securitate a datelor şi tranzacțiilor,** utilizatorii să fie definiți ca aparținând unui grup, iar drepturile să se dea fie pe grup, fie pe utilizator explicit, existând două nivele de protecție a informației: al bazei de date şi mecanism intern de protecție;

2.2 Prevederi de securitate

Sistemul informatic trebuie protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le înmagazinează.

Sistemul trebuie să permită următoarele facilități:

- Controlul complet al accesului utilizatorilor la aplicații şi la fişierele de date
- Ierarhizarea în clase a utilizatorilor finali, conform unei politici de drepturi de acces adaptate şi coerente

- Gestionarea utilizatorilor si a drepturilor de acces prin crearea de grupuri de acces si stabilirea drepturilor la nivel de grup sau la nivel individual. (rezultatul este dat de reuniunea drepturilor de grup cu cele individuale)
- Generarea/înregistrarea de parole şi facilități de administrare
- Împiedicarea utilizatorilor de a se conecta la sistem dacă acesta este în stare de eroare
- Închiderea automată a sesiunilor de lucru ale utilizatorilor în caz de inactivitate pe o anumită durată predeterminată de timp
- Jurnalizarea tranzacțiilor zilnice, individual pentru fiecare utilizator cu drept de acces la modificarea înregistrărilor
- Blocarea accesului direct la baza de date. Toate operațiile se vor face prin conectare la baza de date folosind serverul de aplicație si nu prin utilizatori cu drepturi de acces direct pe baza autentificați sau nu de controlerul de domeniu sau de baza de date
- Asigurarea securității tuturor interfețelor sistemului informatic, împiedicând accesul utilizatorilor neautorizați la sistem
- Întărirea condițiilor de securitate şi a restricțiilor de acces pentru aplicațiile care implică transferuri financiare via interfețe externe
- Raportarea pe baze periodice a detaliilor privitoare la accesul în sistem al utilizatorilor
- Autentificare utilizatorilor in aplicație trebuie sa fie permisa de la orice punct de lucru din cadrul instituției iar accesul sa fie partajat la nivel de utilizator al aplicație si nu al sistemului pana la nivel de funcție sau de rapoartele emise
- Securitatea accesului la baza de date

Prevederile de securitate extinse si functionalitatile ce decurg din acestea sunt prezentate in sectiunea dedicata sistemului de securitate. Ele completeaza cerintele deja mentionate si le extind pentru a crea o arhitectura integrata securizata printr-o infrastructura moderna, bazata pe chei publice (conventional denumita solutie de securizare pe baza de certificate digitale).

3 Descrierea tehnica a proiectului

3.1 Cerințele funcționale ale sistemului

In cadrul acestui capitol sunt descrise cerintele functionale ale sistemului, impartite pe principalele servicii/module oferite:

Serviciu/Modul	Descriere

Serviciul de management al planurile/programelor anuale de achiziții publice	Serviciul trebuie sa ofere autorităților contractante posibilitatea publicării planurilor/programelor anuale de achiziții publice elaborate de acestea pe parcursul unui an bugetar.
Sistemul de achizitie dinamic	Acest serviciu urmareste extinderea proceduriilor de achizitie disponibile in acest moment in SEAP. Sistemul de achizitii dinamic este o procedura de achizitie care se defasoara in intregime electronic, este limitata in timp si deschisa pe intreaga sa durata oricarui operator economic care indeplineste criteriile de calificare si evaluare si care a prezentat o oferta orientativa conforma cu cerintele caietului de sarcini.
Serviciul dosarul companiei	Acest serviciu va permite oricarei entitati autorizate, implicate in fluxul achizitiilor publice (autoritati contractante, operatori economici, sisteme informatice de eProcurement, terte parti implicate) obtinerea unei colectii de documente continand atestari, certificari, declaratii pe proprie raspundere, etc. ale unui operator economic participant in acest flux.
Dosarul electronic al achizitiei	Acest serviciu reprezinta un instrument de gestionare si control a tuturor informatiilor generate pe parcursul fluxului de derulare a unei proceduri de achizitie publica. Dosarul electronic al achizitiei va putea fi folosit de autoritatile contractante ca un mijloc de evidenta a procedurilor de achizitii.
Servicul de marcare temporala pentru documente	Acest serviciu va realizeza marcarea temporală a tuturor documentelor vehiculate în cadrul sistemului de achizitii publice. Este serviciul

	suport pentru alte servicii/module din cadrul SEAP.
Serviciu de management documente si workflow securizat	Acest serviciu joaca rol de suport pentru alte servicii/module din cadrul SEAP si este un instrument de management al documentelor si workflow securizat, ce asigura circulatia documentelor conform fluxurilor definite.

Pentru fiecare dintre aceste servicii exista un echivalent software (module aplicative si servicii) proiectat sa ofere functionalitatile descrise. Aceste componente software ofera acces atat operatorilor normali(autoritati contractante si ofertanti) , cat si operatorilor din cadrul autoritatii publice(CNMSI,ANRMAP,UCVAP, etc) pentru indeplinirea fluxurilor de lucru specifice.

3.1.1 Serviciul de management al planurile/programelor anuale de achiziții publice

Serviciul trebuie sa ofere autorităților contractante posibilitatea publicării planurilor/programelor anuale de achiziții publice elaborate de acestea pe parcursul unui an bugetar. Aceast serviciu are ca scop introducerea unui instrument de management instituțional al achizițiilor publice şi asigurarea transparenței asupra modului de utilizare eficientă a fondurilor publice.

Serviciul trebuie sa permita realizarea planului anual de achizitii publice prin intermediul portalului SEAP prin introducerea de documente initiale si documente corectoare cat si importul planului realizat in propriile sisteme informatice. Programul anual al achizitiilor publice este documentul care contine: contractele de achizitie publica si acordurile cadru ce se intentioneaza a fi atribuite sau incheiate pe parcursul unui an bugetar, precum si, daca este cazul, lansarea unui sistem dinamic de achizitie.

Inintierea procedurile de achizitie implementate in SEAP trebuie sa fie conditionate de existenta pozitiilor bugetare aferente in planul de achizitie anual. Pentru cazurile de exceptie stipulate in lege : situații de forță majoră sau caz fortuit trebuie prevazut un flux special prin care sa fie permisa initierea procedurii pe baza unei note justificative intocmita de autoritatea contractanta si avand aprobarea conducatorului autoritatii contractante.

Sistemul trebui sa permita introducerea introducerea unui plan de achizitii publice pentru fiecare an bugetar. Autoritatiile contractante trebuie sa poata introduce acest plan incepand cu ultimul trimestru al anului precedent.

In ultimul trimestru, cu o perioada detimp configurabila inainte de sfarsitul anului, sistemul trebuie sa verifice care sunt autoritatiile contracatnte care nu au intocmit planul pentru anul urmator si acestea sa fie notificate.

Programul anual trebuie sa cuprinda toate contractele care urmeaza sa fie atribuite in cursul anului. Pentru fiecare contract trebui sa se poata introduce minim urmatoarele informatii:

- obiectul contractului/acordului-cadru
- cod CPV – conform nomenclatorului CPV
- valoarea estimata fara TVA (lei si euro)
- procedura care urmeaza sa fie aplicata – una din urmatoarele optiuni:
    - licitatie deschisa
    - licitattie restransa
    - dialogul competitiv
    - negocierea
    - negociere fara publicarea prealabila a unui anunt de participare
    - cererea de oferte
    - acordul-cadru
    - aistem de achiziti dinamic
    - Alte proceduri stipulate in lege
- data estimata pentru inceperea procedurii
- data estimata pentru finalizarea procedurii
- responsabilul achizitie publice ce urmeaza a fi facuta

Procesul de intocmire al planului de achizitii publice trebuie sa respecte urmatorul flux de activitati(subactivitatiile pot fi realizate fie in SEAP fie in sistemul informatic al autoritatii contractante):

1. Realizarea primei forme a planului(activitate obligatorie)
    a. Intocmire de catre personalul autoritatii contractante
    b. Avizare de catre departamentul financiar contabil al autoritatii contractante

c. Aprobare de catre conducatorul autoritatii contractante

2. Definitivarea planului in urma aprobarii bugetului(activitate obligatorie)
    a. Modificarea planului conform bugetului aprobat de catre personalul autoritatii contractante
    b. Avizare de catre departamentul financiar contabil al autoritatii contractante
    c. Aprobare de catre conducatorul autoritatii contractante
3. Modificarea planului de achizitie(activitate optionala si repetitiva)
    a. Modificarea sau completarea planului de catre personalul autoritatii contractante
    b. Avizare de catre departamentul financiar contabil al autoritatii contractante
    c. Aprobare de catre conducatorul autoritatii contractante

Toate functionalitatiile care se refera la interactiunea dintre SEAP si autoritatile contractante sau UCVAP trebui sa fie expuse prin intermediul serviciilor web.

Acest serviciu trebuie sa asigure interonectarea cu urmatoarele sisteme: sistemele informatice ale autoritatiilor contractante si sistemul informatic al UCVAP.

3.1.2 Sistemul de achizitie dinamic

Procedurile de achizitie trebuie extinse prim implementarea unei noi proceduri: sitemul de achizitie dinamic.

Autoritatile contractante trebuie sa poata initia un Sistem de Achizitii Dinamic pentru achizitia unor produse de uz curent, ale caror caracteristici general disponibile pe piață satisfac nevoile autorității contractante.

Initierea SAD trebuie sa se face prin publicarea anuntului de participare general; la publicarea acestuia sistemul trebuie sa publice automat o procedura electronica SAD, folosind informatii preluate din anuntul de participare. Incepand din momentul publicarii SAD si pe toata perioada derularii acestuia (stabilita de autoritatea contractanta in anuntul de participare), care nu poate depasi 4 ani decat in cazuri exceptionale, temeinic justificate, orice ofertant inscris in SEAP are acces la documentatia de atribuire in format electronic, atasata la anuntul de participare, si isi poate o depune oferta orientativa in scopul admiterii in sistemul dinamic. Autoritatea contractanta are obligatia evaluarii unei oferte orientative in termen de maxim 15 zile de la transmiterea acesteia. Ofertantii admisi in SAD au dreptul de a-si depune oferta ferma la orice procedura de atribuire a unui contract specific, lansata in cadrul SAD.

In vederea atribuirii unui contract in cadrul SAD, autoritatea contractanta trebuie sa publice un anunt de participare simplificat, prin care face cunoscut tuturor ofertantilor interesati termenii achizitiei specifice. La publicarea unui anunt de participare simplificat, sistemul trebuie sa publice automat o procedura de atribuire in cadrul SAD, folosind informatii din anuntul de participare general si cel simplificat. In aceasta faza depunerea ofertelor orientative trebuie sa fie posibila doar pana la data limita specificata de autoritatea contractanta in anuntul de participare simplificat. Desfasurarea fazei finale de depunere a ofertelor ferme este posibila doar dupa ce autoritatea contractanta a evaluat toate ofertele orientative primite.

In faza de depunere a ofertelor ferme ofertarea trebuie realizata dinamic, ofertantii avand posibilitatea imbunatatirii succesive a ofertei, in cadrul unei etape de licitatie electronica. La publicarea licitatiei electronice sistemul trebuie sa trimita automat invitatii de participare tuturor ofertantilor admisi in SAD, in care sunt precizate datele de desfasurare ale fazelor licitatiei electronice; in vederea depunerii ofertei ferme, un ofertant admis in SAD trebuie sa se inscrie la licitatia electronica.

Acest serviciu trebuie sa asigure interonectarea cu urmatoarele sisteme: sistemul informatic al UCVAP, sistemul informatic al ANRMAP si sistemul informatic al CNSC.

3.1.3 Serviciul dosarul companiei

Dosarul virtual al companiei trebuie sa permita oricarei entitati autorizate, implicate in fluxul achizitiilor publice (autoritati contractante, operatori economici, sisteme informatice de eProcurement, terte parti implicate) obtinerea unei colectii de documente continand atestari, certificari, declaratii pe proprie raspundere, etc. ale unui operator economic participant in acest flux. Sistemul va permite obtinerea de la autoritatile emitente a documentelor de atesare si certificare, dar si furnizarea de catre operatorii economici de declaratii pe propria raspundere, documente de calificare, etc. Autoritatile contractante vor avea posibilitatea de a solicita si de a obtine un set de documente specific unei anumite proceduri de achizitie publica.

Aria de cuprindere a sistemului trebuie sa fie la nivel national, si trebuie sa permiteainterconectarea cu sisteme similare ale altor tari. In acest scop realizarea dosarului virtual al companiei trebuie sa se realizeze in acord cu prevederile legislative europene si

eforturile de standardizare la nivel european. Setului de specificatii functionale detaliate pentru dosarul virtual al companiei trebuie realizat in urma unei analize a rezultatelor grupului de lucru PEPPOL si a prevederilor Directivei Europene a Serviciilor.

Acest servicu trebuie sa asigure interonectarea cu urmatoarele sisteme: sistemele informatice al Autoritatilor emitente de documente si sisteme informatice de tip eProcurement din UE.

3.1.4 Dosarul electronic al achizitiei

Acest serviciu reprezinta un instrument de gestionare si control a tuturor informatiilor generate pe parcursul fluxului de derulare a unei proceduri de achizitie publica. Dosarul electronic al achizitiei va putea fi folosit de autoritatile contractante ca un mijloc de evidenta a procedurilor de achizitii, si informatiile cuprinse in dosarele de achizitie vor putea fi puse la dispozitia institutiilor abilitate in domeniul monitorizarii si controlului achizitiilor publice, in vederea facilitarii activitatilor specifice ale acestora.

Dosarul electronic al achizitiei se va deschide automat la publicarea in SEAP a unui anunt de participare sau a unei invitatii de participare si se va actualiza pe masura desfasurarii procesului de achizitie, atat cu documente atasate anuntului din SEAP (documentatie de atribuite, documente de clarificare, documente atasate la intrebarile postate de ofertanti, documente atasate raspunsurilor furnizate de autoritatea contractanta) cat si cu documente generate automat de sistem la realizarea anumitor evenimente in sistem (de ex generarea unui document la publicarea anuntului, pe baza informatiilor cuprinse in acesta, sau generarea unui document la publicarea unei erate, cuprinzand informatiile din erata, etc.), astfel incat la orice moment in timp continutul dosarului electronic sa reflecte stadiul desfasurarii procedurii. Autoritatile contractante vor avea de asemenea posibilitatea incarcarii de alte documente, care au fost generate in afara fluxului SEAP (note justificative, procese verbale, documente constatatoare, avize consultative, etc.)

Crearea si actualizarea dosarului electronic se va realiza prin intermediul unui sistem de management si arhivare a documentelor, specific fluxului de documente in domeniul achizitiilor publice. Coreland acest mecanism cu functionalitatile de semnare electronica si marcare temporala, sistemul de management al documentelor va oferi garantia privind identitatea entitatii care a generat documentul si data la care acesta a fost creat.

Acest servicu trebuie sa asigure interonectarea cu urmatoarele sisteme: sistemul informatic al UCVAP, sistemul informatic al ANRMAP si sistemul informatic al CNSC.

3.1.5 Servicul de marcare temporala pentru documente

Serviciul va realizeza marcarea temporală a tuturor documentelor vehiculate în cadrul sistemului de achizitii publice;

Marcarea temporală va fi realizată utilizându-se un serviciu de marcare temporală public care să funcţioneze în baza prevederilor Legii 451/2004;

Serviciul de marcare temporală din SEAP va trebuie să fie configurabil şi să permită cel puţin următoarele:

- Marcarea temporală a oricărui tip de document indiferent de extensia acestuia;
- Configurarea parametrilor de conectare la un serviciu public de marcare temporală
- Să realizeze validarea mărcilor temporale emise atât în momentul realizării acestuia cât şi la o dată ulterioară ;

Acest servicu trebuie sa asigure interonectarea cu urmatoarele sisteme: sistemele informatice ale furnizorilor acreditati de servicii de certificare si autoritatea de certificare a CNMSI.

3.1.6 Serviciu de management documente si workflow securizat

Serviciul trebuie sa fie construit pe o platforma dedicata de managementul documentelor si workflow securizat, ce asigura circulatia documentelor pe trasee ierarhice stabilite conform fluxurilor definite de administratorul aplicatiei, asigurand in orice moment informatii despre locul unde se afla documentul, stadiul in care se afla, precum si timpul necesar fiecarei activitati in parte. Solutia trebuie sa ofere un mecanism foarte flexibil de configurare a fluxurilor de documente, punand la dispozitia administratorului si a utilizatorilor o interfata vizuala prin care pot modifica fluxul de documente, redefini actiunile care trebuiesc indeplinite asupra unui document si conditiile care trebuiesc indeplinite ca un document sa fie acceptat/validat.

Sistemul de management al documentelor si fluxurilor de lucru digitale trebuie sa asigure urmatoarele functionalitati:

a) Managementul ciclului de viata al documentelor electronice

b) Managementul fluxurilor electronice de documente
c) Arhivarea electronica a documentelor
d) Raportare
e) Administrare facila

Sistemul de management al documentelor si fluxurilor de lucru trebuie sa asigure conformitatea cu standarde internationale recunoscute in domeniu.

Sistemul trebuie sa permita lucrul cu documente clasificate, conform legislatiei in vigoare (Legea 182 din 2002).

Sistemul de management al documentelor trebuie ruleze intr-o singura instanta centrala dar sa permita urmatoarele:

a) Definirea de spatii de lucru izolate, corespunzatoare nivelului unei structuri, in care sa se poate face gestiunea independenta a structurii organizatorice, fluxurilor de lucru, documentelor, utilizatorilor si rolurilor asociate.
b) Posibilitatea ca spatiile de lucru enuntate anterior sa poata comunica intre ele in mod nativ, prin schimbul de documente prin fluxuri electronice comune de lucru.

Acest serviciu trebuie sa se integreaze cu urmatoarele sisteme:

- SEAP: sistemul de management al fluxurilor de lucru existent in SEAP. Serviciul trebuie sa asigure configurarea/remodelarea fluxurilor de lucru existente si preluarea automata de documente intre fluxurile de lucru existente si noile fluxuri
- ANRMAP - sistemul informatic al ANRMAP
- UCVAP - sitemul informatic al UCVAP
- CNSC - sistemul informatic al CNSC.

3.1.6.1 Caracteristici avansate de securitate

Dat fiind caracterul senzitiv al anumitor informatii vehiculate in sistemul de management de documente si fluxuri electronice, sistemul trebuie sa asigure intrisec un set de functionalitati avansate de securizare a lucrului cu acest tip de informatii. Astfel, se doreste ca sistemul sa fie capabil sa ofere

- Autentificare pe baza de elemente avansate de securitate (certificat digital, echipamente de tip token)

- Utilizarea semnaturii digitale la adaugarea si modificarea documentelor, precum si la luarea deciziilor asupra documentelor electronice din sistem, in scopul garantarii integritatii si non-repudierii informatiilor
- Verificarea semnaturii de catre sistem, pe baza recipiselor si a datelor mentinute in sistem
- Controlul strict al accesului la documente, indiferent de starea acestora. Se doreste folosirea unui set cat mai larg de criterii de acordare a accesului (in functie de tipul documentelor, tipul de operatie, starea documentului, etc)
- Monitorizarea stricta a accesului la documente si jurnalizarea operatiilor
- Asigura conformitate cu standardele PKCS #1, PKCS #7, PKCS #11
- Operatiunile implicand semnarea si criptarea se vor realiza utilizand certificate digitale emise de PKI ale furnizorilor acreditati.
- Posibilitatea criptarii simetrice cu urmatorii algoritmi: DES, 3DES, RC4, RC6
- Certificatele digitale ale utilizatorilor vor putea fi stocate pe dispozitive de token USB conforme cu standardul FIPS 140-2 level 2
- Operatiunile criptografice care implica utilizarea cheii private se vor desfasura numai pe dispozitive de tip token USB conforme cu standardul FIPS 140-2 level 2
- Asigurarea legaturii cu serviciul de marcare temporala pentru documente conform RFC 3161
- Folosirea unor certificate digitale separate pentru operatiunile de criptare si semnare
- Autentificarea utilizatorilor in sistem se va realiza pe baza de nume si parola, precum si de certificate emise de PKI CNMSI, cu garantarea validitatii starii certificatelor digitale la acel moment de timp, accesand serviciul de validare OCSP (RFC 2560)
- Compatibilitate cu standardul LDAP v3
- Comunicatia intre partea client a sub-sistemului si partea server trebuie sa fie garantata din punct de vedere al confidentialitatii in orice moment de timp. Pentru

comunicatia online este obligatoriu sa se asigure conexiune de tip HTTPS (SSL 128 biti) cu autentificare reciproca

- La fiecare operatiune senzitiva, de aprobare sau avizare pe fluxurile de documente sistemul va solicita utilizatorului semnarea formularului de date.

3.1.6.2 Managementul ciclului de viata al documentelor

Pentru gestionarea ciclului de viata al documentelor electronice va trebui sa ofere urmatoarele functionalitati:

- Adaugarea de documente in sistem in orice format electronic impreuna cu un set de metadate standard (nume document, tip, data creare, cuvinte cheie, etc)
- Definirea si adaugarea de formulare electronice prin adaugarea de metadate specifice in mod dinamic, prin definirea acestora din interfata grafica. Aceste metadate trebuie sa permita:
    - validari automate
    - reguli de validare
    - valori implicite si liste de valori
    - multiplicitate 1 sau multipla
    - organizarea metadatelor pe sectiuni
    - acordarea drepturilor de acces per metadata sau sectiuni de metadate
- Adaugarea de documente in aplicatie fie document cu document, fie adaugare multipla de documente. Documentele vor putea fi adaugate fie in spatiul privat al unui utilizator, ca si documente de lucru, fie in spatiul public (biblioteca) disponibil tuturor utilizatorilor dupa o schema de acces multi-nivel;
- Posibilitatea de a atasa unui document, la adaugare, si semnatura digitala detasata
- Clonarea categoriilor de documente indiferent de numarul metadatelor definite pe document,
- Configurarea de catre administrator a unor categorii de documente cu un numar nelimitat de metadate standard

- Exportul formularelor in format PDF

- Versionarea automata a documentelor la orice modificare, cu pastrarea si vizualizarea versiunilor anterioare

- Pentru fiecare document, trebuie sa se poata adauga adnotari de tip rich text. Unui document ii pot fi adaugate oricate comentarii atat de catre utilizatorul care a creat documentul, cat si de utilizatorii care au primit documentul pe flux, sau au fost solicitati pentru lucru colaborativ la respectivul document, etc., in general de toti utilizatorii care au drept de editare a documentului

- Pentru fiecare document, trebuie sa se poata adauga cuvinte cheie. Cuvintele cheie definesc un set de cuvinte reprezentative asociate unui document, pentru ca ulterior sa ajute la cautarea facila a documentului. Unui document i se vor putea adauga oricate cuvinte cheie din urmatoarele doua tipuri: cuvinte cheie personale, introduse fara restrictii de fiecare utilizator in parte, respectiv cuvinte cheie globale, care reprezinta o lista arborescenta de cuvinte cheie predefinite de catre un administrator, lista din care utilizatorul poate alege.

- Semnarea digitala a versiunii curente a documentelor si posibilitatea de verificare si validare a semnaturii de catre alti utilizatori. La semnare, sistemul va genera o recipisa electronica, ce va putea fi stocata in aplicatie sau pastrata in afara ei. Recipisa va putea fi folosita pentru verificarea semnaturii in cazul unor contestatii.

- Posibilitatea de a vizualiza documente in formate proprietare fara a fi necesara instalarea de aplicatii suplimentare. Astfel de formate includ: Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Project, Adobe Acrobat, fisiere imagine in formatele consacrate (jpg, gif, tif, bmp), fisiere HTML

- Integrare cu suite de aplicatii Microsoft Office (Word, Excel, Powerpoint) care sa permita salvarea directa in sistem a documentelor editate cu aceasta suita

- Posibilitatea de a organiza documentele pe categorii/taxonomii de documente in scopul regasirii facile a informatiilor prin intermediul explorarii ieharhice multi-criteriale

- Posibilitatea de a organiza documentele in dosare (grupuri de documente), cu pastrarea tuturor functionalitatilor specifice conceptului de document si la nivelul conceptului de dosar

- Posibilitatea de a copia documentele, iar noul document (copia) trebuie sa pastreze o legatura catre original

3.1.6.3 Posibilitatea de indexa automat continutul documentelor in format text cu posibilitatea de cauta documente dupa continut

- Suport pentru gruparea ad-hoc a documentelor in asociatii de mai multe documente si stabilirea de corespondente intre doua grupari de documente

- Sistemul trebuie sa fie capabil sa ofere fiecarui utilizator un spatiu privat de lucru, in care acesta sa-si pastreze si organizeze documentele. Organizarea documentelor trebuie sa se faca sub forma de directoare si subdirectoare de documente. In cadrul structurii de directoare vor putea fi efectuate urmatoarele operatii: adaugare, redenumire, stergere, clonare, mutare director, adaugare/stergere/mutare document intr-un director.

- Suport pentru integrarea cu echipamente de scanare/indexare a documentelor in format hartie, cu posibilitatea de preluare automata a documentelor in mod individual sau in sistem batch.

- Cautarea simpla (set de criterii redus) sau cautare complexa (set de criterii extins). Caracteristici ale cautarii:

    - Cautarea sa se faca atat in metadate cat si in cotinut

    - Sa se poata folosi expresii regulate

    - Sa se poata salva criteriile de cautare

    - Rezultatele sa poata fi salvate in format PDF

- Sarcinile de lucru in cadrul sistemului vor fi transmise sub forma de mesaje interne ale aplicatiei si vor fi vizualizate de fiecare utilizator in propriul inbox virtual din spatiul de lucru propriu.

3.1.6.4 Lucrul in comun pe documente

Sistemul de document management trebuie sa puna la dispozitie diferite tipuri de lucru in comun cu documentele electronice. Astfel, sunt avute in vedere urmatoarele tipuri de colaborare in elaborarea documentelor

- Colaborare formala: in acest caz, etapele prin care trece un document (draft, avizat, aprobat) sunt definite unor fluxuri electronice de lucru, conform unor proceduri de lucru prin configurarea fiecarui pas prin care un document trece, a actorilor implicati si a drepturilor asociate pe fiecare pas, precum si a conditiilor de trazitie intre pasi. La executia fluxului, fiecare utilizator va executa sarcina alocata si va trimite documentul/documentele catre pasul urmator conform regulilor de tranzitie definite (sistemul va afisa automat destinatiile posibile in functie de configurarea fluxului). Trebuie sa fie posibila configurarea fluxului astfel incat in anumiti pasi sa se impuna semnarea digitala a documentului si a deciziilor luate asupra documentului in acel pas.

- Colaborare informala: Posibilitatea de a partaja documentele:

    - direct intre utilizatori, prin publicarea unui document/set de documente catre o lista nominala de utilizatori pentru lucru colaborativ. La publicare sa se poata defini fie un mesaj de lucru comun pentru intreaga lista, fie mesaje individuale pentru fiecare utilizator. Pentru lucrul simultan pe documente trebuie implementat un mecanism de acces exclusiv la document, de tip blocare/deblocare. Odata publicat un document, utilizatorul care a publicat documentul trebuie sa poata vedea stadiul lucrului pentru fiecare utilizator si poate retrage, in orice moment, documentul de la publicare.

    - prin intermediul unei biblioteci de lucru, cu configurarea drepturilor de access. Biblioteca trebuie sa poata fi organizata pe sectiuni si subsectiuni, iar drepturile de access trebuie controlate la nivel de tip de operatie pe (sub)sectiune a bibliotecii. Documente trebuie sa poata fi vizualizate, preluate din biblioteca pentru modificare, pastrand o urma in biblioteca, respectiv sa poata fi retrase complet din biblioteca conform drepturilor alocate pentru fiecare utilizator.

3.1.6.5 Managementul fluxurilor de lucru

In cazul colaborarii formale intre utilizatori, prin intermediul fluxurilor electronice de lucru, se solicita urmatoarele functionalitati:

- Definirea metadatelor generale ale fluxurilor electronice (nume, perioada de valabilitate, durata maxima de executie, etc)
- Definire setului de activitati ce fac parte dintr-un proces si metadatelor asociate (nume, tip, durata maxima, roluri asociate, drepturi de acces si prelucrare asupra documentelor asociate respectivei activitati)
- In fiecare activitate trebuie sa se poata acorda un set de decizii (rezolutii) configurabile la nivel administrativ. Aceste decizii trebuie sa poate fi insotite de comentarii in mod text sau de comentarii vocale (prin inregistrarea de mesaje). Trebuie sa existe posibilitatea de a configura pentru fiecare activitate daca rezolutiile sunt semnate digital.
- Pe langa administrator, trebuie ca si initiatorul unui flux sa poata configura urmatorii parametrii: timpul maxim de executie al intregului proces, timpul maxim de executie al fiecarei activitati
- Definirea tranzitiilor intre activitati si a setului de conditii care trebuie indeplinit pentru executia fiecarei tranzitii. Acest set de conditii trebuie sa includa criterii precum rolurile expeditor, rolurile destinatar, tipul documentelor, rezolutii acordate, etc. De asemenea, pentru a asigura o cat mai mare flexibilitate a tranzitiilor, sistemul trebuie sa ofere o paleta larga de posibilitati de configurare pentru fiecare dintre ele. Printre configurarile posibile trebuie sa se numere:
    - posibilitatea de a executa simultan mai multe tranzitii dintr-o singura activitate catre activitati diferite si posibilatea de a uni un set de tranzitii intr-una singura
    - posibilitatea trimiterii mesajului doar utilizatorilor din acelasi grup de lucru cu expeditorul
    - posibilitatea trimiterii mesajului catre toti utilizatorii ce au rolul destinatar ales
    - posibilitatea trimiterii mesajului numai catre autorul documentului ce parcurge fluxul

- posibilitatea trimiterii mesajului numai catre expeditorul mesajului primit
- posibilitatea trimiterii mesajului catre toti destinatarii posibili
- posibilitatea crearii dependintei dintre activitatea pentru care se defineste tranzitia si o alta activitate a procesului curent
- posibilitatea trimiterii mesajului pe o anumita ierarhie, catre superior sau catre subordonat.
- posibilitatea notificarii prin e-mail a sefului direct sau a tuturor sefilor ierarhici pe o ierarhie aleasa.

- Sistemul va oferi suport pentru modificarea la runtime a fluxurilor de documente electronice, prin modificarea rolurilor implicate, durata activitatilor sau conditiile de tranzitie
- Sistemul va oferi suport pentru vizualizarea fluxurilor electronice finalizate sau a celor aflate in lucru, cu precizarea punctelor in care se gaseste un flux la un moment dat si a pasilor anterior parcursi
- Fluxul trebuie sa poata fi configurat sa faca in mod automat copii ale documentului la parasirea unui activitati din flux, documentul intrand in proprietatea celui care a efectuat acea activitate
- Un flux electronic trebuie sa poata fi configurat astfel incat la finalizarea unei instante documentul sa intre automat fie in proprietatea initiatorului fluxului, fie in biblioteca, cu alegerea sectiunii in care se va depozita documentul.
- Sistemul va oferi suport pentru monitorizarea gradului de incarcare a utilizatorilor implicati in activitatile de flux
- Suport pentru definirea fluxurilor prin intermediul interfetei grafice de tip web
- Suport pentru clonarea fluxurilor in vederea crearii de fluxuri noi pe baza celor deja definite in sistem
- Posibilitatea de a configura sistemul astfel incat sa ia decizii automate prestabilite in cazul in care termenul limita al unei activitati din cadrul unui flux a fost depasit.

3.1.6.6 Fluxuri de lucru pe terminale mobile

- Pentru utilizatori cu rol de decizie sistemul trebuie sa permita accesul la fluxurile electronice de documente de pe terminale mobile. Utilizatorii trebuie sa poata interactiona cu sarcini primite pe telefonul mobil.
- Functionalitatea trebuie sa fie disponibila pe mobil in permanenta si sa poata fi trecuta de utilizator in fundal.
- Sistemul trebuie sa permita accesul de pe terminale mobile atat la sarcinile active, cat si sarcinile finalizate. Sarcinile noi trebuie sa fie evidentiate de restul sarcinilor active. Sarcinile depasite trebuie sa fie marcate suplimentar.
- Pentru fiecare sarcina in parte sistemul trebuie sa permita:
    a. acces la informatii de detaliu despre sarcina primita: numele documentului, expeditorul, starea, nivelul de prioritate, activitatea de pe flux, data la care s-a emis sarcina si termenul de realizare;
    b. acces la documentele specifice sarcinii (documentul principal si atasamente), iar in cazul documentelor de tip formular afisarea pe terminal a campurilor si valorilor acestora;
    c. vizualizarea in ordine cronologica a rezolutiilor acordate anterior pe fluxul electronic;
    d. vizualizarea setului de rezolutii posibile de acordat si selectarea unei rezolutii pentru activitatea curenta de pe flux;
    e. redactarea unui comentariu pe flux, inainte de finalizarea sarcinii;
    f. vizualizarea destinatarilor posibili si selectiarea destinatarului/destinatarilo catre care se trimite documntul mai departe pe flux;
- In cazul finalizarii fluxului, utilizatorul trebuie sa poata selecta pe terminalul mobil in ce folder din biblioteca electronica a sistemului se salveaza documentul.

1.1. Managementul sarcinilor (in afara fluxurilor de lucru)

Sistemul trebuie sa permita transmiterea unor sarcini sau cereri de lucru unor utilizatori, in afara fluxurilor electronice de documente. Aceste sarcini sau cereri de lucru vor avea un caracter formal si se vor monitoriza ca atare. Modulul trebuie sa permita urmatoarele functionalitati:

a) Sa se poata defini de catre administrator tipuri de sarcini sau cereri de lucru;
b) O sarcina sau o cerere de lucru sa poata fi adresata de catre un utilizator altui utilizator, fara sa respecte in mod necesar linia ierarhica din organigama;
c) Posibilitatea numirii unor supervizori pentru anumite sarcini sau cereri de lucru, care sa aiba vizibilitate in orice moment asupra stadiului de realizare a sarcinilor pe care le supervizeaza

d) Posibilitatea definirii unor termene limita de executie pentru sarcinile sau cererile de lucru;
e) Posibilitatea de a realiza operatii privind sarcinile de lucru primite, emise, supervizate (vizualizare, adaugare, cautare) in functie de roluri specifice diferentiate. Sistemul trebuie sa permita monitorizarea sarcinilor primite, emise si supervizate si afisarea unor indicatori de stare si progres. Indicatorii de progres sa se evidentieze procentual si grafic. Raportul de monitorizare trebuie sa poata fi exportat intr-un fisier de tip xls. Starea asociata unei sarcini va putea avea urmatoarele valori: Deschisa, In lucru, Rezolvata, Redeschisa, Inchisa. La fiecare schimbarea a starii, sistemul va trimite mail-uri de notificare catre toti cei implicati in rezolvarea acelei sarcini.
f) Utilizatorul responsabil cu rezolvarea unei sarcini va putea acorda doar una din starile: In lucru sau Rezolvata, iar supervizorul va putea modifica starea sarcinii doar cu urmatoarele valori: Deschisa, Redeschisa, Inchisa;
g) Adaugarea de comentarii de tip text la fiecare schimbare a starii unei sarcini;
h) Cautare rapida si cautare avansata multicriteriala de sarcini;
i) Vizualizarea instoricului modificarilor efectuate asupra unei sarcini
j) Posibilitatea de a fi configurat astfel incat sa trimita automat si la intervale regulate de timp notificari pin email pentru raportarea stadiului de realizare a unei sarcini. De asemenea, sistemul trebuie sa ofere initiatorului posibilitatea de a selecta lista persoanelor care vor fi notificate.
k) Integrare cu Microsoft Outlook astfel incat sarcinile sa figureze in Calendar si in lista de task-uri, fiind accesibile astfel accesibile atat din clientul solid MS Outlook cat si de pe web (Outlook Web Acces) si de pe terminalele mobile care suporta suita MS Outlook.
l) Integrare cu echipamente mobile, astfel incat utilizatorii sa poata vizualiza de pe terminale mobile sarcinile si starea lor si sa raporteze modificari de progres sau de stare.

3.1.6.7 Arhivare

Sa permita arhivarea documentelor in conformitate cu legislatia in vigoare privind arhivarile electronice (legea nr. 135/2007). Se solicita stocarea datelor pe trei nivele: online (in baza de date), nearline (suport accesibil direct din aplicatie) si respectiv offline (pe medii interne si externe magnetice sau optice).

Sistemul trebuie sa ofere facilitati de auto-arhivare.

- Sa respecte legislatia romana in vigoare privind arhivarile.
- Sistemul trebuie sa permita definirea perioadei de pastrare pentru fiecare categorie de documente in parte.

- Sistemul trebuie sa restrictioneze posibilitatile de modificare a documentelor electronice care au fost arhivate.
- Sistemul nu trebuie sa permita mutarea in arhiva electronica a unor documente aflate pe fluxuri electronice de documente sau in colectile personale de documente ale utilizatorilor.
- Documentele electronice vor fi arhivate cu tot cu istoricul lor (versiuni anterioare).
- Sistemul trebuie sa permita definirea politicilor de arhivare pe baza unui set extins de criterii de arhivare (tip document, autor, data adaugare in sistem, grad de clasificare, etc). Aceste politici pot fi definite pentru trecere din online in nearline, respectiv din nearline in offline. Sistemul va face selectia documentelor candidate pentru arhivare electronica si trecerea lor in arhiva in baza politicilor de arhivare, definite in sistem de catre administratorul arhivei electronice.
- Sistemul trebuie sa permita un set extins de operatii asupra politicilor de arhivare (adaugare, vizualizare, modificare, activare, dezactivare, stergere).
- Politicile de arhivare trebuie sa poata fi setate sa ruleze manual, la initiativa administratorului, sau automat.
- Documentele trebuie sa fie trecute din online in nearline sau din nearline in offline doar in baza unor politici definite pentru categoria din care fac parte. Daca pentru un tip de document nu se defineste niciodata o politica de arhivare, sistemul va pastra permanent in documentele corespunzatoare acelui tip de document.
- La depunerea documentelor in arhiva electronica sistemul trebuie sa solicite semnarea digitala a documentelor de catre titularul dreptului de dispozitie asupra documentelor, pentru a garanta integritatea ulterioara a documentelor in arhiva. Semnarea se va face cu un certificat calificat.
- La depunerea documentelor in arhiva electronica sistemul sa sa asigure semnarea digitala de catre administratorul arhivei, pentru a garanta integritatea ulterioara a documentelor pastrate in arhiva.
- La depunerea in arhiva electronica fiecarui document electronic trebuie sa i se asoocieze o fisa electronica de date, care contina atribute ale documentului.
- Documentele electronice arhivate si fisele electronice asociate trebuie referite intr-un registru electronic de arhivare, unic la nivelul unei structuri organizatorice.
- Fisa electronica de date trebuie sa poata fi accesata prin intermediul registrului electronic de arhivare, indiferent daca documentul se afla in nearline sau offline.
- Pentru consultarea documentelor arhivate electronic sistemul trebuie sa permita cautarea dupa un set extins de criterii de cautare si in baza unui drept special de cautare in arhiva. Cautarea trebuie sa se realizeze intre referintele din registrul de arhivare electronica.
- Regasirea documentelor in arhiva electronica trebuie sa tina cont de drepturile utilizatorilor asupra categoriilor de documente, respectiv de nivelurile de clasificare ale documentelor si ale utilizatorilor.

- Daca documentele sunt in arhiva nearline, cautarea in registrul de arhivare electronica trebuie sa aiba ca rezultat un set de atribute referitoare la document si acces la fisa electronica, respectiv la document.
- Daca documentele sunt in arhiva offline, cautarea in registrul de arhivare electronica trebuie sa aiba ca rezultat un set de atribute referitoare la document si acces la fisa electronica. Pentru consultarea documentului din offline sistemul trebuie sa permita lansarea unor cereri de reactivare a documentelor.
- Sa permita reactivarea documentelor arhivate in scopul vizualizarii, in mod parametrizabil. Reactivarea documentelor electronice se va face pentru o perioada limitata de timp, perioada configurabila din interfata de administrare.
- Aplicatia de arhivare sa permita criptarea/decriptarea automata folosind certificate digitale.
- La consultarea documentelor din arhiva electronica sistemul trebuie sa verifice valabilitatea semnaturii electronice a titularului dreptului de dispozitie asupra documentului (validitatea certificatului calificat).

3.1.6.8 Registratura electronica

Sistemul va pune la dispozitie un modul de tip registratura electronica cu urmatoarele functionalitati:

- Numerotarea documentelor in regim automat, semi-automat sau manual, dupa o schema flexibila de numerotare
- Asociarea fiecarui utilizator a cate unui registru de documente personale pentru fiecare nivel de clasificare, care sa tina evidenta pe tuturor documentor adaugate in sistem de acel utilizator pe nivele de clasificare
- Asocierea fiecarui utilizator a cate unui registru al documentelor electronice procesate pentru fiecare nivel de clasificare, care sa tina evidenta pe nivele de clasificare a tuturor documentor pe care un utilizator le-a primit prin intermediul fluxurilor electronice de lucru
- Asociarea unui registru general pe fiecare structura din sistem, registru electronic in care vor fi inregistrate toate documente oficiale ale acelei structuri. Acest registru va tine evidenta documentelor intrare in structura, precum si evidenta documentelor care ies din structura sau sunt depuse in arhiva

- Toate registrele trebuie inregistrate intr-un registru unic in care se tine evidenta tuturor registrelor folosite in sistem

3.1.6.9 Mesagerie organizationala si notificari

Functionalitati solicitate:

- Sarcinile de lucru in cadrul sistemului vor fi transmise sub forma de mesaje interne ale aplicatiei si vor fi vizualizate de fiecare utilizator in sub forma unui inbox virtual din spatiul de lucru propriu
- Utilizatorii trebuie sa poata fi notificati inainte de expirarea unei sarcini sau a intregii instante de flux (procent din timpul ramas, configurabil), precum si la expirarea timpului asociat unei sarcini de lucru primite sau al intregii instante de flux
- Posibilitatea de a defini notificari la modificarea starii unui document pe flux si la adaugarea/retragerea acestuia din biblioteca.

3.1.6.10 Indicatori si rapoarte

Sistemul trebuie sa fie capabil sa genereze automat indicatori si rapoarte configurabile referitoare la:

- Starea fluxurilor in lucru
- Incarcarea utilizatorilor (general, specific, utilizatori in subordinea utilizatorului curent)
- Fluxuri finalizate
- Timpul mediu de executie pe flux
- Timp mediu de executie per activitate per flux
- Gradul de implicare al utilizatorilor per instanta per flux

3.1.6.11 Administrare

Administrarea drepturilor

Functionalitati solicitate:

- Sistemul trebuie sa permita cotrolul accesului la functionalitati si date va fi gestionat printr-o schema de drepturi multi-nivel, schema ce va fi verificata la fiecare operatie atat in mod preventiv cat si reactiv

- Interfata grafica trebuie sa fie dinamica, in sensul ascunderii integrale a datelor si functionalitatilor la care un utilizator nu are acces

- Executia unei operatii sau de acces la date va fi verificata in mod preemtiv in raport cu drepturile utilizatorului de a accesa acele date

- Drepturile de acces vor fi implementate prin intermediul unei scheme ierarhice si dinamice de roluri. Astfel, unui rol i se vor putea asocia drepturi de acces pe diferite nivele (tip document atribute ale documentelor, gradul de clasificare, instanta de document)

- La nivelul fluxurilor de documente, sistemul trebuie sa permita acordarea de drepturi pe setul de fluxuri disponibile pentru fiecare utilizator. De asemenea, la nivelul fiecarei activitati din flux, trebuie sa existe posibilitatea de a da drepturi referitor la cine sunt utilizatorii care pot efectua acea activitate si care sunt drepturile acestora in cadrul respectivei activitati

- La nivelul bibliotecii, sistemul trebuie sa permita acordarea granulata a drepturilor de acces la nivel de sectiuni/subsectiuni din biblioteca, cat si la nivelul setului de operatii disponibile (vizualizare, modificare, preluare, retragere)

- Sistemul trebuie sa permita gestiunea documentelor clasificate, in sensul de a suporta acordarea, in mod obligatoriu, a unui grad de clasificare pentru fiecare document introdus in sistem conform standardelor nationale de protectie a informatiilor clasificate in Romania (HG 585/2002). De asemenea, orice utilizator va avea asociat un nivel maxim de acces la documente clasificate, nivel ce va reglementa, in orice conditii, setul de documente la care un utilizator are acces.

- Sistemul trebuie sa implementeze un modul dedicat de audit si jurnalizare a tuturor operatiilor efectuate in sistem, cu evidentierea autorului, datei si orei, adresei de IP si descrierea operatiei.

Administrarea utilizatorilor

Functionalitati solicitate:

- Adaugare, modificare, inactivare, stergere utilizatori si date asociate
- Asocierea de date personale (nume, prenume, titlu, functie, locatie, cod de identificare, adresa e-mail, etc)
- Asociarea de roluri simple sau compuse si posibiltatea de a delega aceste roluri fie de catre utilizator, fie de catre administrator catre un alt utilizator pe o perioada data. Delegarea rolurilor presupune ca toate drepturile asociate rolurilor delegate sunt preluate automat si temporar de utilizatorul catre care se deleaga. La nivelul fluxurilor electronice de documente, utilizatorul delegat va prelua atat sarcinile curente al utilizatorului cat si cele care ii vor reveni utilizatorului initial pe perioada delegarii
- Sistemul trebuie sa permita preluarea utilizatorilor si a drepturilor acestora dintr-un structura de tip LDAP sau Active Directory
- Personalizarea interfetei in functie de rolurile si drepturile asociate utilizatorului sau grupului de utilizatori

Administrarea structurii organizatorice

Sistemul trebuie sa permita definirea si mentenanta unor strucuri organizatorice multiple, de tip ierarhic. Astfel sistemul trebuie sa permita definirea unui numar nelimitat de structuri organizatorice asociate intre ele sau independente, si pentru fiecare structura, sistemul trebuie sa permita urmatoarele:

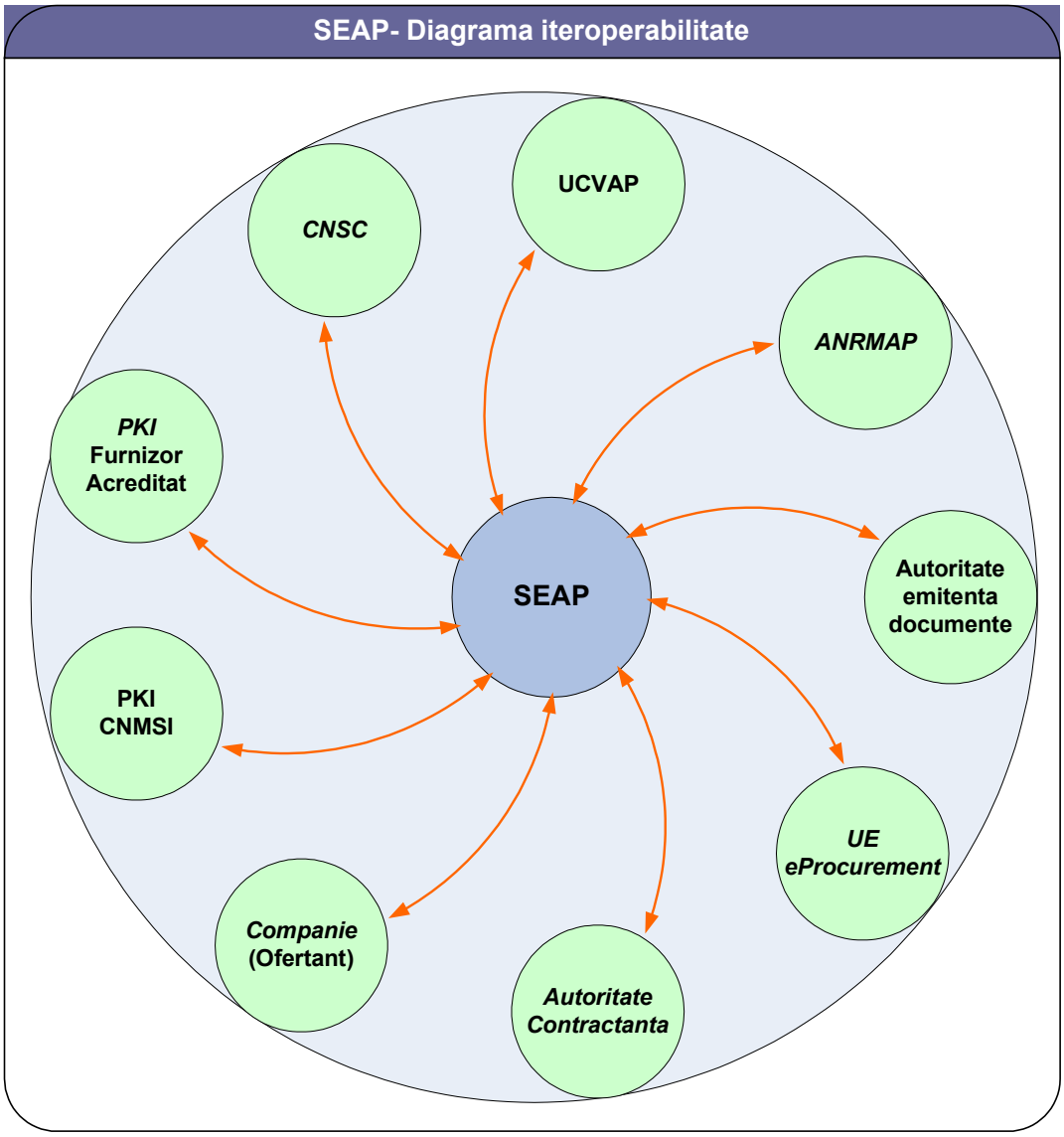
- Definirea de structuri si substructuri, iar pentru fiecare structura sa se poata defini numele, tipul, un cod de identificare, pozitia in ierarhie
- Definirea de persoane in ierahie cu precizarea functiei, pozitiei in structura (sef, subaltern, etc)
- Pastrarea istoricului modificarilor din cadrul unei (sub)structuri
- Adaugare/modificare/stergere/cautare drepturi de acces pe care le poate avea un rol pentru o ierarhie (vizualizare, printare, editare, stergere)

- Suport pentru definirea de nomenclatoare asociate structurii organizatorice (pozitii, adrese, etc)
- Suport pentru vizualizarea grafica a structurilor organizatorice definite in sistem
- Exportul organigramelor structurilor organizatorice definite in sistem in fisiere de tip imagine

Structurile organizatorice vor fi utilizate pentru a face rutarea automata a sarcinilor din fluxurile electronice de lucru, pe cale ierarhica ascendenta sau descendenta.

3.2 Arhitectura functionala a sistemului

Arhitectura functionala a sistemului urmareste integrarea si interoperabilitatea sistemului SEAP cu sistemele informatice ale entitatiilor implicate in procesele de achizitie publica. Integrarea acestor sisteme se realizeaza utilizand standard deschise bazate pe servicii web. In schema urmatoarea sunt prezentate sistemele care vor fi integrate in urma impletarii sistemului:



3.2.1 Criterii de functionare

Sistemul informatic va functiona dupa modelul unui sistem de gestiune a documentelor si a fluxuri de lucru. Prin aceasta se intelege ca va exista un motor de gestiune al documentelor si fluxurilor de lucru care se va comporta generic, indiferent de fluxul de lucru accesat de utilizatori. Acest motor de gestiune va suplini necesitatile practice de executie ale activitatilor rezultate din cerintele noilor servicii.

Fluxurile de lucru vor putea fi initiate de catre un operator uman, precum si de sistemul informatic, conform unor planificari anterioare. Astfel de fluxuri automate vor putea fi initiate de sistem pentru a usura munca operatorilor umani cand sunt indeplinite un set de preconditii ce pot fi specificate in cadrul definitiei fluxului de lucru.

Toate fluxurile de lucru inregistrate in sistem vor beneficia de facilitati standard:

- Pornire / oprire flux de lucru manual sau automat
- Persistenta informatiilor asociate cu fluxul de lucru
- Persistenta starii fluxului si avansarea pe baza de conditii a fluxului la pasul urmator
- Activitati automatizate dar si activitati manuale (ce necesita interventia operatorului uman) ce pot fi executate in cadrul fluxului
- Executie secventiala dar si paralela a activitatilor din cadrul unui flux
- Monitorizare stare fluxuri active
- Raportare fluxuri incheiate precum si parametri flux (viteza, stadiu, operatori implicati, rezultate, etc)

In cadrul fiecarui flux individual se va tine evidenta activitatilor fiecarui actor implicat in flux, precum si a timpilor alocati indeplinirii unei activitati de catre un actor din cadrul fluxului. Orice abatere de la regula de functionare a fluxului va fi raportata catre un operator supervizor ce va putea interveni pentru a corecta eventuale intarzieri in cadrul unui anumit flux.

Totodata, sistemul informatic va fi abordat din perspectiva unei arhitecturi orientate pe servicii. Va fi proiectat modular, permitand adaugarea de servicii independente in cadrul motorului principal de lucru. Serviciile individuale furnizate vor beneficia de interfete clare si functionalitati bine definite in cadrul sistemului, neexistand suprapuneri nejustificate de functionalitati intre servicii. Se va asigura astfel specializarea serviciilor pe domenii de interes.

3.2.2 Criterii de performanță şi disponibilitate

Sistemul informatic trebuie să asigure următoarele performanțe:

- Toate aplicațiile on-line trebuie să îndeplinească un nivel de disponibilitate de 99,87% anual;
- Să fie disponibil on-line pentru utilizatori 24 din 24 ore, exceptand interventiile de mentenanta ce se vor realiza in intervalul: 18.00 – 6.00
- Toate procesele off-line zilnice, care trebuie executate automat pe durata nopții (inclusiv backup de sistem), trebuie derulate în intervalul dintre orele 2:00 şi 5:00 în condiții de operare standard;

3.2.3 Cerințe de flexibilitate

Pentru a-şi desfăşura activitatea în condiții optime este nevoie de capacitatea sistemului de a produce rapoarte cu privire la informația pe care o stochează din diverse perspective, diferite

de cele utilizate pentru raportarea operațională sau managerială zilnică. În acest sens sistemul trebuie:

- să permită administratorului modificări la nivelul structurii organizatorice şi a fluxului informațional în limitele în care să nu afecteze funcționarea aplicației şi rezultatele acesteia;
- să dea posibilitatea dezvoltării de rapoarte individuale, folosind accesul standard pe bază de selecție la informația structurată;
- să permită accesul la toate datele aplicației şi să permită combinarea datelor din baza de date pentru obținerea de rapoarte particulare;
- să vizualizeze rezultatele unui raport dorit (pe ecran) înaintea tipăririi;
- să stocheze definirea unui raport individual pentru utilizări ulterioare.

3.2.4 Componentele sistemului

Din punct de vedere tehnic sistemul informatic va avea la baza urmatoarele tipuri de componente:

- Aplicatii software (definite ca acele componente software care asigura interfata cu utilizatorul)

- Servicii software (definite ca acele componente software care asigura functionarea sistemului in mod automat, fara a avea o interfata cu utilizatorul)

- Componente de infrastructura (asigura realizarea functiunilor sistemului informatic prin construirea de servicii si aplicatii software care beneficiaza de facilitatile infrastructurii)

3.2.4.1 Aplicatii software

Aplicatiile software din cadrul sistemului informatic vor fi proiectate pentru a raspunde strict cerintelor de business (functionale). Ele se vor alinia cu aceste cerinte si vor putea fi expuse utilizatorilor si administratorilor printr-o singura interfata unitara. Arhitectura aplicatiilor software va fi una de tip multi-tier, aceasta insemnand ca efectuarea operatiunilor consumatoare de timp si putere de calcul va fi lasata in seama componentelor ce ruleaza in Back Office. Clientii aplicatiilor vor beneficia de o interfata ce le va oferi acces la functionalitatile ce ruleaza in Back Office.

Pentru fiecare tip de serviciu expus de sistem se va construi un modul aplicativ software distinct care va beneficia de un suport comun de date cu celelalte module aplicative. Desi modulele vor fi concepute si executate distinct, ele nu vor fi expuse clientilor individual ci in mod integrat. Astfel, toate acestea vor fi expuse clientilor intr-o singura aplicatie integratoare, de tip portal web, proiectata

modular si extensibil. Pe viitor se vor putea concepe noi servicii si adaugate ca aplicatii distincte in portalul integrator, fara a necesita interventii asupra portalului ca atare.

Se considera ca aplicatiile si submodulele software aferente trebuie sa expuna si o interfata unitara, pentru a facilita lucrul operatorilor umani. Din acest motiv, proiectarea elementelor vizuale va fi facuta in mod centralizat si se va aplica fiecarei aplicatii printr-un motor de customizare a elementelor vizuale (teme grafice). Interfata va pastra elementele distinctive exitente in portalul SEAP.

3.2.4.2 Servicii software

Pentru ca aplicatiile software sa poata functiona eficient si rapid, ele vor fi deservite de componente active la nivel de Back Office, denumite in continuare servicii. Acestea vor avea un dublu rol, pe de-o parte de a satisface solicitari consumatoare de timp din partea aplicatiilor software, iar pe de alta parte de a executa actiuni automate ale sistemului.

Intrucat aceste servicii nu dispun de o interfata cu utilizatorul, este necesara oferirea unei interfete de monitorizare a statusului de functionare al acestor servicii pentru a facilita accesul administratorilor la informatii despre starea serviciilor sistemului.

3.2.4.3 Componente de infrastructura

In masura in care aplicatiile si serviciile vor rula intr-un mediu software distinct, se va avea in vedere ca acest mediu sa ofere servicii de baza precum:

- Securitatea accesului la resurse
- Tranzactionalitatea accesului la resurse
- Abstractizarea mecanismelor specifice ale lucrului cu resursele fizice
- Indicatori de performanta ale mediului de executie
- Mecanisme de inregistrare (jurnalizare) ale executiilor cu succes si/sau defectuoase
- Mecanisme de comunicatie (ex. email)
- Mecanisme de imbunatatire performante aplicatii (caching, throttling, etc)

3.2.5 Integrarea componentelor

Aplicatiile software livrate in cadrul sistemului informatic vor fi proiectate pe o arhitectura deschisa, avand capabilități de interoperabilitate puse la dispoziție prin expunerea de servicii. Se are in vedere posibilitatea conectarii directe cu orice altă aplicație care respectă standardele de interoperabilitate. Arhiectura orientata pe servicii este asadar o cerinta importanta a sistemului informatic pentru a asigura interconectarea acestuia cu alte sisteme pe viitor.

Toate componentele vor fi integrate cu sistemul SEAP existent si vor extinte functionalitatiile oferite de acesta. Integrarea se va face ata la nivel de interfata cat si la nivel de componente software. Este obligatorie integrarea cu componentele de securitate existente inclusiv cu functiile autoritatii de certificare si a sistemului de autentificare.

Se va realiza migrarea componentelor existente pe noile versiuni de soft de baza(Microsoft SQL 2012, Windows Server 2008) ce va fi pus la dipozitie de catre beneficiar.

3.2.6 Parametri tehnici

La nivel tehnic se vor respecta urmatoarele cerinte minime:

- Arhitectura aplicației globale va fi de tip client-server.
- Baza de date va fi de mari dimensiuni (GB) şi va trebui gestionată de un server software puternic, care să asigure integritatea, consistența, securitatea datelor şi accesul concurent al unui număr mare de utilizatori
- Interfețele cu utilizatorul vor fi "window-based" sau "browser-based".
- Pentru clientii de Windows aplicatia trebuie sa fie prevazuta o procedura automata de auto-update in cazul upgrade-urilor de versiune astfel incit sa nu se poata folosi versiuni care ar fi in neconcordanta cu structura bazei de date.
- Fiecare acces în sistem se face protejat prin intermediul unui nume de utilizator şi al unei parole si certificat digital, corespunzând unui nivel de acces configurabil de către administratorul aplicatiei.
- Ştergerea datelor din baza de date trebuie restricționată, folosindu-se doar inactivarea şi nu ştergerea lor efectivă.
- Etapa de implementare va cuprinde:
  - instalarea şi configurarea sistemului informatic;
  - inițializarea bazei de date cu informații de configurare
  - instruirea personalului administrativ şi operativ
  - asistență la demararea lucrului efectiv (simulări, probe reale)
  - instalarea componentei pentru accesul prin Internet

Algoritmi de calcul

Sistemul trebuie să folosească algoritmi rapizi pentru efectuarea de calcule si pentru efectuarea de activitati automatizate din fluxurile de business suportate.

În acest sens, serverul de baze de date va fi folosit doar pentru relaționare, calculele efectuându-se pe altă stație sau pe client.

Interfața utilizator

Toate ferestrele/ecranele pentru intrări şi ieşiri trebuie să asigure consistența interfețelor utilizator. În acest sens sistemul trebuie:

- să furnizeze toate ferestrele de dialog în limba română si engleza;
- să furnizeze ferestre formatate corespunzător pentru toate intrările şi ieşirile;
- să asigure verificarea câmpurilor de date obligatorii şi opționale
- să furnizeze mecanisme de validare a introducerii datelor pentru evitarea inconsistețelor de tip
- să permită valori inițiale pentru câmpuri de date specificate
- să conducă utilizatorul în interiorul sistemului folosind meniuri de opțiuni
- pentru operatiuni de lunga durata se vor executa comenzi asincrone (fara blocarea interactiunii utilizatorului cu aplicatia)

Se vor utiliza interfete de forma listele tabelare care sa permită:

- ordonarea automata după oricare dintre coloane sau după mai multe coloane
- ascunderea si readucerea uneia sau a mai multor coloane
- gruparea informațiilor după unul sau mai multe criterii
- printarea informațiilor direct din ecran la imprimanta
- exportul datelor din ecranul de culegere in minim următoarele formate (xls, txt, xml, html)

Interfata furnizata va trebui sa arate la fel cu cea existenta acum, interfata existenta trebuie actualizata cu o noua schema de culori si un set adecvat de resurse grafice.

Mesaje de eroare

Sistemul trebuie să furnizeze mesaje de eroare în limba română pentru:

- erori de introducere de date (inconsistență)
- erori de logică de utilizare
- erori provenite din serverul de gestiune a bazei de date.

Mesaje de ajutor

Pentru a sprijini implementarea şi utilizarea sistemului, acesta trebuie să furnizeze facilități de «help» dependent de context (în limba română).

Raportări

Facilitățile standard de raportare trebuie să cuprindă:

- furnizarea tuturor rapoartelor în limba română;
- furnizarea raportărilor on-line dar şi facilități pentru interogări ad-hoc ale bazei de date integrate;
- acordarea de priorități pentru tipărirea unui raport;
- vizualizarea rapoartelor pe ecran înaintea tipăririi;
- anularea tipăririi rapoartelor, înainte sau în timpul tipăririi;
- posibilitatea reluării tipăririi unui raport de la un anumit articol, sau de la o anumită pagină, după o întrerupere accidentală a tipăririi;
- integrarea unui modul de generare de rapoarte.

Salvare / Restaurare

Sistemul informatic trebuie să ofere următoarele facilități:

- să furnizeze un mecanism de blocare care să permită actualizări multiple şi simultane, dar care să nu provoace întârzieri inacceptabile;
- să aibă capacitatea de a efectua salvări de date in mod tranzactional;
- procesul derulării salvărilor nu trebuie să afecteze disponibilitatea sistemului pentru utilizatori şi nici să-i degradeze performanțele;
- salvarea să se poată face pe suporturi de stocare rezistente (optice, magnetice) care pot fi stocate în afara sediului;
- să realizeze o serie de verificări privind:
    - integritatea bazei de date;
    - consistența datelor din sistem
    - corectitudinea informațiilor.
- să asigure posibilitatea ca, utilizând backup off-site, în caz de catastrofă întregul sistem să poată fi recuperat pe un calculator de rezervă.
- Sistemul trebuie protejat împotriva căderilor de tensiune, asigurând o funcționare suficientă în timp pentru efectuarea operațiunilor de oprire a sistemului în mod normal.
- Să permită oricând revenirea la situația anterioara anulării unei operațiuni;

- Pentru minimizarea greşelilor individuale si a încărcării bazei de date aplicația trebuie sa ofere un mecanism eficient de simulare a efectuării unor operații.

Cerințe de localizare

Toate ecranele, mesajele de eroare şi rapoartele generate de aplicațiile software trebuie să fie produse în limba română. Toată documentația utilizator împreună cu materialele pentru instruire vor fi livrate în limba română.

Din punct de vedere al aplicației software, aceasta trebuie adaptată funcțional în totalitate la caracteristicile naționale: coduri corecte, sortări, chei primare/secundare, nomenclatoare, taste speciale, ecrane în limba română, imprimare cu caractere româneşti.

Solutia trebuie sa ofere un mecanism multilingv care sa permita traducerea aplicatiei intr-un numar nelimitat de limbi. Trebuie oferita si varianta in engleza la implementarea solutiei.

3.2.7 Infrastructura de comunicatii

Infrastructura de retea va implementa urmatoarele standardele de comunicatii:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1Q VLAN
- IEEE 802.3 10BASE-T specification
- IEEE 802.3u 100BASE-TX specification
- IEEE 802.3ab 1000BASE-T specification
- IEEE 802.3z 1000BASE-X specification

Se vor achizitiona de catre furnizorul solutiei 4 buc switch-uri ce trebuie sa respecte urmatoarele:

Caracteristici hardware:

- 24 interfete Ethernet: 10/100/1000 Mbps
- 4 sloturi SFP cu suport pentru module de fibra optica: 100BASE-FX, 100BASE-BX, 1000BASE-SX, 1000BASE-LX sau UTP 10/100/1000BASE-T
- Memorie DRAM: minim 512 MB
- Memorie Flash: minim 1 Gbps
- CPU: minim 800 MHz
- Packet switching: minim 50 Gbps

- Throughput(wire speed) Layer 2: minim 40 Mpps

Functionalitati Layer 2 si Layer3:

- Suport pentru 16000 adrese MAC
- Suport pentru 1000 VLAN-uri (cu posibilitatea de a defini pana la 4000 ID-uri) cu posibilitatea de a le aloca in functie de portul fizic sau adresa MAC
- Functionalitati standard conform IEEE: IEEE 802.1ak, IEEE 802.1AB, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.3ad, IEEE 802.3ah.
- Functionalitati standard conform RFC: RFC 791, RFC 783, RFC 792, RFC 793, RFC 826, RFC 894, RFC 903, RFC 906, RFC 1027, RFC 2068, RFC 1812, RFC 1519, RFC 1256, RFC 1058, RFC 2453, RFC 1492, RFC 2138, RFC 2139, RFC 3579, RFC 5176, RFC 2267, RFC 2030, RFC 854, RFC 951, 1542, RFC 2131, RFC 1591, RFC 2474, RFC 2598, RFC 2597
- Functionalitati Layer3 IPv4: 2000 intrari ARP, 6500 rute unicast, RIP v1/v2, rutare statica
- Functionalitati Layer 3 IPv6: rutare statica
- Securitate: filtrare in functie de adresa MAC, Sticky MAC, proxy ARP, static ARP, DHCP snooping, 802.1x

Conditii de instalare si functionare:

- Rackabil: 1 RU
- Temperatura de operare: 0° - 45°C
- Umiditate relativa la operare: 10% - 85% (fara condens)
- Masa maxima: 5 kg

3.2.8 Echipamente hardware

Pentru managementul autentificarii si controlul accesului trebuie sa fie oferite 4 servere instalate cu ultima versiune disponibila de aplicatie gateSAFE. Cerintele hardware pentru cele 4 servere sunt urmatoarele:

Echipament Server (4 buc)	
Procesor	*1x Procesor CISC x86 4-core, la frecventa de min. 3,3 GHz, min. 8 MB smart cache, DMI 5 GT/s, tehnologie pe 22 nm sau echivalent;*
Memorie RAM	*8 GB PC3-10600 1333 MHz ECC DDR3 UDIMM, min. 4 sloturi de memorie fizice, suport pentru min 32GB*
Capacitate de stocare interna	*Suport pentru minim 4 discuri interne 2,5 suport pentru HDD SAS, SATA* *Capacitate instalata - 2 x HDD SAS 300GB 15k rpm 2.5" configurate in RAID 1*

Unitate optica	*DVD-ROM*
Controller RAID intern	*Controller RAID 4 porturi SAS 6 Gbps, suport pentru RAID 0, 1, 10*
Interfata video	*Integrata in sistem, min. 16 MB*
Interfete retea	*2 x Gigabit Ethernet 10/100/1000Mbps integrata pe placa de baza*
Sloturi	*Cel putin 1 x PCI Express 2.0 x4, 1 x PCI Express 3.0 x8, full-height, half-length*
Porturi	*1 x port serial; 6 x port USB 2.0 (2 pe panoul frontal); 2 x RJ-45 LAN; 1 x port VGA*
Management	*Sistem incorporat de monitorizare a: HDD-urilor, ventilatoarelor, surselor de alimentare, temperaturii.*
	Panou cu LED-uri de indicatoare de stare pentru diagnosticarea rapida a starii de functionare a componentelor critice si software pentru management realizat de acelasi producator cu cel al serverului.
	Analize predictive de eroare pentru: HDD-uri, memorii, procesoare, surse alimentare, VRM-uri, ventilatoare cu posiblitatea anuntarii administratorului de sistem despre iminenta defectare a uneia dintre componentele enumerate anterior sau .
	Monitorizarea parametrilor de functionare a sistemului cu posibilitatea de definire de praguri critice pentru generarea de alerte
	Management de la distanta, redirectare interfata grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer), LDAP (Lightweight Directory Access Pro
Carcasa	*Rackmountable 19", maxim 1U, kit de montare in rack inclus*
Ventilatoare	*Redundante N+1*
Sursa alimentare electrica	*Consum maximal de 300 W*
Compatibilitate sisteme de operare	*Serverul trebuie sa compatibil cu urmatoarele sisteme de operare: Microsoft Windows Server 2008 R2 and 2008, Red Hat Enterprise Linux 5 and 6, SUSE Linux Enterprise Server 10 and 11, VMware ESX 4.1, ESXi 4.1, vSphere 5*
Garantie	*3 ani on-site*

3.3 Managementul utilizatorilor si accesul la sistem

Pentru securizarea sistemului informatic se va utiliza un modul de securitate dedicat, ce va contine ansamblul mecanimelor de securitate oferite. Prin mecanisme de securitate se intelege totalitatea masurilor si actiunilor ce sunt aplicate in cadrul unui sistem pentru a asigura buna functionare a acestuia (rezistenta la atacuri). Deasemenea, trebuie sa asigure ca informatiile vehiculate prin sistem nu pot fi alterate de terte parti.

Se identifica urmatoarele categorii principale de capabilitati:

- Administrare utilizatori
- Autentificare
- Asigurarea accesului la resurse
- Trasarea actiunilor in cadrul sistemului

Administrare utilizatori

Functionalitatile de administrare vor fi expuse la nivel de Back Office ca o interfata distincta, acestea urmand sa permita:

a) Definirea/modificarea/stergerea de utilizatori
b) Asocierea de roluri utilizatorilor (roluri ce vor stabili nivelul lor de acces in sistem)
c) Vizualizarea logurilor de activitate ale utilizatorilor

Mecanisme de autentificare

Autentificarea utilizatorilor in cadrul sistemului se poate realiza pe baza de certificat digital, username si parola, certificat digital organizational, username si parola. Indiferent de metoda de autentificare se va folosi comunicarea pe canale securizate pe baza protocolului SSL. In cazul folosirii certificatelor digitale acestea sunt mapate cu un utilizator al sistemului, acesta neavand nevoie de username si parola. Pentru autentificare bazata pe username si parola nu este nevoie ca utilizatorul sa fie in posesia unui certificat digital pentru a accesa sistemul. Autentificarea cu certificat digital organizational, username si parola presupune indentificarea entitatii pe baza certificatului digital si identificarea unui utilizator al entitatii pe baza perechii nume utilizator si parola. Mecanismul de autentificare este un unul generic si configurabil permitand comutarea rapida intre cele 3 modalitati de autentificare.

Asigurarea accesului la resurse

Prin verificare dreptului de acces la resurse se intelege multimea de operatii ce trebuie realizata pentru verificarea rolurilor, drepturilor si competentelor pe care un utilizator le are in cadrul aplicatiei.

Modelul de autorizare folosit trebuie sa fie unul flexibil, bazat pe roluri (Role Based Access Control), facilitand gestiunea utilizatorilor si alocarea acestora conform drepturilor pe care le au in operarea sistemului.

La nivel programatic sunt definite, cu un grad de granularitate ridicat, rolurile de baza ale sistemului si se stabileste legatura dintre roluri si meniurile aplicatiei. Administratorul sistemului are la dispozitie o interfata facila pentru a compune noi roluri din cele de baza. Tot la nivel programatic se stabilesc actiunile pe care un rol le poate indeplinii. Sistemul ofera astfel doua mecanisme de verificare si protectie importiva accesului neautorizat asupra unei resurse:

- Verificare proactiva – la autentificare sistemul incarca pentru fiecare utilizator rolul asociat si compune meniul la care acesta are acces. Se stabileste astfel aria de competente a utilizatorului logat.
- Verificare reactiva – se refera le verificare drepturilor pe care un utilizator (reprezentat prin rolul asociat) le are asupra resurselor din sistem. Acest tip de verificare se realizeaza pentru fiecare operatiune realizata in sistem si impiedica un utilizator autentificat sa obtina acces asupra unor resurse la care nu are acces.

Trasabilitatea actiunilor in cadrul sistemului

Actiunile desfasurate de catre un utilizator in cadrul sistemului sunt inregistrate pentru a oferi o imagine clara asupra fluxurilor sistemului. Aceste informatii pot fi pastrate intr-o zona sigura diferita fata de zona de persistenta a datelor pentru a nu permite alterarea lor de catre operatorul sistemului. Prin analiza logurilor se pot extrage informatii utile despre modalitatea de folosire a sistemului sau eventualele erori ce pot aparea in cadrul sistemului. Logurile pot fi consultate de catre administratorii sistemului insa nu pot fi modificate. Logurile pot fi puse la dispozitia unor institutii abilitate sa auditeze sisteme electronice pentru a demonstra ca sistemul se comporta conform asteptarilor.

3.4 Securitatea sistemului

Taoate componentele software care interactioneaza cu utilizatorul trebuie sa respecte urmatoarele cerinte de securitate:

- să suporte comunicații software prin protocol criptat;
- să fie configurat astfel încât să ofere protecție pentru următoarele vulnerabilități:
    - Cross-site scripting
    - Information leakage
    - Content spoofing
    - Predictable resource location
    - SQL injection
    - Insufficient authentication
    - Insufficient authorization
    - Abuse of functionality

Dat fiind caracterul senzitiv al anumitor informatii vehiculate in, sistemul trebuie sa asigure un set de functionalitati avansate de securizare a lucrului cu acest tip de informatii. Astfel, se doreste ca sistemul sa fie capabil sa ofere

- Autentificare pe baza de elemente avansate de securitate (certificat digital, echipamente de tip token)
- Utilizarea semnaturii digitale PKCS#7 in scopul garantarii integritatii si non-repudierii informatiilor, Trebuie sa se permita crearea de semnaturi anvelopate si semnaturi detasate
- Se va asigura implementarea unui mecanism de tip „semnezi ceea ce vezi” care presupune transpunerea informatiilor ce trebuiesc semnate intr-un format digital de tip imagine (de exemplu tiff, jpeg, bmp) pe care sa poata fi aplicate diverse filtre de culoare in vederea depistarii textului ascuns, care sa nu permita executarea de macrouri sau alte coduri care sa modifice datele pe care utilizatorul le vizualizeaza pe document inainte de semnare si crearea semnaturii pe aceasta forma
- Verificarea semnaturii de catre sistem, pe baza recipiselor si a datelor mentinute in sistem si verificarea starii certificatului cu care s-a realizat semnarea: prin OCSP (RFC 2560) si utilizarea CRL.

- Monitorizarea stricta a accesului la informatii si jurnalizarea operatiilor
- Asigura conformitate cu standardele PKCS #1, PKCS #7, PKCS #11
- Operatiunile implicand semnarea si criptarea se vor realiza utilizand certificate digitale emise de PKI ale furnizorilor acreditati.
- Posibilitatea criptarii simetrice cu urmatorii algoritmi: DES, 3DES, RC4, RC6
- Certificatele digitale ale utilizatorilor vor putea fi stocate pe dispozitive de token USB conforme cu standardul FIPS 140-2 level 2
- Operatiunile criptografice care implica utilizarea cheii private se vor desfasura numai pe dispozitive de tip token USB conforme cu standardul FIPS 140-2 level 2
- Asigurarea legaturii cu serviciul de marcare temporala pentru documente conform RFC 3161
- Folosirea unor certificate digitale separate pentru operatiunile de criptare si semnare
- Autentificarea utilizatorilor in sistem se va realiza pe baza de nume si parola, precum si de certificate emise de PKI CNMSI, cu garantarea validitatii starii certificatelor digitale la acel moment de timp, accesand serviciul de validare OCSP (RFC 2560)
- Pentru autentificare ofertantul trebuie sa furnizeze si si sa utilizeze ultima versiune de aplicatie gateSAFE.
- Compatibilitate cu standardul LDAP v3

3.5 Confidentialitatea datelor

Securitatea mediului de comunicare trebuie asigurata prin folosirea protocolului HTTPS (bazat pe SSL 128 biti). Pentru a permite acest tip de comunicare serverul trebuie sa dispuna de un certificat digital utilizabil pentru criptare si semnare. Folosirea acestui protocol asigura criptarea comunicatiei intre cele doua entitati aflate in discutie facand imposibila intelegerea mesajelor schimbate intre entitati.

Toate informatiile sensibile care trebuie salvate in cadrul sistemului informatic vor fi mai intai criptate sau tinute sub forma de hash. Exemplu de informatii care trebuie tinute criptat ar

fi string-urile de conectare la baze de date daca acestea contin acreditive pentru conectare iar parolele utilizatorilor sunt date care trebuie salvate sub forma de hash.

3.6 Monitorizare, optimizare si analiza date

Organizatia noastra doreste implementarea unei solutii de management de aplicatii, baze de date si infrastructura care sa elimine discontinuitatea serviciilor oferite de IT catre zona de business, unificand in acest fel cele doua componente.

Caracteristici generale:

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 are nevoie de corelarea datelor culese si analizate din perspective multiple. Este nevoie de analiza detaliata a relatiei intre end-user, modelul operational si componentele de infrastructura.

Solutia trebuie sa ajute la cresterea performatelor sistemelor, imbunatatirea service-level, combinat cu scaderea riscurilor si a cheltuielilor operationale

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.

Solutia trebuie sa fie capabila sa coreleaze sute de relationari si mii de indicatori masurati intr-o singura consola relevanta din orice perspectiva

-Din perspectiva serviciului oferit sa se vada modul in care performanta si disponibilitatea afecteaza businessul

-Din perspectiva utilizatorului final sa se vada cum acesta interactioneaza cu aplicatiile si cum acestea raspund nevoilor sale

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

Capabilitati de management:

Solutia ideala trebuie sa aiba urmatoarele capabilitati:

Service Level Management

Sa integreze componente IT diferite in servicii pe care le reprezinta intr-o forma ce are semnificatie pentru business.

- Modelare cross-domain
- Panou de control bazat pe roluri
- Mapare si descoperire automata a serviciilor
- Prioritizarea problemelor bazata pe impactul la nivelul business-ului

Infrastructure Management

Solutia trebuie sa ofere monitorizarea, controlul si diagnosticarea echipamentelor de retea, serverelor, sistemelor de operare si a altor echipamente de infrastructura IT.

Trebuie monitorizat pentru servere:

- CPU
- I/O
- Memorie
- Swap
- Procese
- Utilizatori
- Fisiere de log (cu cautarea si alertarea sa aparitia unor pattern-uri stabilite)

Pentru echipamente de retea:

- Vizualizarea capacitatii routere-lor si switch-urilor LAN/WAN
- Identificarea rateror de erori
- Rapoarte detaliate FECN/BECN (forward explicit congestion notification / backward explicit congestion notification)

- Analize de trafic – Identificarea aplicatiilor consumatoare de trafic
- Analize de disponibilitate si latenta – identificarea depasirilor unor praguri prestabilite

Database Management

Sa monitorizeze orice platforma de baza de date, incluzand Oracle, SQL Server, DB2 LUW si Sybase si sa se constituie intr-o reala platforma enterprise de monitorizare a performantelor si disponibilitatii bazelor de date.

- Monitorizare
- Diagnostic
- Analiza performante real-time si istorica
- Optimizare fraze SQL
- Managementul capacitatii / spatiului

Application Performance Management

Solutia trebuie sa ajute manageri IT si de aplicatie sa inteleaga nivelele acceptate ale serviciilor livrate catre utilizatorii finali pentru a asigura continuitate afacerii in conditii optime.

- Monitorizare si corelare intre nivelul business si componentele de infrastructura
- Monitorizarea tranzactiilor si corelarea intre ce face utilizatorul final si comenzile care ajung la baza de date
- Modelarea dependintelor intre aplicatii
- Detectare rapida a cauzei primare a unei probleme si rezolvarea acesteia

Caracteristici cheie:

Pentru a rezolva alinierea serviciilor IT cu cerintele de business solutia trebuie sa:

-Descopere automat componentele IT si sa permita maparea acestora pe serviciile de business definite. In acest mod se va elimina setarea manuala si administrarea continua.

-Bazat pe aparitia evenimentelor, sa ofere corelare pe nivele multiple, prioritizare de incidente si analiza de impact asupre business-ului

-Sa suporte mediu eterogen, iar integrarea si corelarea sa se faca intr-o interfata unitara

Pentru a oferi o vedere unificata a intregii infrastructuri IT, solutia trebuie sa:

-Permita vizualizarea dependintelor intre servicii, legaturile intre servicii, utilizatori si infrastructura pentru a permite planificarea si prioritizarea

-Aiba o trasabilitate individuala, la nivel de end-user, sa permita rezolvari personalizate pentru orice problema aparuta

-Sa aiba o singura consola pentru a vizualiza intregul sistem (aplicatii, baze de date, infrastructura)

Pentru a oferi o platforma rapida de rezolvare a incidentelor, solutia trebuie sa ofere:

-Diagnostic detaliat pe sistemele de productie, cu determinarea rapida a cauzelor fara a fi necesara reproducerea erorii

-Management unificat intre suport si dezvoltare pentru escaladare si rezolvare rapide

-Audit al modificarilor si management al versiunilor pentru a asigura integritatea mediilor de productie

Pentru a usura adaptarea la schimbarile viitoare, solutia trebuie sa ofere:

-Mapare automata a dependentelor intre servicii

-Fiecare user, sau grup sa poata modifica propriile view-uri si politici

-Sa aiba un workflow predefinit al proceselor si sa permita customizarea acestuia pentru a fi conform cu politicile interne ale organizatiei

Avantajele solutiei ideale

Solutia aleasa trebuie in mod obligatoriu sa permita urmatoarele:

Management avansat al serviciilor:

- Vizualizarea impactului modificarilor asupra business-ului
- Creare si management de SLA
- Descoperire automata si mapare a serviciilor

Panouri de comanda si control cu operare si administrare bazate pe roluri

- Securitatea trebuie sa poata fi integrata cu platforme tip LDAP
- Interfata trebuie sa fie web fara a necesita instalarea de plug-in-uri
- Sistemul trebuie sa permita auditarea tuturor operatiilor efectuate (mecanism de self-audit)

Solutia trebuie sa aiba mecanism de failover si clustering out-of-the-box

Diagnostic, Analiza de Performanta, Managementul Spatiului si Optimizare baze de date

Pentru o administrare completa a bazei de date este nevoie de o consola centralizata intuitiva, usor de instalat si utilizat, ale carei module sa ajute in administrarea si monitorizarea instantelor de baze de date, sesiunilor, obiectelor, schemei si utilizatorilor. De asemenea, avem nevoie de solutii care sa permita administratorilor bazelor de date sa administreze mai multe obiecte si baze de date dintr-o singura interfata grafica flexibila si orientata catre utilizator. Interfata grafica sa permita accesul rapid si centralizat la toate modulele. Solutia trebuie sa integreze in acelasi produs module pentru administrarea bazelor de date (managementul instantelor, managementul schemei, managementul securitatii, managementul serviciilor), optimizare instructiuni SQL, diagnosticarea si managementul performantelor, managementul spatiului. Solutia trebuie sa permita conectarea la mai multe instante de baze de date simultan indiferent de versiunea acestora, precum si conectarea la platforme diferite de baze de date.

Suita de management al performantelor trebuie sa se integreze cu sistemul de monitorizare.
Toate modulule acestei suite trebuie sa fie disponibile pentru diferite platforme de baze de date (Oracle, SQL Server, DB2, Sybase, etc), avand functionalitati similare.

Functionalitati pentru administrarea bazelor de date

Pentru administrarea bazelor de date, solutia trebuie să aiba urmatoarele functionalitati:

sa permita ca procedurile, functiile si pachetele sa poata fi compilate, verificate si depanate

sa permita modificarea parametrilor de configurare si a optiunilor bazei de date

sa permita crearea si planificarea de joburi

sa prezinte sabloane particularizabile pentru proceduri, functii, triggeri si pachete

existenta unui buffer urias pentru undo/redo, sintaxa colorata, facilitate de scriere type-ahead, liste de selectie pentru coloane sau proceduri din pachete, localizarea rapida a erorilor si afisarea lor intr-o semifereastra, localizarea rapida a componentelor din pachete (prin afisarea lor într-o fereastra din stanga ferestrei de editare), posibilitatea de salvare sau recuperare pe/de pe disc in formate variate cum ar fi HTML, Excel, statement-uri INSERT,

sa permita o administare completa a securitatii din baza de date prin crearea, modificarea, stergerea utilizatorilor, rolurilor şi profilurilor

sa permita vizualizarea si administrarea tablespace-urilor, fisierelor redolog, segmentelor rollback, fisierelor de control pentru managementul de spatiu

sa contina editoare de scripturi SQL, proceduri, functii, trigere etc, care să aiba functii de tip “make” si “strip” de portare fraze sql direct din si catre alte aplicatii

la nivel de schema sa poata crea si modifica rapid obiectele din baza de date, sa poata vizualiza dependentele dintre obiectele schemei, sa poata realiza comparari si afisari de rapoarte pe schema si pe obiectele din ea, precum si diagrame cu obiectele din schema

sa permita cautarea după criterii diverse a obiectelor din baza de date

sa permita compararea de scheme, fisiere de cod

sa permita formatarea customizata a codului pentru o mai buna lizibilitate, sa permita encriptarea codului stocat in baza de date

sa contina o colectie completa de „code snipets”(mici blocuri de cod reutilizabile) pentru majoritatea functiilor bazei de date

sa includa si un modul specializat de debug al codului pl/sql care sa faciliteze crearea unor asa-zise view-uri imbunatatind serios timpul de detectare al erorilor.

sa detecteze erorile de logica in programare, sa efectueze rulari pas cu pas si sa faciliteze rezolvarea problemelor fara scrierea de cod suplimentar pentru detectarea portiunilor de cod in dubiu

prin intermediul lui sa se poate urmari evolutia unei proceduri sau functii (chiar apelata si din exterior) fara inserare de cod suplimentar
sa contina wizard-uri detaliate pentru operatiunile de import, export, data pump şi sqlload
sa permita exportul ad-hoc al rezultatului unui query in formatele uzuale (csv, text, excel, etc.)
sa contina un modul cu functionalitate de Group Policy care sa adauge un strat intermediar peste securitatea nativa Oracle care sa permita o mai buna gestiune a accesului utilizatorilor la functionalitatile produsului de administrare.
sa permita lucrul in echipa cu functionalitati de versionare a codului si functii "check-in" si "check-out"

Functionalitati de analiza a performantelor

-Sa permita colectarea de date referitoare la performantele bazei de date, folosind servicii de colectare cu rata mare de esantionare (sub o secunda) si necostisitori din punct de vedere a resurselor consumate
-Sa permita culegerea de informatii direct din structurile de memorie ale instantei bazei de date (fara a cauza intarzieri sau blocaje in procesele bazei de date)
-Sa permita ajustarea nivelului de ocupare al procesorului de catre agentul de colectare, cu posibilitatea reducerii ratei de esantionare in momentele de varf de activitate
-Sa interogheze „Performance Views" cu o frecventa care sa nu ingreuneze activitatea in baza de date
-Produsul trebuie sa fie capabil sa asocieze fiecarei fraze SQL informatii detaliate referitoare la : CPU utilizat, IO consumat, sesiunea utilizata (OS User, DB user, aplicatie, statie de lucru, etc.), blocaje, utilizarea memoriei si evenimentele de tip wait
-Sa invete comportamentul bazei de date in functie de ora din zi, ziua din sapatamana, etc. si in acest mod sa creeze un „baseline", o referinta la care raporteaza activitatea curenta semnaland orice deviatie de la aceasta
-Sa permita o analiza curenta si istorica a performantelor bazei de date
-Sa arate marii consumatori de resurse in termeni de instructiuni SQL, sesiuni, utilizatori, programe
-Sa contina rapoarte de comparare a intregii activitati, precum si particulariazat pana la nivelul de granularitate a unei singure fraze SQL

-Sa permita un change management in detaliu. Sa arate orice modificare in baza de date in intervalul de timp selectat, inclusiv modificarile planurilor de executie ale frazelor SQL

-Sa permita organizarea unui warehouse cu datele de performanta in care sa pastreze pe o perioada nelimitata datele culese si ofera facilitati OLAP de analiza a performantelor

-Sa permita comparatia detaliata a activitatii din baza de date. Adica, sa se poata vizualiza activitatea unui modul (aplicatie), a unui utilizator sau chiar a unei fraze sql individuale comparativ in perioade diferite de timp. De asemenea, sa permita compararea unor indicatori diferiti, a unui modul cu altul in perioade diferite de timp (pentru a fi utilizat la inlocuirea, sau upgrade-ul aplicatiilor)

-Sa contina rapoarte predefinite privind performantele curente si istorice ale bazelor de date

-Sa permita crearea de rapoarte individualizate privind performantele curente si istorice ale bazelor de date

-Sa prezinte un „Dashboard" care consolideaza indicatorii cheie de performanta, permite intelegerea dintr-o privire a sanatatii bazei de date si contine rezultatele testelor de performanta sub forma unor „Best Practices" si/sau „Performance Advisories"

-Sa permita executia programata a acestor rapoarte, exportul automat in formate doc, sau pdf si transmiterea pe mail

-Sa permita analiza performantelor mediilor de stocare (storage) ale bazelor de date

-Va pastra toate datele colectate pentru 5 ani

-Sa aiba posibilitatea de playback si playforward, astfel incat sa se poate analiza comportamentul istoric si previziona cel viitor

-Sa functioneze si in mod silentios, sa nu fie nevoie astfel de supraveghere permanenta. Solutia va permite emiterea de alerte in cazul depasirilor consumurilor de avarie

-Solutia trebuie sa se integreza cu un produs de monitorizare care sa centralizeze si sa pastreze toate alarmele.

-Solutia trebuie sa suporte Oracle RAC si sa ofere analiza de ansamblu a RAC-ului si individual pe fiecare instanta, tinand cont de infrastructura tehnologica existenta in cadrul CNMSI

-Produsul trebuie sa contina modul integrat de analiza in timp real a bazei de date utilizat in detectarea unui numar mare de probleme de performanta, modul care:

o Sa programeze si sa execute o analiza pe datele colectate in intervalul stabilit, pe zile, pe momente de incarcare maxima sau pe alte criterii arbitrare, si pregateste rapoarte detaliate

care contin toate problemele aparute la nivelul bazei de date (Database Health Check) pe baza statisticilor colectate la intervale de timp stabilite

o Sa ofere diagnoze expert privind performanta instantelor bazelor de date si sa includa un set complet de recomandari si instructiuni detaliate si sa puna la dispozitia personalului desemnat solutii clare pentru toate problemele depistate

o Sa ofere diagnoza avansata si un plan de actiune coerent pentru maximizarea performantei si scalabilitatii bazei de date

o Sa contina rapoarte cu link-uri pentru a face „drill-down" la toate problemele aparute in baza de date pentru a oferi dovezi solide si solutii de rezolvare

o Sa contina doua tipuri de rapoarte de analiza, unul privind probleme de performanta si sfaturi de rezolvare, iar altul privind sugestii de aplicare a celor mai bune practici in administrarea si tuningul bazelor de date

o Rapoartele trebuie sa poata fi programate spre executie automata, inclusiv sa poata fi distribuite pe mail si/sau exportate in toate formatele uzuale (pdf, doc, html, etc)

o Cu ajutorul acestor analize sa se poata identifica:

o erori in configurarea instantei de baze de date

o fraze SQL consumatoare de resurse

o probleme in gestionarea spatiului

o anomalii in administrarea schemelor de baza de date

o sugestii de imbunatatire a performantelor

.

Functionalitati pentru diagnosticarea performantelor in timp real

- Produsul trebuie sa realizeze diagnosticul activitatii sistemului in timp real
- Sa permita conectarea din aceeasi consola la multiple instante de baze de date, indiferent de versiunea acestora
- Sa aiba o interfata vizuala, respectiv o harta a arhitecturii bazei de date din care sa se poata vizualiza exact componentele sale precum si fluxul de date intre acestea
- Interfata vizuala sa fie insotita de explicatii privind fiecare element al arhitecturii bazei de date cu acces rapid si link-uri catre manuale electronice la topic-ul care explica exact elementul din arhitectura bazei de date pe care s-a dat click
- Sa permita executarea unei aplicatii pe client in momentul aparitiei unei alarme

- Sa permita diagnosticul atat al bazei de date cat si al sistemului de operare de pe serverul de baza de date
- Sa identifice vizual gatuirile la nivel de sistem avand facilitati de inspectare detaliata (drill down)
- Sa notifice administratorul de baze de date prin intermediul alarmelor vizuale, auditive, mail sau pager cand un anumit prag critic este depasit (threshold). Sa permita customizarea acestor praguri de alertare, precum si configurarea lor automata in functie de activitatea bazei date printr-un proces de calibrare.
- Sa permita trimiterea selectiva de alerte, pe baza de reguli, inclusiv doar a alertelor care nu au fost detectate de administrator (de exemplu s-au petrecut noaptea sau in pauza)
- Sa permita un istoric al incidentelor cu posibilitaea reproducerii exacte a activitatii din momentul producerii lor. Inregistrarea activitatii bazei de date in scopul reproducerii se va face pe o perioada de mai multe zile in functie de spatiul alocat pentru aceasta
- Administratorul sa poata in orice moment, in mod vizual sa faca „replay" la activitatea din baza de date pentru a vizualiza cu exactitate situatia in care a fost generata o alerta
- Solutia sa fie disponibila pentru cele mai cunoscute platforme de baze de date si sa permita monitorizarea acestor platforme din aceeasi consola (Oracle, Oracle RAC, SQL Server, Sybase, DB2)
- Produsul trebuie sa suporte Oracle RAC
- Sa permita diagnosticarea Oracle RAC, atat la nivelul unui nod individual, cat si la nivelul clusterului ca entitate
- Sa permita vizualizarea incarcarii interconect a latentei si overheadului cauzate de cluster
- Sa permita diagnosticarea si alertarea cu privire la subsistemul I/O
- Sa permita vizualizare alert log-ului
- Sa permita in configuratia Oracle RAC, combinarea alert log-urilor individuale de pe fiecare instanta intr-unul singur global.
- Sa contina un modul de diagnostic predictiv care sa detecteze inconsistentele in trendul performantei frazelor SQL
- Sa suporte ASM

Functionalitati pentru gestiunea spatiului

- Sa asigure reorganizarea si defragmentarea tablespace-urilor, tabelelor si indecsilor intr-un mod automatizat
- Sa detecteze problemele legate de spatiu si sa faca previziuni si analize asupra problemelor de spatiu si capacitate
- Sa afiseze grafic harta tablespace-urilor
- Sa determine momentul in care obiectele isi depasesc spatiul alocat
- Sa ofere o analiza a cresterii dimensiunii bazei de date
- Sa permita planificarea capacitatii tablespace-urilor
- Sa ajute la minimizarea utilizarii resurselor salvand spatiu de disk si costurile asociate
- Sa permita reorganizarea bazelor de date fara a intrerupe accesul utilizatorilor de aplicatii (datele din tabele sa ramana accesibile, pentru citire si modificare, pe durata reorganizarii)
- Sa permita reorganizarea tabelelor care includ coloane de tip LONG (foarte utilizate in majoritatea aplicatiilor) fara a intrerupe accesul la baza de date (datele din tabele sa ramana accesibile, pentru citire si modificare, pe durata reorganizarii)
- Sa permita partitionarea tabelelor si repararea „chained rows" (datele din tabele raman accesibile, pentru citire si modificare, pe durata partitionarii si a repararii „chained rows")
- Sa permita executia task-urilor de catre un agent, astfel incat acestea se vor executa fara sa depinda de aplicatia sau clientul bazei de date

Functionalitati pentru optimizarea instructiunilor SQL

- Sa detecteze instructiunile SQL cu probleme de performanta, direct din obiecte stocate in baza de date (proceduri, vederi etc.) sau din fisiere sursa fara a necesita executia lor; in plus permite si detectarea instructiunilor SQL dinamice (create la momentul executiei)
- Sa ofere posibilitatea de a scana, gasi si optimiza instructiunile ineficiente
- Sa permita vizualizarea in detaliu planurile de executie ale instructiunilor SQL
- Sa gaseasca automat instructiunile SQL alternative - instructiuni cu sintaxa diferita dar echivalente semantic (produc exact acelasi set de rezultate)
- Sa execute automat scenariile asociate cu originalul si cu alternativele gasite in vederea colectarii de statistici privind executia lor
- Sa permita compararea statisticilor aferente si alegerea automata a celui mai bun scenariu.
- Sa permita utilizatorului sa decida intre scenariile alternative, varianta pe care o considera optima

- Sa se integreze cu un modul de Benchmarking pentru teste de scalabilitate
- Sa aiba facilitati de generare alternative de indecsi pentru o anumita instructiune SQL in relatie cu tabelele referite, permite simularea lor si alegerea celor mai bune variante
- Sa permita crearea si gestionarea de planuri de executie (outlines)

Functionalitati pentru simularea accesului si testarea bazei de date

- Sa permita executia unor teste standard in industrie (AS3AP, Scalable Hardware, TPC-B, TPC-C, TPC-D, TCP-H)
- Sa permita crearea propriilor scenarii de test prin introducerea frazelor sql
- Sa permita capturarea frazelor sql direct din fisierele sql trace ale bazei de date, putand in acest fel reproduce in mod exact activitatea din baza de date
- Pentru simularea frazelor sql, produsul sa aiba dictionare detaliate (nume, coduri postale, localitati, etc.), precum si functii speciale de generare aleatoare si/sau unice de valori (numerice, de tip data, de tip text). In acest mod se va evita repetarea la nesfarsit a unei singure fraze sql (lucru nerelevant pentru analiza), sau un efort prea mare de concepere a scenariului de test
- Sa permita combinarea tuturor acestor scenarii de test
- Sa permita analiza scenariilor executate si culegerea de statistici de tipul „transaction/second”, „response time”, etc
- Sa permita executia scenariilor de test in paralel cu multiple conexiuni la baza de date, in acest fel simulandu-se activitatea concurenta a utilizatorilor
- Sa permita folosirea de agenti comandati de la o consola centralizata pentru a putea balansa numarul de conexiuni deschise statiile client. Adica daca se doreste simulare cu 400 de useri concurenti, sa se poata face de pe 10 statii de lucru, fiecare cu cate 40 de sesiuni deschise la baza de date

Securitate, Audit Trail si Compliance

Pentru conformitatea cu regulile de securitate interne si externe, 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.

Infrastructura actuala se confrunta cu necesitatea auditului, colectarii si stocarii tuturor logurilor de acces, securitate si operationale din organizatie (sau dintr-un subdomeniu).

Pentru conformitatea cu orice standard de securitate, intern sau extern, vor trebui realizate urmatoarele:

- culegere automata de loguri din toate sursele

o Servere

o Aplicatii

o Statii de lucru

o Echipamente de retea

- Stocare pe termen lung (de obicei 3-5 ani) a tuturor logurilor fara posibilitatea de a altera logurile stocate

o Stocare cu rata mare de compresie

o Criptare pentru logurile stocate

- Rapoarte flexibile pentru toate tipurile de loguri

- Posibilitatea de a tine intr-o baza de date relationala logurile doar de un anumit tip si doar pe o anumita perioada de timp pentru a minimiza costurile hardware

- Acces rapid la logurile arhivate

- Alerte flexibile si integrare cu alte console de monitorizare

- Corelare de evenimente in functie de utilizatorul din LDAP

Cerinte minime:

o Sa ofere redundanta automata in cazul defectarii serverului de colectare si alertare. Acest lucru va elimina posibilitatea de a pierde loguri in caz de eroare hardware

o Sa permita crearea unei zone criptate de cache unde logurile sunt salvate automat pe masura ce sunt create. Acest lucru elimina posibilitatea alterarii de loguri de catre

administratori rau intentionati. Adica un administrator care face operatiuni suspecte cu serverul scos din retea si apoi sterge logul sa nu se poata feri de acest mecanism.

o Sa ofere un storage pe termen lung cu rata de compresie de 1:100 unde toate logurile sa fie pastrate in format criptat (de exemplu conform standardului 3DES 168 bit). Acest repository sa fie unica sursa de log si sa nu mai fie necesar backup-ul logurilor la sursa.

o Sa simplifice operatiunea de masurare a comportamentului in retea si sa permita detectarea incidentelor de securitate. Pentru a detecta aceste evenimente suspecte, este necesar sa ofere posibilitatea de comparare a evenimentelor suspecte cu pattern-urile masurate in mod normal (functionlitate de Anomaly Analizer)

o Sa trimita alerte direct prin mail, sau prin intermediul unei aplicatii de monitorizare

o Sa automatizeze colectarea securizata de loguri, iar prin programarea job-urilor de colectare sa se minimizeze impactul asupra retelei

o Sa coreleze in mod automat evenimentele critice si sa alerteze cu privire la orice activitate neobisnuita

Cerinte functionalitati:

- Stocarea logurilor sa fie arhivata si criptata pe terment nelimitat cu necesitati minime de storage (rata de compresie de pana la 1:100).
- Garantia ca toate logurile astfel pastrate provin din sursele originale, nu au fost modificate dupa colectare si pot fi utilizate ca dovezi.
- Arhitectura sa fie flexibila si scalabila, precum si usurinta in producerea rapoartelor de securitate pentru tehnologiile propietare.
- Sa ofere corelarea tuturor evenimentelor din organizatie, din orice sursa in functie de contul din LDAP
- Detectare automata a activitatilor suspecte pe baza unui pattern stabilit automat (prin Anomaly Analizer)
- Sa aiba un portal ce asigura totalitatea task-urilor pentru conformitatea cu standardele SOX, HIPAA, Basel II, ISO 27001, 27002, ITIL, COBIT
- Sa permita monitorizarea tuturor sistemelor si sa asigure conformitatea cu standardele de securitate
- **Sa colecteze logurile in mod securizat:** Solutia trebuie sa garanteze integritatea si securitatea logurilor. Solutia trebuie sa cripteze si comprime logurile inainte de transmisie

- **Sa pastreze multe date online:** Solutia trebuie sa ofere un mod flexibil de stocare in care sa se poata pastra online cat mai multe loguri pe cat mai mult timp. Logurile trebuie pastrate in mod arhivat si comprimat. Solutia care va oferi cel mai mare grad de compresie in acest storage este candidatul ideal.
- **Ai aiba o consola de raportare inteligenta:** Solutia trebuie sa ofere rapoarte predefinite, precum si osibilitatea de a crea rapoarte noi. Aceste rapoarte sa poata fi distribuite si exportate in formatele cunoscute: pdf, excel, text, csv, etc.
- **Sa imbunatateasca securitatea si performanta:** Solutia trebuie sa ofere alertare realtime. Sa existe posibilitatea de a defini alerte noi, iar acestea sa poata fi trimise direct pe mail, sau catre o alta consola de monitorizare (MOM)
- **Sa ofere suport pentru compliance:** Solutia sa ofere mecanisme care sa rezolve controalele cerute de standardele de securitate interne si externe prin monitorizarea accesului la sistemele critice si detectarea evenimentelor suspicioase.
- **Sa ofere automatizarea completa:** Coletarea logurilor trebuie sa fie complet automatizata fara interventie manuala.
- **Sa monitorizeze activitatea userilor:** Sa colecteze si sa coreleze userii si administratorii si sa alerteze in mod automat la aparitia oricarei activitati anormale
- **Sa garanteze integritatea logurilor:** Sa permita crearea unui cache, a unei zone tampon pe serverele monitorizate unde logurile sa fie duplicate pe masura ce sunt create. Acest lucru trebuie sa impiedice alterarea logurilor de catre administratori pana ce acestea sunt colectate de procesul automat de colectare.
- **Redundanta:** Solutia trebuie sa permita existenta unui server redundant catre care sa poata fi cu usurinta mutate configuratia, si task-urile de colectare si raortare.
- **Compresia datelor:** Solutia trebuie sa ofere un mecanism de stocare a datelor care sa fie conform cu standardele ce securitate (criptat si arhivat). Acest mecanism trebuie sa inlocuiasca backup-ul traditional al logurilor de pe sistemul sursa. Logurile ajunse in acest loc sa nu mai poata fi alterate in nici un fel, cu nici un fel de parola, sau alta metoda de acces.
- **Analiza anomaliilor:** Solutia trebuie sa simplifice descoperirea tendintelor in activitatea din sistem si sa detecteze incidentele de securitate cum ar fi tentativele de acces in sistem, sau in internet
- **Alertare in timp real:** Solutia trebuie sa ofere o consola de alertare si posibilitatea de a configura alerte bazate pe politici flexibile. Aceste alerte trebuie sa fie trimise catre aceasta

consola, sau catre alta consula de alertare utilizata. Acest lucru este necesar pentru a nu folosi mai multe console de alertare in organizatie.

- **Rapoarte flexibile:** Solutia trebuie sa contina rapoarte predefinite si customizabile. Rapoartele treuie sa aibe sursa deschisa pentru a putea crea alte rapoarte noi pe baza celor existente. De asemenea sa existe posibilitatea de a exporta aceste rapoarte in formatele traditionale (HTML, XML, PDF, CSV and TXT, as well as Microsoft Word, Visio and Excel)
- **Instalare rapida si deplyment usor:** Solutia trebuie sa permita instalarea usoara, configurarea prin wizard-uri, iar agentii de monitorizare sa poata fi instalati centralizat.
- **Interfata de raportare si administrare usor de utilizat:** Solutia trebuie sa ofere o interfata Windows de administrare bazata pe roluri integrata in LDAP. De asemenea mecanismul de raportare sa aiba posibilitatea de a configura accesul utilizatorilor pana la cea mai fina granularitate (raport individual), iar accesul sa fie integrat cu LDAP.

Cerinte de arhitectura:

1	Solutia sa poata fi configurata astfel incat sa ofere conformitatea cu regulile de securitate ale companiei.
2	Solutia sa ofere un management scalabil al evenimentelor, putand gestiona multiple site-uri si echipamente.
3	Solutia trebuie sa permita integrarea cu echipamentele de retea (routere cu management), precum si cu alte echipamente generatoare de log de acces, cum ar fi cele care tin de securitatea fizica (carduri de acces).
4	Solutia trebuie sa permita crearea de template-uri pentru a putea include in mecanismele de colectare si alte loguri decat cele standard.
5	Solutia trebuie sa ofere un mecanism de incredere pentru a garanta integritatea si securitatea logurilor transportate in cadrul procesului de colectare.
6	Solutia trebuie sa ofere un mecanism de protejare a datelor stocate. Aceste loguri nu trebuie sa poata fi modificate sub nici o forma.
7	Solutia trebuie sa ofere facilitatea de a normaliza logurile fara a pierde informatia.
8	Solutia trebuie sa suporte failover pentru componentele sale critice.
9	Solutia nu trebuie sa aiba impact major asupra sistemelor monitorizate. Colectarea trebuie sa se faca cu, sau fara agenti. Alertarea trebuie sa fie implementata pentru toate sistemele indiferent de natura acestora. Trebuie sa existe posibilitatea de alertare in timp real pentru sistemele pe care nu se

	doreste, sau nu se poate instala agenti. Acestea pot fi masini UNIX/Linux, sau routere si alte echipamente de retea cu management.

Colectarea datelor si normalizarea:

1	Produsul trebuie sa permita colectarea logurilor de securitate de pe toate sistemele fara a utiliza agenti: sisteme Unix, Linux, Windows, baze de date si aplicatii personalizate si loguri de tip text
2	Produsul trebuie sa permita stocarea criptata si arhivata a tuturor logurilor adunate.
3	Produsul trebuie sa pastreze logurile intr-o structura diferita de baza de date pentru a minimiza necesarul de stocare pentru pastrarea logurilor pentru minim 3 ani. Prim mecanisme automate aceste loguri sa poata fi oricand accesate si aduse intr-o baza de date pentru raportare, analize si investigatii.
4	Produsul trebuie sa permita accesul rapid la logurile salvate cu costuri minime de stocare (fara a implica medii lente nesigure, cum ar fi benzile de backup).
5	Sa permita crearea unui cache, a unei zone tampon pe serverele monitorizate unde logurile sa fie duplicate pe masura ce sunt create. Acest lucru trebuie sa impiedice alterarea logurilor de catre administratori pana ce acestea sunt colectate de procesul automat de colectare.
6	Sa permita colectarea de pe toate sistemele din organizatie cu sau fara agenti instalati pe aestea
7	Sa permita filtrarea, arhivarea si criptarea logurilor la nivelul sursei pentru a minimiza impactul asupra comunicatiilor
8	Sa permita compresia evenimentelor. Cerinta este ca toate logurile sa fie pastrate online pentru o perioada de cel putin 3 ani

Monitorizare

1	Produsul trebuie sa contina un mecanism de alertare asupra evenimentelor sensibile de securitate cu posibilitatea de a crea noi alerte cu politici flexibile
2	Produsul trebuie sa permita trimiterea de alerte catre alte sisteme de monitorizare
3	Produsul trebuie sa permita monitorizare in timp real pe sisteme UNIX/Linux si echipamente de retea fara a utiliza agenti
4	Produsul trebuie sa permita monitorizare a logurilor in timp real pentru sisteme Windows cu posibilitatea de creare de alerte si actiuni personalizate.
5	Produsul trebuie sa contina o lista predefinita si cuprinzatoare de alerte pentru a facilita implementarea politicilor de securitate ce se impun: - alerte pentru o modificari de conturi de calculator

	o creare de conturi de calculator o stergere de conturi de calculator o autentificare reusita pentru user o autentificare nereusita pentru user (cont blocat) o utilizator creat o utilizator sters o utilizator deblocat o membru adaugat in grup o membru sters din grup o grup adaugat o grup sters o modificari in politicile de audit la nivel de domeniu o politica de domeniu modificata o oprirea auditului o drepturi administrative adaugate pentru un utilizator/grup o drepturi administrative sterse pentru un utilizator/grup o membru adaugat unui grup administrativ o incercare de modiciare de parola pentru cont administrativ o autentificare reusita la ore nenormale o evenimente multiple de access interzis o evenimente de autentificari nereusite multiple o evenimente multiple de incercari de modificare de parole o evenimente de autentificare reusita dupa cateva evenimente de autentificare nereusita o logul de audit curatat o salvare de log de audit
6	Sa permita acknowledgement si facilitati de notificare

Consolidare si Raportare

1	Sa permita consolidarea diferitelor colectii de loguri din locatii geografic diferite
2	Produsul trebuie sa contina rapoartele de securitate grupate pe standardele de securitate SOX, HIPAA, ISO17799, etc.
3	Accesul la rapoarte trebuie sa fie integrat cu platforme gen LDAP
4	Rapoartele trebuie sa aiba sursa deschisa. Acest lucru este necesar pentru a putea

	modifica rapoartele si pentru a crea noi rapoarte pe baza celor existente
5	Rapoartele trebuie sa poata fi generate si distribuite automat pe baza unei programari si pe baza continutului acestora.

Deployment si administrare:

1	Sistemul trebuie sa fie scalabil, sa permita organizarea echipamentelor monitorizate pe site-uri. Trebuie sa fie capabil sa descopere singur echipamente noi si sa le includa automat in procesul de colectare
2	Sa permita deployment rapid si usor
3	Configurarea trebuie sa fie usoara si bazata pe wizard-uri
4	Accesul la configurarea si administrarea produsului sa se faca integrat cu platforme tip LDAP

Model de licentiere

Modelul de licentiere trebuie sa nu tina cont de numarul de servere de colectare instalate, ci doar de numarul echipamentelor de pe care se face colectarea. De exemplu 20 se echipamente in aceeasi locatie cu un singur server de colectare trebuie sa fie echivalent cu 20 servere in 4 locatii diferite, fiecare cu serverul ei de colectare.

4 Demonstratie practica

Autoritatea contractanta solicita realizarea unei demonstratii practice a principalelor functionalitati ale solutiei oferite in special cu serviciul de management documente si workflow securizat. Demonstratia practica se va realiza la sediul autoritatii contractante, pentru ofertele declarate conforme. Autoritatea contractanta va comunica in scris detaliile privind realizarea demonstratiei, cu minim 5 zile lucratoare inainte de data realizarii demonstratiei.

Demonstratia practiva va viza caracteristicile solutiei oferite pentru serviciul de management documente si workflow securizat cu accent pe:

- Autentificarea utilizatorilor folosind aplicatia gateSAFE
- Managementul ciclului de viata al documentelor
- Indexarea automata a continutului documentelor in format text
- Lucrul in comun pe documente
- Managementul fluxurilor de lucru
- Fluxuri de lucru pe terminale mobile
- Managementul sarcinilor

- Arhivarea documentelor
- Registratura electronica
- Mesagerie organizationala si notificari
- Indicatori si rapoarte specifice
- Utilizarea serviciului de marcare temporala pentru documente

5 Mentenanta si sustenabilitate

Pentru intretinerea sistemului livrat in gama performantele optime se vor oferta atat servicii de mentenanta preventiva cat si corectiva.

5.1 Servicii de mentenanta preventiva

5.1.1 Servicii pentru aplicatiile software

In vederea asigurarii parametrilor de performanta ai sistemului acordarea serviciilor de mentenanta pentru toate modulele sistemului.

Acest pachet de servicii se adreseaza urmatoarelor componente:

- Sistem de operare
- Server baza de date
- Componente software (aplicatii, servicii, portal, etc.)

Pentru fiecare din aceste componente se vor efectua urmatoarele tipuri de activitati:

- Monitorizare componente
- Prelevare de esantioane de date privind functionarea acestora si analizarea acestora pentru identificarea de indicii privind o posibila degradare a performantei
- Efectuarea de optimizari asupra componentelor la nivel de cod, script sau consola pentru a asigura functionarea sistemului in parametrii optimi;
- Configurarea politicilor de securitate, a listelor de control a accesului

5.1.1.1 Sistem operare

Sistemul de operare prezinta un important punct in buna-functionare a sistemului gestionand resursele sistemului si ruland toate componentele acestuia.

Monitorizarea acestuia presupune verificarea log-urile sistemului pentru identificarea eventualelor probleme, verificarea functionarii serviciilor si aplicatiilor prin intermediul utilitarelor de sistem. Pentru identificarea eventualelor probleme de performanta se vor extrage la diverse perioade de timp informatii de tip Performance Counters menite sa ofere o viziune de ansamblu asupra functionarii sistemului si a alocarii resurselor. Astfel se pot identifica si eventuale necesitati de upgrade hardware

ale sistemului, caz in care se vor prezenta Beneficiarului sugestii privind extinderea sau organizarea platformei hardware.

Pentru a asigura buna-functionare si protectia sistemului se vor evalua regulat actualizarile disponibile prin mecanisme de update si se vor instala cele ce aduc un real beneficiu si ce nu interfereaza intr-un mod negativ cu functionarea sistemului.

Din punct de vedere proactiv, se va realiza verificarea privind functionarea corespunzatoarea a:

- Bazei de date prin analiza incarcarii procesoarelor, timpilor de executie a principalelor tipuri de tranzactii, timpi de asteptare, analiza si verificarea logurilor sistemului de operare de erori, spatiu pe disc, incarcare memorie RAM, verificarea dimensiunilor fiserelor de baze de date;
- Serverelor de aplicatie – analiza si verificarea logurilor sistemului de operare de erori, incarcarii procesoarelor, spatiu pe disc, incarcare memorie RAM;
- Echipamente de comunicatii – analiza informatiilor privind tranzactiile procesate, verificarea logurilor de erori;
- Solutia de backup – se va analiza corectitudinea efectuarii tuturor job-urilor de backup atat la nivel aplicativ cat si la nivelul sistemului de operare

5.1.1.2 Server baza de date

Se vor monitoriza urmatoarele aspecte ale functionarii bazei de date:

- verificarea job-urilor
- verificarea secventei de backup
- urmarirea alertelor
- verificarea si refacerea indecsilor pentru a asigura timpi de rulare cat mai scurti pentru activitatile critice
- verificarea regulata a consistentei bazei de date
- se va verifica dimensiunea bazei de date si se va evalua necesitatea cresterii spatiului alocat acesteia

Pentru a identifica eventuale scaderi de performanta se vor alege ferestre de timp in pe parcursul functionarii sistemului si se vor extrage statistici de functionare folosind Performance Counters sau unelte de tip Profiler, putand astfel identifica si remedia comenzile SQL non-optime. In cazul intampinarii unor situatii in care platforma privita ca intreg nu poate da randamente mai bune se vor sugera mecansime alternative de utilizare:

- modificarea functionalitatii astfel incat sa isi pastreze utilitatea dar sa poate rula intr-un timp mai scurt (exemplu fiind rularea anumitor calcule pe perioade mai scurte, sau spargerea unor rapoarte in cateva subtipuri permitand astfel optmizarea separata pe diverse scenarii)

- extinderea platformei hardware sau, dupa caz, a resurselor

5.1.1.3 Componente software

Monitorizarea acestor componente presupune urmarirea functionarii:

- fiecarei entitati software distincte
- serverului web si a serverului de aplicatie
- log-urilor de activitate si de eroare

In cazul identificarii de functionalitati cu timp nejustificat de mare de incarcare se vor efectua activitati specifice de optimizare, precum: modificare mecanisme software, optimizare scripturi SQL etc.

5.2 Servicii de mentenanta corectiva

5.2.1 Identificarea si remedierea disfunctionalitatilor

Pentru a permite gestionarea si urmarirea disfunctionalitatilor semnalate de beneficiar fiecare observatie va fi consemnata utilizand documente de interventii. Un document va contine o singura disfunctionalitate. Dupa completare, documentul va fi transmis catre FURNIZOR spre rezolvare utilizand elementele de contact transmise (persoana, telefon, email).

Pentru fiecare disfunctionalitate se va asocia un anumit grad de severitate tinand cont de impactul disfunctionalitatii asupra functionarii aplicatiei software in ansamblu. In cele ce urmeaza sunt detaliate tipurile de severitate.

- “Severitate 1” – identifica o problema critica (“critical fault”) care are un impact foarte mare asupra functionalității. In acest caz, sistemul nu este utilizabil, rezultând un impact critic în operații.
- “Severitate 2” - identificat o problema care are un impact mare asupra functionalității. In acest caz, sistemul este utilizabil dar cu anumite limitări.
- “Severitate 3” - identifica o problema care are un impact mediu asupra functionalității. In acest caz, sistemul este utilizabil cu excepția unor funcționalități mai puțin semnificative (necritice pentru operații).
- “Severitate 4” - identifica o problema care are un impact minim asupra functionalității. In acest caz, problema are un impact minor în operații sau permite implementarea unei izolari rezonabile.

Furnizorul va confirma nivelul de severitate al unei disfunctionalitati utilizand timpii de raspuns specificati in tabelul de mai jos.

Niveluri de severitate	Timpi de interventie pe niveluri de severitate	
	Solutie provizorie	Rezolvare
1	6 ore lucratoare*	2 zile lucratoare
2	1 zi lucratoare	4 zile lucratoare
3	3 zi lucratoare	6 zile lucratoare
4	nu este cazul	20 zile lucratoare

* Orele lucratoare se incadreaza in intervalul 9.00-17.00 aferent zilelor lucratoare

Activitatile desfasurate in vederea atingerii obiectivelor stabilite pentru acest pachet de servicii sunt:

1. Asigurarea unui serviciu de help-desk pentru inregistrarea solicitarilor. Acest serviciu va fi disponibil in intervalul 8:30 – 18:30. Solicitările se vor primi prin e-mail sau telefonic si vor fi confirmate telefonic. La rezolvarea defectului, solicitarea va fi inchisa dupa caz, in help-desk si/sau prin raportul de activitate. Informarea privind activitatile intreprinse se va realiza prin e-mail sau telefonic.
2. Diagnosticarea defectelor:
    - In momentul solicitării serviciului solicitantul trebuie să furnizeze datele necesare pentru identificarea problemei.
    - Catalogarea defectului in unul din cele 4 niveluri de severitate.
    - Replicarea defectului – replicarea şi identificarea defectului şi a situaţiei exacte în care acesta s-a produs;
    - Consultarea logurilor în vederea identificării cauzei care a produs incidentul
    - Se va furniza o rezolutie privind incidentul.
    - In cazul in care disfunctionalitatea defectul nu are drept sursa sistemul ci alte aplicatii externe acesteia, se vor indica surse posibile de defect si de remediere
3. Remedierea defectelor si verificarea eliminarii disfunctionalitatilor;

5.2.1.1 Remedierea disfunctionalitatilor datorate aplicatiilor software

In cazul in care disfunctionalitatea este datorata aplicatiilor software se va demara procesul de corectarea a acesteia. In cazul in care defectul are ca rezultat generarea unui patch sau a unei noi versiuni de aplicatie se va realiza si:

- Testarea noii versiuni de aplicatie care corecteaza defecturl
- Instalarea noii versiuni de aplicatie pe un sistem de test si realizarea testelor specifice
- Instalarea noii versiuni de aplicatie pe sistemul de productie
- Urmarirea sistemului de productie pentru a asigura eliminarea problemei

5.2.2 Asistenta tehnica

Inregistrarea solicitarii de asistenta tehnica va fi facuta prin serviciul de help-desk pus la dispozitia Beneficiarului. Acest serviciu va fi disponibil in intervalul 8:30 – 18:30. Solicitările se vor primi prin e-mail sau telefonic si vor fi confirmate telefonic.

Aceste pachet de servicii contine urmatoarele:

- asistenta in utilizarea componentelor software ale sistemului;
- furnizarea de asistență tehnică pentru componentele de infrastructura software;

5.2.3 Recuperare in caz de dezastru

Pentru a permite repunerea in functiune a sistemului in cel mai scurt timp si pentru a adresa cerintele de inalta disponibilitate specifice sistemului, in cadrul acestui pachet se vor efectua operatiile specifice de restaurare a sistemului in cel mai scurt timp.

Restaurarea va fi facuta pe baza datelor si a echipamentelor puse la dispozitie, in conditiile in care planul de backup inmanat Beneficiarului a fost respectat cu strictete.Operatiile de restaurare a sistemului vor incepe indata ce datele si echipamentele for fi puse la dispozitie de catre Beneficiar, iar timpii asumati pentru efectuarea restaurarii vor fi masurati de la inceperea acestor operatii.

La sfarsitul reviziei tehnice in caz de a locatiei respective se va completa si semna un Raport de Mentenanta Periodica in care se vor trece in mod obligatoriu rezultatele verificării şi acțiunile recomandate pentru a îmbunătăți disponibilitatea sistemului.

Coordonator proiect – Delia POPESCU
Manager de proiect – Mirela TOMA
Asistent coordonator – Roxana POPESCU
Responsabil implementare IT – Gabriel – Catalin DUMITRU
Responsabil financiar – Alexandra COSTACHE