Oficiului Naţional de Prevenire şi
Combatere a Spălării Banilor

1509
08 MAR. 2022

Aprob,

Propun aprobarea

CAIET DE SARCINI
Servicii mentenanţă şi asistenţă tehnică

1. Introducere

Oficiul National de Prevenire si Combatere a Spalarii Banilor cu sediul in Str. Ion Florescu, nr. 1, sector 3, Bucuresti îndeplineşte rolul de Autoritate contractantă pentru procedura de achizitie care face obiectul prezentului caiet de sarcini.

2. Contextul realizării acestei achiziţii de produse

2.1. Informaţii despre Autoritatea contractantă

Oficiul National de Prevenire si Combatere a Spalarii Banilor este Unitatea de Informatii Financiare a Romaniei de tip administrativ, cu rol de lider in elaborarea, coordonarea si implementarea sistemului national de combatere a spalarii banilor si finantarii terorismului.

Functiile de baza ale Oficiului National de Prevenire si Combatere a Spalarii Banilor, in conformitate cu prevederile legale in materie, respectiv Legea nr. 129/2019 si H.G. nr. 491/2021 sunt urmatoarele:

- Primirea, analizarea, prelucrarea si diseminarea informatiilor cu caracter financiar. in cazurile in care din analiza datelor si informatiilor prelucate la nivelul institutiei, rezulta indicii temeinice cu privire la spalare a banilor sau de finantare a terorismului, Oficiul informeaza de indata Parchetul de pe langa inalta Curte de Casatie si Justitie. Oficiul informeaza de asemenea Serviciul Roman de Informatii cu privire la suspiciuni de finatare a terorismului, sau organele de urmarire penala cu privire la indicii de savarsire a altor infractiuni decat cele de spalare a banilor sau de finantare a terorismului, in conformitate cu prevederile legii. Aceasta activitate constituie functia de diseminare a informatiilor catre autoritatiile competente
- Supravegherea si controlul entitatilor raportoare, conform legii, in scopul prevenirii si combaterii spalarii banilor si finantarii terorismului;

- Oficiul este autoritate competenta in domeniul punerii in aplicare a sanctiunilor internationale, in conformitate cu dispozitiile Ordonantei de Urgenta a Guvernului nr. 202/2008 privind punerea in aplicare a regimului sanctiunilor internationale, aprobata prin Legea nr.217/2009 cu modificarile si completarile ulterioare;
- Prevenirea si combaterea finantarii actelor de terorism. Oficiul, prin atributiile conferite de legislatia in materie, are un rol important in prevenirea si combaterea finantarii actelor de terorism, fapt ce a determinat ca institutia sa fie parte componenta a Sistemului National de Prevenire si Combatere a Terorismului (S.N.P.C.T.), participand activ, potrivit competentelor sale, atat la activitatea de stopare a unor eventuale fluxuri de finantare a gruparilor teroriste, cat si la analizarea si evaluarea riscurilor la care se expun entitatile raportoare.
- Primirea, procesarea si analiza cererilor de informatii. In scopul efectuarii unor analize complexe, cat mai ample care implica tranzactii financiare cu elemente de extraneitate.

2.2. Informaţii despre contextul care a determinat achiziţionarea produselor

Contractul de mentenanta si asistenta tehnica care se desfasoara in prezent se va incheia la data de 30.04.2022, fiind necesara incheierea unui contract nou care sa ne asigure buna functionare a sistemului pana la sfarsitul anului 2022 cu posibilitatea prelungirii prin act aditional pe o perioada de maxim 4 luni.

2.3. Informaţii despre beneficiile anticipate de către Autoritatea contractantă

Serviciile de mentenanta si asistenta tehnica vor mentine sistemul de raportare on-line complet funcțional, actualizat conform prevederilor legale și accesibil tuturor beneficiarilor, în permanenta, asigura evitarea pierderii informațiilor vitale, ce ar putea aduce instituției prejudicii de imagine, de ordin financiar sau de alta natura.

3. Descrierea produselor solicitate

3.1. Descrierea situaţiei actuale la nivelul Autorităţii/entităţii contractante

Sistem Electronic de Transmitere Date on-line al ONPCSB are doua componente: una accesibila prin internet care este destinata raportorilor non-bancari si una accesibila in reteaua de comunicatii interbancare, destinata raportorilor bancari. Sistemul de operare al celor doua servere corespunzatoare celor doua componente este Windows 2008 R2. Aplicatia Sistem Electronic de Transmitere Date a fost pusa in functiune in anul 2010, a fost dezvoltata utilizand PHP, Zend Framework, Java, si utilizeaza ca baza de date MySQL.

De-a lungul timpului au fost incheiate contracte pentru mentenanta si dezvoltare cu diverse firme astfel incat in momentul de fata structura sistemului este una eterogena ca urmare a viziunilor diferite pe care le-au avut prestatorii acestor servicii.

3.2. Obiectivul general la care contribuie furnizarea produselor

Prin contractarea serviciilor de mentenanta si asistenta tehnica cerute prin prezenta documentatie de achizitie, ONPCSB urmareste asigurarea securitatii sistemului de raportare on-line, actualizarea conform prevederilor legale, mentinerea acestuia in conditii optime de functionare si adaptarea lui la tehnologiile actuale.

3.3. Obiectivul specific la care contribuie furnizarea produselor

Conform legii nr. 129/2019, ONPCSB pune la dispozitia entităţilor raportoare un canal prin care acestea sa transmita rapoartele prevazute de lege, numai în format electronic. Acest sistem trebuie sa fie functional, adaptat specificului fiecarei categorii de entitati raportoare si disponibil permanent.

3.4. Produsele solicitate şi operaţiunile cu titlu accesoriu necesar a fi realizate

Produselor care vor fi achiziţionate sunt servicii de mentenanta si asistenta tehnica pentru sistemul de raportare on-line.

3.4.1. Principalele activităţi care se prestează sunt:

3.4.1.1. Mentenanţă

3.4.1.1.1. Servicii de mentenanţă preventivă

Activităţile de mentenanţă preventivă au ca scop prevenirea apariţiei oricărui inconvenient sau a oricărei întreruperi în funcţionarea sistemelor. Activităţile de mentenanţă preventivă sunt activităţi planificate periodic de verificare a stării de funcţionare a serverelor, a aplicaţiilor şi a bazelor de date utilizate, precum şi de realizare a copiilor de siguranţă ale acestora.

Înainte de efectuarea operaţiunilor de mentenanţă preventivă, contractantul comunică autorităţii contractante lista operaţiunilor de mentenanţă care trebuie efectuate. Este posibil ca mentenanţa preventivă să trebuiască a fi realizată în afara orelor normale de lucru sau la sfârşit de săptămână sau în sărbători legale. Operaţiunile de mentenanţă preventivă care necesită o oprire a functionarii, se efectuează in zile si intervale de timp ce vor fi agreate de comun acord.

După fiecare intervenţie preventivă, contractantul trebuie sa efectueze teste de funcţionare ale produsului şi să prezinte un raport care să includă activităţile realizate si rezultatele testelor.

3.4.1.1.2. Servicii de mentenanţă corectivă

Activităţile de mentenanţă corectivă sunt activităţi derulate pentru corectarea unei defecţiuni manifestate sau în curs de manifestare în cadrul sistemelor. Au rolul de a reduce cât mai mult posibil timpii de nefuncţionare sau de funcţionare defectuoasă a sistemelor şi de a înlătura deserviciile cauzate utilizatorilor finali de anomaliile existente la nivelul sistemului. Furnizorul va investiga erorile şi dificultăţile care apar în funcţionarea aplicaţiei informatice pentru identificarea cauzelor care le determină, în vederea remedierii acestora.

Mentenanta corectiva pentru sistemul de raportare poate include activitati precum cele exemplificate in continuare, fara a se limita la acestea:

1. Operationalizarea transmiterii rapoartelor de transferuri externe de corectie si de completare
2. Aplicarea in mod unitar a regulilor de validare a informatiilor similar din sectiuni diferite ale rapoartelor
3. Rezolvarea problemelor generate de numele utilizatorilor (de exemplu: nume care contin spatii sau utilizatori care au acelasi nume)

4. Corectarea modului de editare al anumitor sectiuni din raportul de tranzactii suspecte in sensul permiterii stergerii si/sau modificarii informatiilor introduse

Exemplele sunt prezentate pentru ca ofertantii sa evalueze corect complexitatea si volumul activitatilor pe care urmeaza sa le desfasoare.

Dacă este cazul, furnizorul va folosi copiile de siguranță pentru restaurarea bazei de date și a aplicațiilor.

Furnizorul va asigura menținerea instrucțiunilor de folosire a aplicațiilor (Ajutor) în conformitate cu modul curent de funcționare.

3.4.1.1.3. Servicii de mentenanţă evolutivă

Activităţile de mentenanţă evolutivă sunt sunt activităţi de actualizare a aplicațiilor care constau în furnizarea de versiuni noi, în vederea satisfacerii solicitărilor de implementare a unor noi funcţionalităţi, reguli de business noi sau modificate, precum şi alte adaptări necesare datorită schimbărilor legislative, administrative sau procedurale legate de funcţionarea sistemelor.

Mentenanta evolutivă pentru sistemul de raportare poate include activitati precum cele exemplificate in continuare, fara a se limita la acestea:

1. Adaptarea modulului de inregistrare pentru transmiterea automata a credentialelor de acces; trimiterea parolelor catre entitatile raportoare neactivate pana in prezent pe adresele de e-mail completate la inregistrare de catre acestea.
2. Actualizarea formularelor generate la inregistrare pentru alocare cont si comunicare credentiale de acces
3. Implementarea unei proceduri de editare, upload si validare pentru raportul de transfer de fonduri
4. Implementarea unui modul de interfata pentru editarea unui format simplificat de raport de tranzactii suspecte destinat entitatilor nonbancare

Exemplele sunt prezentate pentru ca ofertantii sa evalueze corect complexitatea si volumul activitatilor pe care urmeaza sa le desfasoare.

Modificarile vor fi dezvoltate intr-un mediu de test si vor fi aplicate in mediul de productie dupa acceptarea acestora de catre reprezentantii beneficiarului.

Documentatia „Ajutor" a sistemului va fi actualizata in concordanta cu modificarile efectuate.

3.4.1.1.4. Servicii de mentenanţă adaptivă

Activităţile de mentenanţă adaptivă sunt activităţi de adaptare a software-ului aferent sistemelor care constau în actualizarea acestora, cu scopul de a le păstra funcţionalitatea, disponibilitatea şi de a le îmbunătăţi performanţele în condiţiile unor modificări intervenite în mediul în care rulează. Modificările pot fi la nivelul platformei hardware şi/sau software pe care este instalată soluţia.

3.4.1.2. Activităţi de instalare şi configurare

În vederea îndeplinirii obiectivului prevăzut de contract, în situaţiile în care activităţile de mentenanţă sunt însoţite de actualizări ale sistemelor dezvoltate, vor fi desfăşurate activităţi de instalare şi configurare a soluţiei, ori de câte ori este necesar.

De asemenea, Contractantul va realiza actualizarea certificatelor de Securitate pe serverele care fac obiectul contractului.

3.4.1.3. Activităţi de testare

După fiecare modificare minoră sau majoră care are loc în program se va realiza testarea unor aspecte cum ar fi: funcționarea, integritatea, performanţa, securitatea aplicaţiei, etc.

3.4.1.4. Servicii de suport tehnic

Serviciile de suport tehnic sunt activităţi de preluare şi soluţionare a tuturor cererilor de suport care apar în contextul derulării contractului.

Pe toata durata contractului, în perioada de garanţie, Contractantul va asigura suport tehnic pentru problemele aparute in exploatarea sistemelor, atat la nivelul Autoritatii contractante cat si la nivelul entitatilor raportoare.

Contractantul va asigura un punct de contact dedicat personalului autorizat al Autorităţii/entităţii contractante unde se poate semnala orice problemă/defecţiune care necesită suport tehnic în gestionarea unui incident, disponibil, pentru a se asigura că orice situaţie semnalată este tratată cu promptitudine. Pentru buna gestionare a activitatilor si incidentelor se va utiliza un sistem de ticketing care va asigura notificarea in timp real (prin e-mail sau sms).

Contractantul va răspunde în timp util la orice incident semnalat de Autoritatea contractantă, în funcţie de nivelul de prioritate. Fiecare incident este caracterizat de un nivel de prioritate, care va evidenţia impactul acestuia asupra funcţionalităţilor produsului.

Contractantul trebuie să asigure disponibilitatea serviciilor de suport tehnic. În cazul incidentelor cu prioritate "urgent" intervenţia va fi asigurată 24 x 7, din momentul primirii sesizării şi până la remedierea definitivă a problemei şi asigurarea funcţionalităţii integrale a produsului.

Contractantul va trebui să respecte următorii timpi de răspuns, corelaţi cu nivelul de prioritate a incidentului:

Nivel prioritate	Timp de răspuns	Timp de implementare soluţie provizorie	Timp de rezolvare
Urgent	30 minute	4 ore	24 ore
Critic	2 ore	24 ore	48 ore
Major	4 ore	Următoarea zi lucrătoare	Următoarea zi lucrătoare
Minor	6 ore	Următoarea zi lucrătoare	Următoarea zi lucrătoare

Nerespectarea timpilor de mai sus dă dreptul Autorităţii/entităţii contractante de a solicita penalităţi/daune interese în conformitate cu clauzele contractului de achiziţie publică/sectorială de produse.

In cazul interventiilor onsite, contractantul va asigura prezenta expertilor desemnati in termen de maxim 60 de minute de la semnalarea incidentului de catre beneficiar.

3.4.1.5. Servicii de optimizare

Serviciile de optimizare constau în îmbunătățirea performanței aplicațiilor. Furnizorul va face recomandări pentru a îmbunătăți performanţele aplicaţiilor şi va stabili modificările de software şi de hardware necesare, estimând costurile pe care le presupun aceste modificări.

Serviciile de optimizare pentru sistemul de raportare vor include simplificarea modului de transmitere a rapoartelor de corectie, fara a se limita la aceasta.

3.4.2. Securitatea informaţiei

Furnizorul va respecta Politica de securitate a resurselor informatice și de comunicații a ONPCSB.

În relaţia dintre Beneficiar şi Furnizorul de servicii se stabileşte contractual faptul că toate informaţiile Beneficiarului la care furnizorul are acces sunt CONFIDENŢIALE.

Informațiile vor fi folosite numai în scopul îndeplinirii sarcinilor contractuale și nu vor fi divulgate unor terți.

3.4.3. Prestarea serviciilor

Autoritatea contractanta solicita disponibilitatea on-line sau on-site, după caz, în zilele lucrătoare, de luni pana vineri, timp de 4 ore, a unui specialist care sa asigure serviciile mai sus menționate și respectarea, fără excepție, a termenelor de remediere a incidentelor, pe perioada derulării contractului.

Pentru expertii care vor asigura serviciile solicitate se vor prezenta documente care sa ateste studii de specialitate, certificari si experienta in proiecte similare, pe tehnologia folosita la nivelul sistemului de raportare.

Furnizorul trebuie să dețină certificat ISO 9001.

DEFINIŢII

Politica de securitatea resurselor informatice şi de comunicaţii reprezintă totalitatea măsurilor necesare pentru asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

- Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate;
- Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat;
- Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor sistemului.
-

Timp de remediere. Prin timp de remediere părţile înţeleg timpul scurs între momentul în care BENEFICIARUL notifică FURNIZORUL asupra apariţiei unui incident în legătură cu sistemul de raportare on-line si/sau a website-ului şi momentul în care Furnizorul repune sistemul în stare de funcţionare la parametrii conveniţi.

Incident de nivel minor reprezintă o eroare care afectează o funcţie sau proces, dar funcţionarea întregului sistem nu este afectată sau este afectată nesemnificativ. Impactul este minim, riscul ca activitatea să nu se desfăşoare normal este practic inexistent.

Incident de nivel major reprezintă o eroare apărută la o funcţie sau proces, care afectează într-o mare măsură funcţionarea întregului sistem de raportare on-line si/sau a website-ului. Poate avea impact asupra proceselor de business ale Beneficiarului. Există riscul ca incidentul să se extindă.

Incident de nivel critic reprezintă o eroare care afectează majoritatea funcţionalităţilor sistemului de raportare on-line sau a funcţiilor principale. Impact foarte mare asupra mediului intern şi extern. Risc mare privind: neexecutarea în termen a activitatilor specifice Beneficiarului, deteriorarea imaginii Beneficiarului în relaţiile cu entitatile raportoare.

Incident de nivel urgent reprezintă un incident de nivel critic pentru care nu există soluţii alternative (workaround) care pot fi aplicate. Impact foarte mare asupra mediului intern şi extern. Risc mare privind: neexecutarea în termen a lucrărilor, deteriorarea imaginii Beneficiarului în relaţiile cu institutiile partenere si entitatile raportoare.