Vizualizare anunt

PUBLICAT | NR ANUNT: ADV1111426 | TIP ANUNT: CUMPARARI DIRECTE | DATA CREARE: 22.10.2019 09:43 | DATA PUBLICARE: 22.10.2019 09:44

DATE IDENTIFICARE AUTORITATE CONTRACTANTA

Denumire oficiala: OFICIUL NATIONAL DE PREVENIRE SI COMBATERE A SPALARII BANILOR CIF: 11806010

Adresa: Strada General Ion Florescu, Nr. 1, Sector: 3 Tara: Romania

Tel: +40 213155207 Fax: +40 213155227 E-mail: onpcsb@onpcsb.ro Punct(e) de contact: Veronica Rata In atentia: : Veronica Rata

ANUNT

Denumire contract:

SERVICII MENTENANTA SI ASISTENTA TEHNICA SROL si SITE ONPCSB

Data limita depunere oferta:

28.10.2019 09:36

Tip anunt:	Tip contract:	Cod si denumire CPV:	Valoare estimata:	Caiet de sarcini:
Cumparari directe	Servicii	72611000-6 - Servicii de asistenta tehnica informatica (Rev.2)	6.386,54 RON	**Caiet de sarcini mentenanta.pdf**

Descriere contract:

contractul va fi incheiat pentru perioada 01 noiembrie-31 decembrie 2019

Conditii referitoare la contract:

cf caiet de sarcini

Conditii de participare:

cf caiet de sarcini

Criterii de atribuire:

PRETUL CEL MAI SCAZUT

Informatii suplimentare:

oferta va fi trimisa pe adresa de mail: economic@onpcsb.ro

Vizualizare anunt

PUBLICAT NR ANUNT: ADV1111426 TIP ANUNT: CUMPARARI DIRECTE DATA CREARE: 22.10.2019 09:43 DATA PUBLICARE: 22.10.2019 09:44

Aprob,
PREȘEDINTELE
Oficiului Național de Prevenire și Combatere a Spălării Banilor,
DANIEL- MARIUS STAICU

CAIET DE SARCINI

Servicii mentenanță și asistență 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 achiziții de produse

2.1. Informații 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. 1599/2008, sunt urmatoarele:

- Colectarea, procesarea si analiza informatiilor financiare. In conditiile in care, din analiza datelor si informatiilor prelucrate la nivelul institutiei, rezulta indicii temeinice cu privire la spalarea banilor, Oficiul sesizeaza de indata Parchetul de pe langa Inalta Curte de Casatie si Justitie, iar in situatia in care se constata finantarea unor acte de terorism, institutia noastra sesizeaza de indata si Serviciul Roman de Informatii cu privire la operatiunile suspecte de finantare a actelor de terorism, in conformitate cu prevederile legii speciale, fiind astfel conturata functia de diseminare a informatiilor catre autoritatile competente;

- Supravegherea, verificarea si controlul entitatilor raportoare care nu sunt supravegheate de o alta autoritate de supraveghere prudentiala, a carei implementare consta in totalitatea activitatilor de evaluare si monitorizare sistematica a indicatorilor de risc de spalare de bani;

- Functia Oficiului de factor responsabil in procesul de implementare a regimului sanctiunilor internationale, urmare intrarii in vigoare a Legii nr. 217/2009 pentru aprobarea O.U.G. nr.202/2008 privind punerea in aplicare a regimului sanctiunilor internationale, luand in considerare calitatea sa de supraveghetor pentru acele entitati raportoare care nu au o autoritate de supraveghere prudentiala, conform legii speciale;

- 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. Informații despre contextul care a determinat achiziționarea produselor

Contractul de mentenanta si asistenta tehnica incheiat pentru anul in curs a fost reziliat si este necesara asigurarea acestor servicii in continuare.

Ca urmare a promulgarii Legii Nr. 129 din 11 iulie 2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative au fost modificate limitele si termenele de raportare si sunt in curs de elaborare noi norme privind forma si continutul rapoartelor.

2.3. Informații despre beneficiile anticipate de către Autoritatea contractantă

Serviciile de mentenanta si asistenta tehnica vor mentine sistemul de raportare on-line si web-site-ul ONPCSB complet funcționale, actualizate și accesibile tuturor beneficiarilor, în permanenta, pentru evitarea pierderii informațiilor vitale, ce ar putea aduce instituției prejudicii de imagine, de ordin financiar, etc.

3. Descrierea produselor solicitate

3.1. Descrierea situației actuale la nivelul Autorității/entității contractante

Sistemul de raportare on-line al ONPCSB are doua componente: una conectata la internet care este destinata raportorilor non-bancari si una conectata in reteaua de comunicatii interbancare destinata raportorilor bancari. Sistemul de operare instalat pe cele doua servere corespunzatoare celor doua componente este Windows 8 R2. Sistemul de Raportare on-line a fost dezvoltat în PHP, Zend Framework, Java, are baza de date MySQL si a fost pus in functiune in anul 2010.

Web-site-ul este realizat in PHP + HTML + CSS.

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 si a web-site-ul ONPCSB, actualizarea, mentinerea acestora in conditii optime de functionare si adaptarea lor la tehnologiile actuale.

3.3. Obiectivul specific la care contribuie furnizarea produselor

Conform legii nr. 129/2019, ONPCSB trebuie sa puna 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.

Web-site-ul ONPCSB este platforma prin care oficiul prezinta informatiile de interes public privind activitatea proprie si pune la dispozitia entitatilor interesate informatiile necesare in scopul conformarii prevederilor legale privind prevenirea si combaterea spalarii banilor si finantarii terorismului. Site-ul trebuie, de asemenea, sa fie permanent functional si accesibil.

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 si web-site-ul ONPCSB.

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 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 produsului 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.

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

Timpul de remediere, este stabilit în funcție de gravitatea incidentului, astfel:

- Incident de nivel minor – maxim 3 zile lucrătoare
- Incident de nivel major – maxim o zi lucrătoare
- Incident de nivel critic – maxim 6 ore (program de lucru)
- Incident de nivel urgent – maxim 3 ore (program de lucru)

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

3.4.1.1.3. Servicii de mentenanță evolutivă

Activitățile de mentenanță evolutivă sunt activități de actualizare a aplicațiilor care constau în furnizarea de versiuni noi, în vederea satisfacerii solicitărilor de implementare a unor noi funcționalități, reguli de business noi sau modificate, precum și alte adaptări necesare datorită schimbărilor legislative, administrative sau procedurale legate de funcționarea sistemelor.

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 mentenanță adaptivă

Activitățile de mentenanță adaptivă sunt activități de adaptare a software-ului aferent sistemelor care constau în actualizarea acestora, cu scopul de a le păstra funcționalitatea, disponibilitatea și de a le îmbunătăți performanțele în condițiile unor modificări intervenite în mediul în care rulează. Modificările pot fi la nivelul platformei hardware și/sau software pe care este instalată soluția.

3.4.1.2. Activități de instalare și configurare

În vederea îndeplinirii obiectivului prevăzut de contract, în situațiile în care activitățile de mentenanță sunt însoțite de actualizări ale sistemelor dezvoltate, vor fi desfășurate activități de instalare și configurare a soluției, ori de câte ori este necesar.

3.4.1.3. Activități de testare

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

3.4.1.4. Servicii de suport tehnic

Serviciile de suport tehnic sunt activități de preluare și soluționare a tuturor cererilor de suport care apar în contextul derulării contractului.

Pe toata durata contractului, în perioada de garanţie, Contractantul va asigura suport tehnic.

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.

Contractantul va răspunde în timp util la orice incident semnalat de Autoritatea contractantă, în funcţie de nivelul incidentului. 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.

3.4.1.5. Servicii de optimizare

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

3.4.2. Securitatea informaţiei

Furnizorul va respecta **Politica de securitate a resurselor informatice şi de comunicaţii** a beneficiarului.

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

Informaţiile vor fi folosite numai în scopul îndeplinirii sarcinilor contractuale şi nu vor fi divulgate unor terţi.

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 menţionate şi respectarea, fără excepţie, a termenelor de remediere a incidentelor, pe perioada derulării contractului.

Pentru specialistul care va asigura serviciile solicitate se vor prezenta documente care sa ateste studii de specialitate si experienta in proiecte similare.

Avand in vedere ca una din componentele sistemului de raportare al ONPCSB este accesibila exclusiv d in Reteaua de Comunicatii Interbancare operata de Banca Nationala a Romaniei, furnizorul de servicii de mentenata trebuie sa detina o conventie valabila cu BNR privind conectarea la aceasta retea. In acest sens vor fi prezentate documente doveditoare.

Furnizorul trebuie să deţină certificat ISO 9001 si ISO 14001.

DEFINIŢII

Politica de securitate a 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 si/sau a website-ului sau a funcţiilor principale. Impact foarte mare asupra mediului intern şi extern. Risc mare privind: neexecutarea în termen a lucrărilor, 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 relațiile cu business-ul, pierderea imaginii pozitive a Beneficiarului în relația cu entitatile raportoare.

Director DTIS : Mircea Pascu

Sef serviciu STI: Marius Dumitriu

Analist financiar: Mihaela Dăescu