Caiet de sarcini pentru achiziția de

Echipamente, servicii de suport și licențe, destinate infrastructurii de comunicații și securitate IT.

1 Introducere

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Caietul de sarcini conține, în mod obligatoriu, specificații tehnice. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni, precum și sisteme de asigurare a calității, terminologie, simboluri, teste și metode de testare, ambalare, etichetare, marcare, condițiile pentru certificarea conformității cu standarde relevante sau altele asemenea.

În cadrul acestei proceduri, MINISTERUL FINANȚELOR PUBLICE îndeplinește rolul de Autoritate contractantă , respectiv Autoritatea contractantă în cadrul Contractului.

Orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

Ofertele care nu îndeplinesc toate cerințele minimale vor fi declarate neconforme. Nu se acceptă depunerea de oferte alternative. Nu se admit ofertele parțiale din punct de vedere cantitativ și calitativ, ci numai ofertele integrale, care corespund tuturor cerințelor stabilite prin prezentul caiet de sarcini. Orice ofertă care se abate de la cerințele minimale va fi considerată admisibilă numai în condițiile în care aceasta asigură un nivel calitativ superior cerințelor minimale.

În conformitate cu regulile de elaborare a documentației de atribuire din Legea nr. 98/2016, privind achizițiile publice, cu modificările și completările ulterioare, art. 156, alin (2) și (3), specificațiile tehnice din prezentul Caiet de sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate și care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică se consideră a fi însoțite de cuvintele “sau echivalent”, indiferent dacă aceste cuvinte sunt prevăzute expres sau nu în prezentul document.

2 Contextul realizării acestei achiziții de produse

2.1 Informații despre Autoritatea contractantă

Ministerul Finanțelor Publice este un minister cu rol de sinteză, care se organizează și funcționează ca organ de specialitate al administrației publice centrale, cu personalitate juridică, în subordinea Guvernului, care aplică strategia și Programul de guvernare în domeniul finanțelor publice.

Ministerul Finanțelor Publice aplică Programul de guvernare și contribuie la elaborarea și implementarea strategiei în domeniul finanțelor publice, în exercitarea administrării generale a finanțelor publice, asigurând utilizarea pârghiilor financiare, în concordanță cu cerințele economiei de piață și pentru stimularea inițiativei operatorilor economici.

Ministerul Finanțelor Publice îndeplinește toate atribuțiile și are toate competențele conferite prin legi sau prin alte acte normative în vigoare, monitorizează și coordonează atribuțiile conferite de lege unităților subordonate.

Sediul principal al Ministerului Finanțelor Publice este în municipiul București, Bulevardul Libertății nr. 16, sectorul 5. Ministerul Finanțelor Publice își desfășoară activitatea și în alte sedii deținute potrivit legii.

Informații suplimentare despre Autoritatea Contractantă, Ministerul Finanțelor Publice, se pot regăsi pe site-ul web oficial al instituției: www.mfinante.gov.ro.

2.2 Informații despre contextul care a determinat achiziționarea produselor

Sistemul informatic al Ministerului Finanțelor Publice (MFP) este unic în România atât din punct de vedere al complexității și specificității aplicațiilor, cât și al numărului de entități ale administrației publice și entități private deservite, precum și al întinderii teritoriale. Numărul de aplicații informatice, volumul de date, numărul de entități deservite și numărul de utilizatori interni și externi crește permanent, crescând implicit și volumul de muncă depusă, precum și necesarul de resurse pentru dezvoltarea și administrarea sistemului informatic. Actualmente sistemul informatic al Ministerului Finanțelor Publice este cel mai mare furnizor de date din România pentru instituțiile publice și instituțiile financiare din România și din străinătate.

Sistemul Informatic Integrat Vamal este destinat să asigure desfășurarea eficientă a activităților din domeniul vamal, fiind o componentă esențială a sistemului informatic al Ministerului Finanțelor Publice.

Sistemul Informatic Integrat Vamal este cea mai importantă verigă tehnologică necesară pentru funcționarea sistemului vamal din România. Sistemul Informatic Integrat Vamal este un conglomerat de mai multe sisteme, unele implementate în parteneriat cu structurile responsabile din cadrul ANAF/MFP, care trebuie să asigure adaptarea sistemelor TIC cu noile cerințe ale Comisiei Europene și ale utilizatorilor (numărul acestora fiind în continuă creștere). Sistemul Informatic Integrat Vamal este un sistem de importanţă strategică, ce necesită o protecţie deosebită pe domeniul politicilor de securitate informatică și are un nivel ridicat de sensibilitate al datelor/informațiilor prelucrate, nefuncționalitatea acestuia având un impact major în funcționarea sistemului. Din aceste motive, este necesar să fie asigurate continuitatea funcţionării, securitatea, integritatea, și disponibilitatea datelor/informațiilor ce fac obiectul tranzacțiilor economice. Pentru excluderea riscurilor cu impact major în funcţionarea Sistemului Informatic Integrat Vamal este necesară achiziționarea la timp a soluțiilor de securitate, pentru menținerea unei infrastructuri fiabile, securizate şi de perspectivă, eliminând astfel riscurile ce pot duce la pierderi financiare la bugetul de stat.

LOT 1. **Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal**.

1.1 Servicii de suport Check Point Security Management & GW Internet și Intranet

Serviciile de suport specifice soluției de management, sunt absolut necesare pentru a garanta continuitatea serviciilor de securitate specifice Sistemului Informatic Integrat Vamal. Soluția de management asigură interfața între utilizatorii soluției (personalul responsabil cu configurarea politicilor de securitate) și software-ul integrat în echipamentele ce compun soluția de securitate. Cu ajutorul interfeței soluției de management se pot gestiona politicile de securitate configurate la nivelul clusterelor firewall ce deservesc conexiunile cu toate birourile vamale și a altor instituții, la nivelul cărora sunt configurate politicile de acces Internet/DMZ precum și soluția de conectare securizată SSL care asigură conectarea operatorilor economici la componentele Sistemului Informatic Integrat Vamal.

La nivelul acestor echipamente este integrat software specializat pentru servicii VPN, fișiere log pentru activitatea monitorizată, URL filtering, Aplication Control, Liste de control al accesului, Advanced Networking & Clustering, Network Policy Management, End Point Media Encryption, Management Portal Blade, Provision Software Blade, User Directory Blade.

Suportul Check Point Security Management & GW Internet și Intranet, a expirat la data de 08 Martie 2017.

1.2 Servicii de suport Check Point Smart 1-50 Smart Event

Soluția Check Point Smart Event asigură în timp real jurnalizarea evenimentelor de securitate. Un mare avantaj al soluției constă în faptul că jurnalizarea evenimentelor se face în mod centralizat monitorizând toate echipamentele Check Point ce compun soluția de securitate. Prin automatizarea agregării datelor și corelarea datelor din fișierele jurnal brute (foarte greu de analizat la nivel individual pe fiecare appliance) se reduce volumul de date ce trebuie analizat, se izolează și se prioritizează amenințările de securitate. Cu ajutorul soluției Smart-Event se pot efectua interogări de cautare, sortare sau filtrare a evenimentelor și generarea rapoartelor ce pot fi distribuite automat.

Suportul Check Point Smart 1-50 Smart Event a expirat la data de 08 Martie 2017.

1.3 Servicii de suport pentru soluția de conectare securizată SSL Check Point-Connectra.

În cadrul infrastructurii IT ce deservește Sistemul Informatic Integrat Vamal, sunt instalate în mod cluster două echipamente Check Point 12600 Next Generation Firewall Appliance, echipamente ce asigură conectarea securizată a operatorilor economici la Sistemul Informatic Integrat Vamal prin portalul de acces https://sslvpn.customs.ro.

Suportul pentru soluția de conectare securizată ssl, a operatorilor economici la Sistemul Informatic Integrat Vamal a expirat la data de 27 mai 2016.

LOT 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții.

Necesitatea achiziției reiese din faptul că soluția de securitate firewall existentă în cadrul Direcției Tehnologia Informației, Comunicații și Statistică Vamală a beneficiat de suport hardware și software până la data de 08.03.2017. De la data de 1 aprilie 2017, producătorul echipamentelor ce compun soluția firewall existentă nu mai furnizează servicii de suport hardware/software, echipamentele existente fiind considerate “end of support”.

Urmare a acestui fapt reiese necesitatea achiziționării unei noi soluții care să o înlocuiască pe cea existentă, cu posibilitatea asigurării integrării în infrastructura existentă, respectiv migrarea tuturor politicilor, regulilor și configurațiilor existente.

În acest sens, având în vedere gradul ridicat de complexitate tehnică al soluției, se cere derularea unui proces de consultare a pieței, Autoritatea contractantă dorind obținerea informațiilor/recomandarilor cât mai relevante cu privire la potențialele soluții tehnice pentru satisfacerea nevoii autorității contractante, atât pentru completarea caietului de sarcini în vederea inițierii procedurii de achiziție, cât și obținerea de informații cu privire la prețul estimativ al achiziției. De asemenea, este necesară o analiză a întregii infrastructuri de securitate și comunicații atât a Sistemului Informatic Integrat Vamal aflat în Centrul de Date Primar (CDP), cât și a site-ului redundat (Disaster Recovery), aflat în Centrul de Date Secundar (CDS), în vederea stabilirii soluțiilor optime din punct de vedere tehnic (echipamente /software/licențe), dar și d.p.d.v. financiar.

În cadrul procesului de consultare a pieței, Autoritatea contractantă dorește să lămurească unele aspecte pentru evitarea impunerii unor condiții de natură tehnică ce pot fi considerate încălcări ale principiului nediscriminării, transparenței ori tratamentului egal. Informațiile/recomandările obținute în cadrul consultării pieței vor fi puse la dispoziția tuturor ofertanților și vor fi avute în vedere de către Autoritatea contractantă doar la întocmirea Caietului de sarcini și stabilirea valorii estimate pentru achiziția ce urmează a fi derulată.

Corespondența, respectiv transmiterea opiniilor, sugestiilor sau a recomandărilor și a altor informații cu privire la subiectul consultării pieței se va derula prin mesagerie electronică la adresele de contact ce se vor stabili ulterior, precum și prin întâlniri ale reprezentanților beneficiarului cu participanți interesați. Interesul participanților de a stabili contacte directe cu beneficiarul pentru lămurirea unor aspecte de natură tehnică, va fi exprimat prin mesagerie electronică, urmând a fi stabilită de comun acord o dată pentru întâlnirile de consultare.

În situația în care ofertanții doresc ca unele informații confidențiale sau care sunt considerate drepturi de proprietate intelectuală, să nu fie puse la dispoziția tuturor ofertanților, Autoritatea contractantă va respecta dorința acestora cu mențiunea că vor fi informați toți ofertanții cu privire la acest aspect. Participanții vor specifica în mod expres acele aspecte sau informații pe care le consideră sensibile și nu doresc să fie utilizate fără acordul lor.

LOT 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero.

Având în vedere că s-au înmulţit atacurile de tip “ziua zero” (atacuri ce exploatează vulnerabilităţi nedescoperite până în momentul atacului), pentru creşterea securităţii Sistemului Informatic Integrat Vamal este necesară prelungirea licenței și a suportului pentru soluţia de prevenire a atacurilor de tip “ziua zero” pentru WEB-http. Valabilitatea suportului și a licenței pentru update-ul de conținut a expirat la data de 8 martie 2017.

LOT 4. Echipamente de comunicații date, tip router

Dimensiunea Sistemului Informatic Integrat Vamal, corelată cu cerinţele de securitate naţionale şi comunitare ridică nevoia de asigurare a securității şi disponibilităţii sistemului la un nivel de importanţă strategică. În acest sens este necesar ca echipamentele de comunicaţii IT să fie în permanenţă actualizate şi modernizate în funcţie de necesităţile de trafic, pentru a

preîntâmpina încărcări pe procesor sau congestii de date ce afectează funcţionarea Sistemului Informatic Integrat Vamal la parametri normali.

2.3 Informații despre beneficiile anticipate de către Autoritatea/ contractantă

Achiziția produselor solicitate în prezentul Caiet de sarcini are în vedere:

- Asigurarea unui grad ridicat de disponibilitate a infrastructurii de comunicații și securitate informatică a Sistemului Informatic Integrat Vamal (SIIV);
- Protecția datelor gestionate în cadrul sistemului informatic al MFP;
- Alinierea MFP cu strategiile asumate și cu eforturile întreprinse la nivel național, în domeniul protecției infrastructurilor critice.

2.4 Alte inițiative/proiecte/programe asociate cu această achiziție de produse:

Nu este cazul

2.5 Cadrul general al sectorului în care Autoritatea contractantă își desfășoară activitatea:

Neaplicabil

2.6 Factori interesați și rolul acestora, în implementarea Contractului sunt:

- Ministerul Finanțelor Publice prin Centrul Național pentru Informații Financiare care administrează și dezvoltă Sistemul Informatic Integrat Vamal (SIIV);
- Ministerul Finanțelor Publice prin Centrul Național pentru Informații Financiare care va implementa Contractul și va intra în relație directă cu Contractantul pe perioada derulării acestuia;
- Angajații din Agenția Națională de Administrare Fiscală aparat central și instituții subordonate din teritoriu care utilizează Sistemul Informatic Integrat Vamal.

3 Descrierea produselor solicitate

3.1 Descrierea situației actuale la nivelul Autorității contractante

Arhitectura existentă

Informațiile de mai jos sunt prezentate cu următoarele scopuri:

- Înțelegerea infrastructurii fizice în care vor fi integrate produsele livrate;
- Înțelegerea tehnologiilor cu care produsele ofertate trebuie să se

interconecteze

În prezent o componentă a soluției de securitate existentă la nivelul infrastructurii SIIV constă în două clustere de echipamente Check Point, respectiv două echipamente Check Point Power-1 5077 (cluster Intranet) și două echipamente Check Point Power-1 9070 (cluster Internet).

Echipamentele sunt o componentă principală a infrastructurii de securitate și îndeplinesc cumulativ funcțiile de Firewall, Application Control, Intrusion Prevention System, NAT support,

URL filtering, VLAN support, VPN support, content filtering, Advanced Networking & Clustering, Network Policy Management, End Point Media Encryption, Management Portal Blade, Provision Software Blade, User Directory Blade.

Astfel se asigură conectarea VPN la infrastructura Sistemului Informatic Integrat Vamal a peste 1200 utilizatori (personal propriu și operatori economici), utilizatori beneficiari de certificate digitale tip p12, și a peste 2000 de utilizatori (operatori economici) care se conectează cu certificat digital tip .pfx. Certificatele tip .p12 sunt emise de autoritatea internă de certificare a clusterului Internet Check Point Power 1-9070 iar certificatele tip .pfx sunt emise de o autoritate interna de certificare Windows Server 2012 R2.

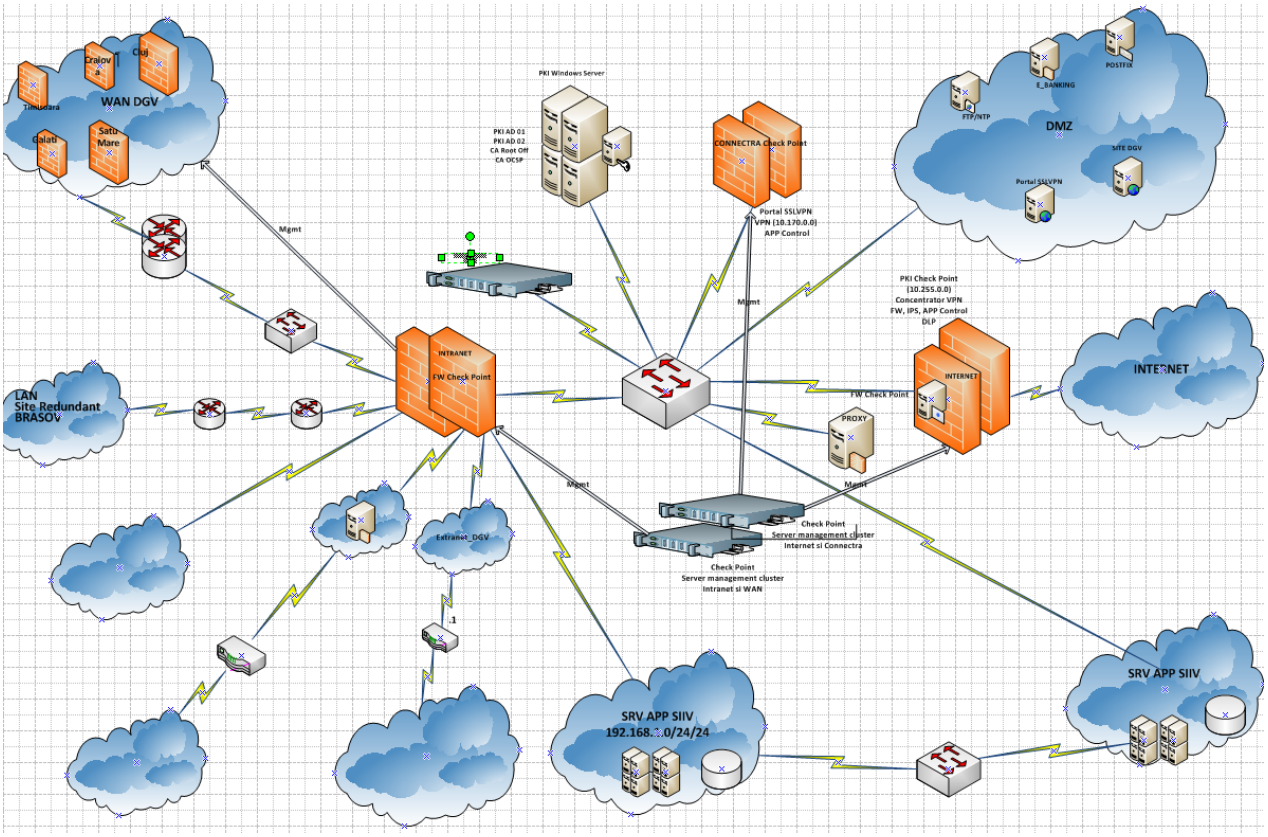
La nivelul soluției firewall sunt configurate peste 600 de politici de acces care asigură interoperabilitatea utilizatorilor cu serverele de aplicații ale infrastructurii SIIV, 16 conexiuni VPN permanente (System to System), precum și peste 140 rețele LAN ce deservesc toate sediile birourilor vamale și a direcțiilor regionale vamale din țară.

Conectarea securizată SSL, în prezent, este asigurată de un cluster Check Point 12600, echipamente care la rândul lor sunt integrate cu soluția de management existentă.

Soluția de management centralizat a infrastructurii de securitate se face pe o platformă Check Point Smart Dashboard R77.30, platformă extensibilă ce permite extinderea infrastructurii cu alte echipamente de securitate (ex. IPS, DLP).

Cu ajutorul interfeței soluției de management se gestionează politicile de securitate configurate la nivelul clusterelor firewall ce deservesc conexiunile cu toate birourile vamale și a altor instituții, la nivelul cărora sunt configurate politicile de acces Internet/DMZ precum și soluția de conectare securizată SSL care asigură conectarea operatorilor economici la componentele Sistemului Informatic Integrat Vamal.

Soluția Check Point Smart Event asigură în timp real jurnalizarea evenimentelor de securitate. Un mare avantaj al soluției constă în faptul că jurnalizarea evenimentelor se face în mod centralizat monitorizând toate echipamentele Check Point ce compun soluția de securitate. Prin automatizarea agregării datelor și corelarea datelor din fișierele jurnal brute (foarte greu de analizat la nivel individual pe fiecare appliance) se reduce volumul de date ce trebuie analizat, se izolează și se prioritizează amenințările de securitate.



Activitățile proiectului se vor desfășura în centrele de date ale Ministerului Finanțelor Publice, Centrul de Date Primar (CDP) localizat în București, respectiv Centrul de Date Secundar (CDS) localizat în Brașov.

Pentru elaborarea unei propuneri optime care să satisfacă necesitățile autorității contractante, potențialii ofertanți ar trebui să înțeleagă arhitectura fizică/logică în care vor fi integrate produsele livrate și tehnologiile cu care produsele ofertate trebuie să se interconecteze.

Infrastructura de securitate IT existentă este situată în Centrul de Date Primar care asigură alimentare cu energie electrică neîntreruptibilă, echipamentele fiind poziționate în dulapuri metalice (rack-uri) de maxim 42U.

Cablarea este tip structurat cu canal de cabluri suspendat. Acest canal va fi folosit la realizarea conectivităţii fizice a echipamentelor achiziționate în conformitate cu acest caiet de sarcini.

LOT 1. Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal

Managementul clusterului FW Internet se realizează cu soluția de management Check Point SmartDashboard R77.30-OS GAIA, instalată pe un echipament Bull Novascale R440 F2.

– Managementul clusterului FW Intranet se realizează cu soluția de management Check Point SmartDashboard R77.30-OS GAIA, instalată pe un echipament Bull Novascale R440 F2.

– Corelarea și analiza evenimentelor în vederea implementării politicilor de acces și a interpretării atacurilor se realizează cu ajutorul soluției de management al evenimentelor Check Point Smart 1-50 Smart Event.

– Soluția de conectare securizată SSLVPN este compusă din două echipamente CheckPoint 12600 HA, configurate în cluster.

LOT 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții

– Soluția de securitate informatică constă în două clustere de echipamente Check Point, respectiv două echipamente Check Point Power-1 5077 (cluster Intranet) și două echipamente Check Point Power-1 9070 (cluster Internet).

LOT 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero

– Soluția de prevenire a atacurilor de tip ziua zero, constă intr-un echipament tip FireEye 4400NX-HW WEB MPS.

LOT 4. Echipamente de comunicatii date, tip router

– Echipamentele de comunicații date existente sunt Cisco 4451, Cisco3845, Cisco 2821, Cisco 1841 și Cisco 1941 și Cisco Catalyst 2960.

3.2 Obiectivul general la care contribuie furnizarea produselor

Asigurarea unui grad ridicat de disponibilitate a infrastructurii de comunicații și securitate informatică a Sistemului Informatic Integrat Vamal (SIIV), la un nivel de peste 99,5%.

3.3 Obiectivul specific la care contribuie furnizarea produselor

Scopul achiziţionării acestor produse este mentinerea nivelului de securitate a Sistemului Informatic Integrat Vamal (SIIV), precum si îmbunatatirea gradului de protectie împotriva atacurilor informatice asupra acestuia. Totodată este necesar ca produsele care asigură securitatea SIIV, precum şi soluţiile de securitate care le include, să fie în permanenţă actualizate şi modernizate pentru a permite gestionarea lor în condiţii optime, pentru a preîntâmpina atacuri sau alte activităţi neautorizate care pot duce la distrugerea sau deteriorarea funcţionalităţii SIIV.

3.4 Produsele solicitate și operațiunile cu titlu accesoriu necesar a fi realizate

3.4.1 Produse și servicii solicitate

3.4.1.1 LOT 1: Servicii de Suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal

Cantitate	Unitate de măsură	Loc de livrare*	Data de livrare solicitată**	Specificații tehnice SAU cerințe funcționale minime	Specificații tehnice SAU cerințe funcționale extinse	Durata minima garanție / termen de valabilitate
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**
1	buc.	Centrul Primar de Date București	60 zile de la intrarea în vigoare a contractului	conform precizărilor de mai jos***	-	12 luni

* Locația exactă la care vor fi livrate echipamentele va fi precizată Contractantului declarat câștigător, în cadrul Contractului.

** Data de livrare include și acceptarea de către Autoritatea contractantă (recepția cantitativă și calitativă)

***Specificații tehnice / cerințe funcționale minime:**

Autoritatea contractanta doreste achizitionarea următoarelor licențe și subscripții, inclusiv serviciile de suport aferente produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal:

Subscripție	Cantitate	Nivel suport
1.1. Suport Check Point Security Management & GW Internet și Intranet		
CP Reporting blade for 1 gateway (CPSB-RPRT-F-SSVU)	1	CPCES-CO-Standard
CP Security bundle-including SG204U and SM007-FW, VPN, ACCL, ADN, NPM, EPM, LOGS, MNTR, MPTL,PRVS and UDIR (CPSG-P204U-CPSM-PU007-F)	1	CPCES-CO-Standard
CP Security Management Container for Unlimited gateway and 7 blades –NPM, EPM, LOGS, MNTR, MPTL, UDIR and PRVS (CPSM-PU007-F)	1	CPCES-CO-Standard
CPEP-C1-101TO1000-Licence	1	CPCES-CO-Standard

CPSB-EP-VPN-P-License	1	CPCES-CO-Standard
1.2. Suport Check Point Smart 1-50 SmartEvent		
Smart 1-50 Smart Event Appliance with 3 management blades (CPAP-SM5003-EVNT)	1	CPCES-CO-Standard
1.3. Suport pentru soluția de conectare securizată ssl Check Point-Connectra		
Mobile Access blade for unlimited number of concurrent users (CPSB-MOB-U)	2	CPCES-CO-Standard
12600 NextGenerationFirewall Appliance (FW, VPN, ADNC, IA, MOB5, IPS, and APCL Blades-CPAP-SG12600-NGFW)	2	CPCES-CO-Standard

3.4.1.2 LOT 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții.

Cantitate	Unitate de măsură	Loc de livrare*	Data de livrare solicitată**	Specificații tehnice SAU cerințe funcționale minime	Specificații tehnice SAU cerințe funcționale extinse	Durata minima garanție/termen de valabilitate
1.	2.	3.	4.	5.	6.	7.
1	buc.	Centrul Primar de Date București si Centrul Secundar de Date Brașov	60 zile de la intrarea în vigoare a contractului	conform precizărilor de mai jos***	Consultarea pieței	36 luni inclusiv Subscripții și suport tehnic

* Locația exactă la care vor fi livrate echipamentele va fi precizată Contractantului declarat câștigător, în cadrul Contractului.

** Data de livrare include și acceptarea de către Autoritatea contractantă (recepția cantitativă și calitativă)

*** **Specificații tehnice/ cerințe funcționale minime:**

În cadrul Sistemului Informatic Integrat vamal (SIIV) componenta de securitate firewall cluster Intranet și Internet asigură conectarea la infrastructura SIIV a aproximativ 1200 utilizatori (personal propriu și operatori economici), utilizatori care se conectează cu certificate digitale emise de CA internă Check Point, și a aproximativ 2000 de utilizatori (operatori economici) care se conectează la infrastructura SIIV cu certificat digital, emise de o altă autoritate internă de certificare Windows Server 2012. Tot la nivelul soluției de securitate sunt configurate peste 400 de politici de securitate care asigură inter-operabilitatea utilizatori-componente SIIV, precum și conexiuni VPN permanente (S2S).

Contractantul va asigura atât migrarea/testarea politicilor de acces existente, fără a afecta continuitatea funcționalităților existente, cât și licențele pentru activarea și actualizarea serviciilor, Antispam, Prevenirea Intruziunilor,etc.(trebuie activate toate licențele posibile pe echipament). De asemenea, Contractantul va integra soluția de securitate cu soluția de management existentă, asigurând astfel existența unei singure platforme de management, și trebuie sa conțină pachetul de înaltă performanță.

Soluția ce urmează a fi achiziționată va trebui să nu fie declarată de producător “end of support” cel puțin cinci ani de la data achiziției, va prelua integral configurările existente, va asigura cel puțin funcționalitățile soluției existente, fără întreruperea activității și va include servicii de instalare, configurare și testare.

Personalul Contractantului desemnat pentru activitățile de instalare/configurare/ testare și suport tehnic trebuie să dețină certificări specifice domeniului de activitate și să aibă pregătirea necesară pentru asigurarea acestor activități.

Soluția ofertată trebuie să asigure cel puțin următoarele funcționalități software:

FIREWALL

– Sistemul firewall trebuie să asigure cel mai înalt nivel de securitate cu proprietăți de control al accesului, securitatea aplicațiilor, autentificare și NAT astfel încât să se blocheze accesul utilizatorilor neautorizați și să protejeze sistemul informatic al beneficiarului;
– Sistemul trebuie să fie de tip “statefull packet inspection” sau echivalent;
– Sistemul trebuie să asigure NAT, cu reguli automate sau manual;
– Sistemul trebuie să suporte IP-uri dinamice;
– Sistemul trebuie sa aibă set extins de politici de obiect pe noduri individuale, rețele, grupuri;
– Sistemul trebuie să funcționeze pe IPv4 și IPv6;
– Sistemul trebuie să asigure metode multiple de autentificare pe bază de user, client și sesiune;
– Sistemul trebuie să asigure baza de date cu utilizatori locali;
– Sistemul trebuie să asigure minim autentificare pe baza de RADIUS și Grupuri RADIUS, TACACS+
– Sistemul trebuie să suporte autentificare multifactor;
– Sistemul trebuie să asigure Autoritate de certificare internă;
– Soluția trebuie să suporte certificate X.509 folosind CA internă inclusă în pachetul software oferit, sau o terță CA;

VPN

– Sistemul VPN trebuie să asigure conectivitatea securizată între diverse locații ale achizitorului și a utilizatorilor mobili. Sistemul trebuie să asigure controlul accesului, autentificarea utilizatorilor și să cripteze comunicația peste internet;
– Sistemul trebuie să asigure suport criptare minim pe DES, 3DES, AES;
– Sistemul trebuie să asigure autentificare pe baza parole, RADIUS, TACACS, X.509, smart card;
– Sistemul trebuie să suporte minim topologile stea și plasă;
– Sistemul trebuie să asigure VPN bazat pe Interfețe Tunel Virtuale;

– Sistemul trebuie să asigure moduri Site-to-site VPN bazate pe domeniu sau pe rute;

– Sistemul trebuie să asigure VPN direcțional între sau în comunitate;

– Sistemul trebuie să asigure software IPsec VPN pentru diverse medii statice sau mobile, pentru medii windows, windows mobile, Iphone;

– Sistemul trebuie să asigure acces de tip SSL VPN;

– Sistemul trebuie să scaneze anti-malware mașinile de pe care se inițiază conexiuni SSL VPN inainte de admiterea lor în rețeaua locală;

– Aplicațiile client vpn vor fi disponibile gratuit, fără costuri suplimentare și vor avea următoarele specificații:

- Autentificare IKE cu certificat(v1 și v2);
- Alegerea dinamică a celei mai bune căi de transport pentru conexiuni securizate fără reautentificare când se schimbă locația sau se iese din modul sleep;
- Detecția automată a conexiunii LAN-WiFi-GPRS;
- Detecția automată a proxy-urilor;
- Capacitate internă de scanare de malware pentru a asigura conformitatea cu politicile de protecție a informației din companie.

– Soluția trebuie să suporte NAT-Transversal care permite Ipsec să traverseze static sau dinamic dispozitive NAT.

– Să suporte cel puțin următoarele sisteme de operare:

a. Windows 2000 Professional 32-bits cu SP1-4 ;
b. Windows XP Home & Professional 32-bits, cu sau fără SP1-3 ;
c. Windows Vista 32 si 64 bits;
d. Windows 7 32/64 bits;
e. Windows 8;
f. Windows 10;
g. Android, iOS;

IPS

– Funcția IPS trebuie să asigure cel puțin protecția împotriva amenințărilor la adresa clienților, serverelor, vulnerabilităților de SO, infecțiilor cu malware. Sistemul trebuie să dețină motoare de detecție multi-nivel care să combine mai multe metode de detecție minim cele bazate pe semnături, pe validarea protocoalelor, detecția anomaliilor, analiza comportamentală;

– Sistemul trebuie să asigure performanțe IPS de minim 4 Gbps;

– Sistemul trebuie să asigure protejarea performanței firewall-ului sub încărcare printr-un bypass software configurabil;

– Sistemul trebuie să asigure detecție multi-metodă bazată cel puțin pe:

a. Semnături ale vulnerabilităților și ale exploiturilor;
b. Validarea Protocolului;
c. Detecția Anomaliilor;
d. Detecție bazată pe comportament;

– Sistemul trebuie să asigure protecție în timp real cel puțin pentru:

e. Vulnerabilități ale serverelor și ale clienților;
f. Exploituri;

g. Folosirea greșită a protcoalelor;
h. Comunicații malware ;
i. Încercări de Tunelare;
j. Controlul aplicațiilor;

– Sistemul trebuie să asigure protecție extinsă împotriva atacurilor DoS;

– Sistemul trebuie să permită aplicarea acelorași politici de protecții pe grupuri, profile;

– Sistemul trebuie să aibă profile predefinite, optimizate pentru securitate sau performanță;

– Sistemul să poată funcționa și în mod “doar detecție” fără oprirea traficului;

– Sistemul trebuie să asigure pe grafice temporale vizualizări configurabile (e.x. Evenimente de securitate doar asupra componentelor rețelei);

– Sistemul trebuie să afișeze informații detaliate despre:

a. Descrierea vulnerabilităților și a amenințărilor;
b. Severitatea amenințărilor;
c. Impactul asupra performanței;
d. Nivelul de încredere;

– Sistemul trebuie să permită crearea de excepții în protecție.

CONTROLUL APLICAȚIILOR

Sistemul trebuie să permită crearea de politici complexe de securitate pe utilizatori și grupuri AD sau locale, prin care să se identifice, să se permită, să se blocheze sau să se limiteze utilizarea aplicațiilor care comunică în internet, indiferent de portul folosit, inclusiv pe web 2.0 și rețele sociale.

ANTI-BOT

– Sistemul Anti-Bot trebuie să poată detecta mașinile infestate cu bot și trebuie să blocheze comunicațiile cu serverele Command and Control (C&C);Sistemul trebuie să fie capabil să descopere bot analizând cel puțin adrese IP, URL-uri bazate pe reputație Web, reputație E-mail. Acestea trebuie actualizate zilnic de către producator prin semnături;

– Sistemul Anti-Bot trebuie să investigheze în timp real adrese IP, URL-uri și adrese unde sunt cunoscute centre Command and Control;

– Sistemul trebuie să detecteze mașinile infestate cu bot aflate în rețeaua locală folosindu-se de modele de comunicație specifice pentru bot, adrese IP, DNS și URL și folosindu-se de comportamentul atacului.

– Sistemul trebuie să oprească atacurile de tip APT (Advanced Persistent Threat) și să prevină deteriorarea mașinilor ce au contactat un centru de tip Command and Control (C&C);

– Sistemul Anti-Bot trebuie să ofere rapoarte ce descriu cel puțin: mașina infestată și user-ul acesteia, numele bot-ului, acțiunile și rezultatele comunicației cu serverul Command and Control (C&C).

FILTRARE URL

– Sistemul Filtrare URL trebuie să permită, blocheze sau să limiteze în timp real, accesul utilizatorilor la un site web, atât pentru site-uri criptate prin SSL, cât și pentru cele necriptate;

– Sistemul Filtrare URL să aibă definite categorii de conținut;

– Sistemul trebuie să poată analiza traficul SSL-criptat cu posibilitatea adăugării de excepții;

– Sistemul Filtrare URL trebuie să permită controlul atât asupra întregului site cât și asupra anumitor pagini din site-ul web;

– Sistemul Filtrare URL trebuie să permită crearea de white lists / black lists pentru anumite site-uri web definite de administrator;

– Sistemul Filtrare URL trebuie să poată transmite utilizatorilor o pagină personalizată de atenționare în cazul în care conținutul la o pagină web a fost restricționat;

– Sistemul trebuie să poată permite, bloca sau limita accesul la un site web, în mod granular, pentru un anumit utilizator / anumit grup de utilizatori;

– Sistemul trebuie să asigure protecție pentru porturile non-standard și trebuie să poată analiza/inspecta tot traficul;

– Sistemul trebuie să elimine tehnicile de tip “bypass”;

– Sistemul Filtrare URL trebuie să poată realiza rapoarte detaliate privind activitatea utilizatorilor, timpul de navigare, statistici, evenimente etc.;

ROUTING și QOS

– Sistemul trebuie să includă caracteristici avansate de rețea cum ar fi rutare dinamică, prioritizare QoS, încărcare echilibrată a aplicațiilor. Trebuie să asigure optimizarea performanțelor rețelei astfel încat aplicațiile critice să funcționeze corespunzător.

– Sistemul trebuie să asigure protocoale dinamice de rutare cum ar fi:

a. RIP RFC 1058;
b. RIP Versiunea 2;
c. RIPng (IPv6) ;
d. OSPFv2;
e. OSPF NSSA;
f. OSPFv3 (IPv6) ;
g. BGP4;
h. BGP4++;

– Sistemul trebuie să asigure balansarea încărcării serverelor prin distribuirea traficului de rețea pe multiple servere, folosind metode variate de distribuire a încărcării și verificarea disponibilității;

– Sistemul trebuie să asigure redundanța de provider Internet prin funcționarea cel puțin în modurile “împarțirea încărcării” sau “primar/rezervă”;

– Sistemul trebuie să permită setarea de restricții asupra lațimii de bandă alocată aplicațiilor non-critice;

– Sistemul trebuie să asigure QoS configurabil cel puțin pe greutate, sursă, destinație, protocol, aplicație, VPN.

ACCELERARE ȘI CLUSTERING

– Sistemul trebuie să asigure funcționarea optimă a rețelei în medii ultra performante și să ofere funcții de accelerare a traficului de rețea și posibilitatea de implementare de sisteme HA;

– Sistemul trebuie să suporte moduri Activ/Pasiv și Activ/Activ.

– Sistemul trebuie să ofere soluții HA proprii și să suporte soluții HA oferite de terțe părți;

ADMINISTRAREA POLITICILOR, CLIENȚILOR, CONFIGURAȚIILOR

– Sistemul trebuie să poată fi administrat prin intermediul consolei unice de management existente la nivelul SIIV cel puțin pentru următoarele module:

a. Firewall ;
b. VPN;
c. IPS;
d. Anti-Bot ;
e. Filtrare URL;
f. Application control;
g. QOS.

– Sistemul trebuie să asigure căutări pe bază de interogare pe reguli și obiecte;

– Sistemul trebuie să asigure crearea ușoară a clonelor unui sistem de management al politicilor de rețea pentru recuperearea lor în urma unui dezastru;

– Sistemul trebuie să asigure administrare bazată pe roluri prin acces și permisinuni administrative globale și granulare;

– Sistemul trebuie să permită controlul reviziilor prin menținerea de multiple versiuni ale politicilor;

– Sistemul trebuie să permită integrare cu parteneri terți;

– Sistemul trebuie să permită SNMP;

– Sistemul trebuie să asigure administrarea configurațiilor;

ADMINISTRARE LOGURI ȘI EVENIMENTE

– Sistemul trebuie să poată oferi în mod grafic informații despre incidentele de securitate a informației și despre evenimentele pe gateway, tunele, utilizatori la distanță;

– Sistemul trebuie să asigure captură de pachete pentru analiza de evenimente IPS;

– Sistemul trebuie să asigure jurnale cel puțin de tip conexiune, activ, audit;

– Sistemul trebuie să asigure transportul securizat al jurnalelor;

– Sistemul trebuie să asigure menținerea unui procent din spațiu de pe disc liber, specificarea alertelor de menținut pentru ziua specificată și rularea unui script predefinit;

– Sistemul trebuie să poată asigura informații de stare firewall și IPS,

Specificații minime hardware cluster Internet:

– Interfețe 10/100/1000Base-T RJ45 : 10 ;

– Sloturi de rețea suportate: 8x 10/100/1000Base-T RJ45, , 4 x1000Base-F SFP, 4 x10GBase-F SFP+, 4 x 10/100/1000Base-T Fail-Open NIC, 2 x 10GBase-F Fail-Open NIC;

– Suport pentru Link Aggregation: 802.3ad ;

– Suport pentru High Availability ;

- Suport pentru mod HA Active/Active - L3 mode;
- Suport pentru mod HA Active/Passive - L3 mode;
- Suport pentru session failover în cazul modificări routării;
- Suport pentru detecția defecțiunilor echipamentului;
- Suport pentru detecția defecțiuni link-urilor;
- Memorie: 16GB upgradabil la 32 GB;
- Minim 5 GB Throughput cu toate funcționalitățile activate;
- Stocare 1 x 500 GB;
- Tensiune de intrare: AC 220-240V, 45-65Hz;
- Sursă de alimentare redundantă hot-swap: 250 W.

Specificații minime hardware cluster Intranet:

- Interfețe 10/100/1000Base-T RJ45 : 10 ;
- Sloturi de rețea suportate: 8x 10/100/1000Base-T RJ45, , 4 x1000Base-F SFP, 4 x10GBase-F SFP+, 4 x 10/100/1000Base-T Fail-Open NIC, 2 x 10GBase-F Fail-Open NIC;
- Suport pentru Link Aggregation: 802.3ad ;
- Suport pentru High Availability ;
- Suport pentru mod HA Active/Active - L3 mode;
- Suport pentru mod HA Active/Passive - L3 mode;
- Suport pentru session failover în cazul modificări routării;
- Suport pentru detecția defecțiunilor echipamentului;
- Suport pentru detecția defecțiuni link-urilor;
- Lights Out Management card: inclus;
- Memorie: 16GB upgradabil la 32 GB;
- Minim 5 GB throughput, cu toate funcționalitățile activate;
- Stocare 1 x 500 GB;
- Tensiune de intrare: AC 220-240V, 45-65Hz;
- Sursă de alimentare redundantă hot-swap: 250 W .

3.4.1.3 LOT 3: Licență și servicii de suport pentru soluția de prevenire a atacurilor de tip "ziua zero"

Cantitate	Unitate de măsură	Loc de livrare*	Data de livrare solicitată**	Specificații tehnice SAU cerințe funcționale minime	Specificații tehnice SAU cerințe funcționale extinse	Durata minima garanție / termen de valabilitate
1.	2.	3.	4.	5.	6.	7.
1	buc.	Centrul Primar de Date București	60 zile de la intrarea în vigoare a contractului	conform precizărilor de mai jos***	-	12 luni

* Locația exactă la care vor fi livrate produsele va fi precizată Contractantului declarat câștigător, în cadrul Contractului.

** Data de livrare include și acceptarea de către Autoritatea contractantă (recepția cantitativă și calitativă)

*** **Specificații tehnice/ cerințe funcționale minime:**

Autoritatea contractantă dorește achiziționarea următoarelor licențe și subscripții, inclusiv serviciile de suport aferente soluției de prevenire a atacurilor de tip "ziua zero", pentru un echipament tip Fire Eye 4400NX-HW WEB MPS.

- Licență (LK2-CONTENT_UPDATES)
- Subscripție Suport FireEye (LK2-FIREEYE_SUPPORT)

3.4.1.4 Lotul 4: Echipamente de comunicații date, tip router

Cantitate	Unitate de măsură	Loc de livrare*	Data de livrare solicitată**	Specificații tehnice SAU cerințe funcționale minime	Specificații tehnice SAU cerințe funcționale extinse	Durata minima garanție/termen de valabilitate
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**
140	buc.	Centrul Primar de Date București	60 zile de la intrarea în vigoare a contractului	conform precizărilor de mai jos***	-	36 luni

* Locația exactă la care vor fi livrate echipamentele va fi precizată Contractantului declarat câștigător, în cadrul Contractului.

** Data de livrare include și acceptarea de către Autoritatea contractantă (recepția cantitativă și calitativă)

*** **Specificații tehnice/ cerințe funcționale minime:**

Carcasa	Router rack-mount 19 inch de 1U cu kit de montare în rack de la acelasi producator
Interfețe	2 interfețe WAN RJ45 FastEthernet 1000 Mbps electrice sau combo 8 interfețe LAN 10/100/1000 Mbps Ethernet; Interfata USB 2.0 pentru conectare memorie externa; Un port consolă (pentru acces direct la interfata de configurare a echipamentului)
Memorie	Memoria instalată va trebui sa asigure simultan toate funcționalitățile solicitate
Performante	Performanțe de trafic cu servicii simultane de Firewall, QoS, IPSec, NAT: (throughput agregat) minim 100 Mbps. Număr de tunele IPSec VPN concurente: minim 50; Functionalitătile de criptare VPN IPSec ale sistemului trebuie să fie accelerate

	hardware;
Conditii alimentare	Alimentare curent alternativ 230V, 50 Hz;
Mediu de functionare	Temperatura: 0 to 40°C Umiditate: 10 to 85% (umiditate relativa)
Certificare ISO	Certificat ISO 9001 sau echivalent
Accesorii/bucată	1 X cablu consolă 1 X cablu de alimentare energie electrică tip schuko conform standardelor româneşti Documentaţie cu manual de utilizare şi configurare tipărit Documentaţie cu manual de utilizare şi configurare în format electronic 1 X kit de instalare cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse
Functionalitati firewall	Stateful Firewall (routing/transparent) Suport pentru împărtirea interfetelor in zone si crearea de politici de firewall intre zone
Functionalităti VPN	Suport IKEv1 si IKEv2 Suport Layer 2 si Layer 3 VPN, IPSec, L2TPv3;
Functionalităti retelistică si rutare	Suport DHCP Client/Relay/Server,DHCPv6; Rutare bazată pe politici Rutare dinamică IPv4: RIPv1 RIPv2, OSPF, EIGRP, BGP v4, Multicast (PIM), IS-IS Rutare dinamica IPv6: RIPng, OSPFv3, BGP; Suport VRRP, balansare cu impartire de incarcare automata intre doua echipamente si Link Failure Control Suport VLAN Tagging (802.1Q) Multi-Link Aggregation – 802.3ad Posibilitatea de a exporta statistici despre trafic care sa includa si informatii despre aplicatii, intr-un format general acceptat (Netflow sau similar)
Functionalităti QoS	Limitare/garantare/prioritizare a benzii de trafic prin politici Traffic Shaping per aplicatie si adresă IP cu posibilitatea de rezervare de banda exclusiva pentru un tip de trafic marcat prioritar; Traffic shaping bazat pe clase; Suport pentru marcare si prioritizare trafic dupa DSCP si ToS; Suport pentru pastrarea marcarii DSCP in headerul IPSEC dupa criptarea traficului QoS class-based WFQ, Hierarchical QoS , Weighted Random Early Detection (WRED);
Functionalităti de administrare	Administrare prin interfata WEB (HTTP/HTTPS), Telnet, Secure Command Shell (SSH) pentru IPv4 si IPv6, Functionalitate de descarcare/incarcare a configuratiei prin FTP, SCP, TFTP, USB Flash; Vor fi furnizate licenţele pentru software-ul care rulează în echipament inclusiv licentele pentru criptarea traficului.
Functionalităti de log-are si monitorizare	Interfata grafică pentru monitorizare în timp real Optiune de păstrare/stocare a log-urilor pe suportul local Suport SNMPv3

Functionalități de autentificare a utilizatorilor	Definire locală a utilizatorilor Integrare cu RADIUS/TACACS+ Suport Xauth prin RADIUS pentru IPSec VPN

3.4.2 Disponibilitate

Produsele si serviciile ce fac obiectul prezentului caiet de sarcini sunt componente ale infrastructurii de Securitate a SIIV, sistem a cărui disponibilitate trebuie să fie mai mare de 99%.

3.5 Extensibilitate/Modernizare

Nu este cazul

3.5.1 Garanție

LOT 1. **Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal**.

Nu este cazul

LOT 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții

Garanția produselor achiziționate va fi asigurată de către contractant în condițiile politicii de garanție a producătorului cu acces direct în numele beneficiarului la serviciile de garanție și suport ale acestuia, având în vedere prevederile Legii nr. 449/2003 precum și toate modificările acesteia (actualizarea din 2008 și OG nr. 9/2016) privind vânzarea produselor și garanțiile asociate acestora precum și prevederile prezentului Caiet de Sarcini.

Garanția tehnică oferită va fi pentru o perioadă minimă conform cap.3.4.1., atât pentru produse, cât și pentru accesorii, garanția începând din momentul recepției finale.

În cazul în care producătorii oferă perioade de garanție mai mari decât perioadele minime indicate de autoritatea contractantă, perioadele de garanție ofertate vor fi cel puțin cât perioadele oferite de producători;

Garanția de bună funcționare a produselor este distinctă de garanția de bună execuție a contractului și decurge de la data recepției (semnării procesului-verbal de recepție finală).

Pe perioada de garanție și suport tehnic Contractantul va garanta că produsele livrate/serviciile prestate sunt conforme cu specificațiile tehnice din prezentul caiet de sarcini și nici o componentă/echipament nu va eșua în a-și îndeplini funcțiunile, în situația în care este corect utilizată.

Modalitatea de asigurare a serviciilor de garanție se va prezenta în propunerea tehnică.

Garanția va fi asigurată doar la sediile autorității contractante (on-site), cu timp de intervenție următoarea zi lucrătoare (Next Business Day) pentru toate echipamentele și accesoriile acestora.

În perioada de garanție și suport tehnic Contractantul va trebui să asigure:

- garanția de bună funcționare, calitatea și performanțele tuturor produselor livrate în conformitate cu specificațiile producătorului acestora;
- suport tehnic de specialitate pentru echipamentele livrate;
- acces direct la suportul oferit de producător pentru echipamentele livrate;
- corectarea gratuită, pentru produsele livrate, a oricăror erori, defecte și neconformități constatate, cu excepția cazurilor în care defectele se datorează în mod exclusiv utilizării inadecvate / necorespunzătoare de către personalul autorității contractante;
- înștiințarea autorității contractante de apariția unor îmbunătățiri sau modificări aplicabile echipamentelor livrate și software-ului aferent, pentru o posibilă aplicare a acestora;
- înștiințarea autorității contractante privind încetarea producției oricăruia din tipurile de echipamente livrate în baza Contractului sau privind încetarea suportului oferit de producător.

În cazul în care echipamentele și accesoriile necesită înlocuire în perioada de garanție tehnică ca urmare a defectării sau funcționării neconforme cu cerințele specificate în prezentul caiet de sarcini, aceasta se va realiza în maximum 24 de ore, în timpul programului de lucru al autorității contractante, transportul de la și înapoi la autoritatea contractantă întrând în sarcina contractantului.

În perioada de garanție, Contractantul are obligația sa asigure funcționarea produsului, reparând sau înlocuind prin grija și pe cheltuiala lui orice componentă hardware sau accesoriu. În perioada de garanție și suport tehnic Contractantul are obligația de a răspunde unei solicitări de suport tehnic de specialitate sau unei solicitări de reparare/înlocuire a unui echipament defect astfel:

- în aceeași zi, în termen de 4 ore de la primirea unei solicitări efectuate în zilele lucrătoare, în intervalul orar 09.00 -17.00, ora României;
- în prima zi lucrătoare, în intervalul orar 09.00 -12.00, ora României, în cazul unei solicitări efectuate după ora 17.00.

Contractantul va asigura un punct de contact dedicat personalului autorizat al autorității contractante unde se poate semnala orice problemă/defecțiune care necesită mentenanță preventivă sau corectivă sau solicită suport tehnic Contractantului în gestionarea unui incident, disponibil, pentru a se asigura că orice situație semnalată este tratată cu promptitudine.

În perioada de garanție, toate costurile legate de înlocuirea sau repararea bunurilor, precum și de remedierea defecțiunilor cad în sarcina Contractantului (diagnosticare, transport, costuri de asigurare, taxe în vamă, manoperă pentru reparare etc.).

După efectuarea reparației și punerea în funcțiune a echipamentului / componentei defecte, între contractant (partenerul de service acreditat al Contractantului, după caz) și autoritatea contractantă se întocmește un proces-verbal de recepție.

Perioada de garanție se va prelungi, pentru echipamentele (componentele) în cauză, cu durata totală a imobilizării.

Pe perioada de garanție și suport tehnic Contractantul va garanta că produsele livrate/ serviciile prestate sunt conforme cu specificațiile tehnice din prezentul caiet de sarcini și niciun produs nu va eșua în a-și îndeplini funcțiunile, în situația în care este corect utilizat.

LOT 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero

Nu este cazul

LOT 4. Echipamente de comunicații date, tip router

Garanția produselor achiziționate va fi asigurată de către contractant în condițiile politicii de garanție a producătorului cu acces direct în numele beneficiarului la serviciile de garanție și suport ale acestuia, având în vedere prevederile Legii nr. 449/2003 precum și toate modificările acesteia (actualizarea din 2008 și OG nr. 9/2016) privind vânzarea produselor și garanțiile asociate acestora precum și prevederile prezentului Caiet de Sarcini.

Garanția tehnică oferită va fi pentru o perioadă minimă conform cap.3.4.1., atât pentru produse, cât și pentru accesorii, garanția începând din momentul recepției finale.

În cazul în care producătorii oferă perioade de garanție mai mari decât perioadele minime indicate de autoritatea contractantă, perioadele de garanție ofertate vor fi cel puțin cât perioadele oferite de producători;

Garanția de bună funcționare a produselor este distinctă de garanția de bună execuție a contractului și decurge de la data recepției (semnării procesului-verbal de recepție finală).

Pe perioada de garanție și suport tehnic Contractantul va garanta că produsele livrate/serviciile prestate sunt conforme cu specificațiile tehnice din prezentul caiet de sarcini și nici o componentă/echipament nu va eșua în a-și îndeplini funcțiunile, în situația în care este corect utilizată.

Modalitatea de asigurare a serviciilor de garanție se va prezenta în propunerea tehnică.

Garanția va fi asigurată doar la sediile autorității contractante (on-site), cu timp de intervenție următoarea zi lucrătoare (Next Business Day) pentru toate echipamentele și accesoriile acestora.

În perioada de garanție și suport tehnic Contractantul va trebui să asigure:

- garanția de bună funcționare, calitatea și performanțele tuturor produselor livrate în conformitate cu specificațiile producătorului acestora;
- suport tehnic de specialitate pentru echipamentele livrate;
- acces direct la suportul oferit de producător pentru echipamentele livrate;
- corectarea gratuită, pentru produsele livrate, a oricăror erori, defecte și neconformități constatate, cu excepția cazurilor în care defectele se datorează în mod exclusiv utilizării inadecvate / necorespunzătoare de către personalul autorității contractante;
- înștiințarea autorității contractante de apariția unor îmbunătățiri sau modificări aplicabile echipamentelor livrate și software-ului aferent, pentru o posibilă aplicare a acestora;
- înștiințarea autorității contractante privind încetarea producției oricăruia din tipurile de echipamente livrate în baza Contractului sau privind încetarea suportului oferit de producător.

În cazul în care echipamentele și accesoriile necesită înlocuire în perioada de garanție tehnică ca urmare a defectării sau funcționării neconforme cu cerințele specificate în prezentul caiet de sarcini, aceasta se va realiza în maximum 24 de ore, în timpul programului de lucru al autorității contractante, transportul de la și înapoi la autoritatea contractantă întrând în sarcina contractantului.

În perioada de garanție, Contractantul are obligația sa asigure funcționarea produsului, reparând sau înlocuind prin grija și pe cheltuiala lui orice componentă hardware sau accesoriu. În perioada de garanție și suport tehnic Contractantul are obligația de a răspunde unei solicitări de suport tehnic de specialitate sau unei solicitări de reparare/înlocuire a unui echipament defect astfel:

- în aceeași zi, în termen de 4 ore de la primirea unei solicitări efectuate în zilele lucrătoare, în intervalul orar 09.00 -17.00, ora României;
- în prima zi lucrătoare, în intervalul orar 09.00 -12.00, ora României, în cazul unei solicitări efectuate după ora 17.00.

Contractantul va asigura un punct de contact dedicat personalului autorizat al autorității contractante unde se poate semnala orice problemă/defecțiune care necesită mentenanță preventivă sau corectivă sau solicită suport tehnic Contractantului în gestionarea unui incident, disponibil, pentru a se asigura că orice situație semnalată este tratată cu promptitudine.

În perioada de garanție, toate costurile legate de înlocuirea sau repararea bunurilor, precum și de remedierea defecțiunilor cad în sarcina Contractantului (diagnosticare, transport, costuri de asigurare, taxe în vamă, manoperă pentru reparare etc.).

După efectuarea reparației și punerea în funcțiune a echipamentului / componentei defecte, între contractant (partenerul de service acreditat al Contractantului, după caz) și autoritatea contractantă se întocmește un proces-verbal de recepție.

Perioada de garanție se va prelungi, pentru echipamentele (componentele) în cauză, cu durata totală a imobilizării.

Pe perioada de garanție și suport tehnic Contractantul va garanta că produsele livrate/ serviciile prestate sunt conforme cu specificațiile tehnice din prezentul caiet de sarcini și niciun produs nu va eșua în a-și îndeplini funcțiunile, în situația în care este corect utilizat.

3.5.2 Livrare, ambalare, etichetare, transport si asigurare pe durata transportului

LOT 1. **Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal**.

Nu este cazul

LOT 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții

Livrarea, se va realiza conform unui ”Plan de livrare, instalare, punere în funcțiune,

testare, instruire și recepție” propus de către Contractant și agreat cu Autoritatea contractantă imediat după încheierea contractului.

Termenul de livrare este cel menționat pentru fiecare produs în parte la cap 3.4.1. Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate și produsul/echipamentul este acceptat de Autoritatea contractantă.

Produsele vor fi livrate cantitativ și calitativ la locul indicat de Autoritatea Contractantă pentru fiecare produs în parte. Fiecare produs va fi însoțit de toate accesoriile/subansamblele/părțile componente necesare instalării, punerii și menținerii în funcțiune.

Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită.

Ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, sării și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimii și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanta față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.

Transportul și toate costurile asociate sunt în sarcina exclusivă a contractantului. Produsele vor fi asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului și cauzate de orice factor extern.

Contractantul este responsabil pentru livrarea în termenul solicitat și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca nici un motiv de întârziere sau costuri suplimentare.

Contractantul, în condițiile legii, va prezenta, la livrare, următoarele:

- documentele de însoţire a mărfii (Aviz de însoțire a mărfii/Aviz de expediție etc.);
- documentație tehnică(*), respectiv:
  - descrierea tehnică a echipamentelor;
  - documentaţia de instalare, configurare şi utilizare (inclusiv documentația de network engineering - capabilități hardware-software);
  - documentatia de întreținere și remediere a defecțiunilor;
  - documentele de licențiere pentru produse software;
- certificat de garanție tehnică de la producător/ furnizor/ distribuitor;
- certificat de calitate/ conformitate;

(*)Contractantul va pune la dispoziția Autorității contractante, pentru fiecare echipament livrat, documentația tehnică prevăzută la alineatele de mai sus, în format electronic digital agreat de Autoritatea contractantă.

Destinația de livrare pentru fiecare produs este conform cap.3.4.1.

LOT 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero

Nu este cazul

LOT 4. Echipamente de comunicatii date, tip router

Livrarea, se va realiza conform unui *"Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție"* propus de către Contractant și agreat cu Autoritatea contractantă imediat după încheierea contractului.

Termenul de livrare este cel menționat pentru fiecare produs în parte la cap 3.4.1. Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate și produsul/echipamentul este acceptat de Autoritatea contractantă.

Produsele vor fi livrate cantitativ și calitativ la locul indicat de Autoritatea Contractantă pentru fiecare produs în parte. Fiecare produs va fi însoțit de toate accesoriile/ subansamblele/ părțile componente necesare instalării, punerii și menținerii în funcțiune.

Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită.

Ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, sării și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimii și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanta față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.

Transportul și toate costurile asociate sunt în sarcina exclusivă a contractantului. Produsele vor fi asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului și cauzate de orice factor extern.

Contractantul este responsabil pentru livrarea în termenul solicitat și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca nici un motiv de întârziere sau costuri suplimentare.

Contractantul, în condițiile legii, va prezenta, la livrare, următoarele:

- documentele de însoţire a mărfii (Aviz de însoțire a mărfii/Aviz de expediție etc.);
- documentație tehnică(*), respectiv:
  - descrierea tehnică a echipamentelor;
  - documentaţia de instalare, configurare şi utilizare (inclusiv documentația de network engineering - capabilități hardware-software);
  - documentatia de întreținere și remediere a defecțiunilor;
  - documentele de licențiere pentru produse software;
- certificat de garanție tehnică de la producător/ furnizor/ distribuitor;
- certificat de calitate/ conformitate;

(*)Contractantul va pune la dispoziția Autorității contractante, pentru fiecare echipament livrat, documentația tehnică prevăzută la alineatele de mai sus, în format electronic digital agreat de Autoritatea contractantă;

Destinația de livrare pentru fiecare produs este conform cap.3.4.1.

3.5.3 Operațiuni cu titlu accesoriu

3.5.3.1 Instalare, punere în funcțiune, testare

Lot 1. Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal

În cadrul activităților de instalare, punere în funcțiune și testare, Contractantul va trebui să asigure:

- Activarea serviciilor de suport;
- Actualizarea / instalarea noilor versiuni software, patch-uri;

Contractantul va efectua pe cheltuiala sa și fără nici un fel de costuri din partea Autorității contractante toate testele pentru a asigura funcționarea produsului la parametri agreați.

Lot 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții

Instalarea, punerea în funcțiune, testarea se vor realiza conform unui *"Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție"* propus de către Contractant și agreat cu Autoritatea contractantă la încheierea contractului.

Contractantul va detalia în cadrul soluției propuse strategia și modalitatea aleasă pentru îndeplinirea cerințelor Autorității Contractante, fără perturbarea fluxului tehnologic.

Odată ce produsele sunt asamblate, Contractantul va realiza și apoi toate configurările/setările necesare pentru a pune produsele în funcțiune. Punerea în funcțiune include, de asemenea, toate ajustările și setările necesare pentru a asigura instalarea corespunzătoare, în ceea ce privește performanța și calitatea, cu toate configurațiile necesare pentru o funcționare optimă.

Contractantul va efectua pe cheltuiala sa și fără nici un fel de costuri din partea Autorității contractante toate testele pentru a asigura funcționarea produsului la parametri agreați.

Serviciile de instalare, configurare, testare și punere în funcțiune se vor realiza cu îndeplinirea următoarelor cerințe (minime și obligatorii):

- Echipamentele oferite se vor instala în spațiile existente în locațiile indicate de către Autoritatea contractantă;
- Montarea echipamentelor se va realiza conform specificațiilor producătorului, de comun acord cu Autoritatea contractantă și conform Planului de cablare agreat.
- Conectarea echipamentelor la rețeaua electrică și interconectarea accesoriilor necesare punerii în funcțiune a echipamentelor;
- Contractantul va asigura punerea în funcțiune a tuturor echipamentelor livrate;
- Contractantul va instala, configura, integra și testa produsele software ofertate;
- Contractantul va instala licențele, conform drepturilor acordate Autorității contractante, va documenta procesul de instalare, configurare și va genera din sistem lista prin care să fie indicată totalitatea software-ului livrat solicitată la cap.3.6 și care va fi verificată în cadrul recepției calitative, conform cap.5.2

– Contractantul va întocmi un Raport de livrare și instalare a licențelor conform cap.3.6.
– Instalarea produselor se va realiza conform specificațiilor producătorului, de comun acord cu Autoritatea contractantă și conform Planului de livrare, instalare, punere în funcțiune, testare, instruire și recepție agreat;
– Serviciile de instalare/configurare vor fi prestate de către persoanele prezentate în ofertă. Persoanele menționate în ofertă vor fi autorizate/certificate în administrarea/configurarea soluției ofertate și vor semna o declarație de confidențialitate. Ofertantul poate înlocui persoanele respective doar cu personal cu calificare egală sau superioară persoanelor înlocuite, fără costuri suplimentare.

Contractantul trebuie să instaleze toate produsele în mod corespunzător, asigurând-se în același timp ca spațiile unde s-a realizat instalarea rămân curate. După livrarea și instalarea produselor, Contractantul va elimina toate deșeurile rezultate și va lua măsurile adecvate pentru a aduna toate ambalajele și a le elimina de la locul de instalare.

Contractantul rămâne responsabil pentru protejarea produselor luând toate masurile adecvate pentru a preveni lovituri, zgârieturi și alte deteriorări, până la acceptare de către Autoritatea contractantă.

Pe perioada executării activităţilor de instalare, configurare, punere în funcțiune și testare a produselor, Contractantul are următoarele obligaţii:

- să nu afecteze serviciile existente în reţeaua de comunicaţii a MFP;
- să respecte toate regulile privind confidenţialitatea informaţiilor, accesul în locaţii şi protecţia muncii;
- să nu afecteze prin activităţile desfăşurate buna funcţionare a echipamentelor existente în locaţii, precum şi mediul de comunicaţii pus la dispoziţie.

Soluţionarea eventualelor probleme de natură tehnică apărute pe parcursul derulării Contractului referitoare la soluția livrată cade în sarcina exclusivă a Contractantului

Lot 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero

În cadrul activităților de instalare, punere în funcțiune și testare, Contractantul va trebui să asigure:

- Activarea serviciilor de suport;
- Actualizarea / instalarea noilor versiuni software, patch-uri;

Contractantul va efectua pe cheltuiala sa și fără nici un fel de costuri din partea Autorității contractante toate testele pentru a asigura funcționarea produsului la parametri agreați.

Lot 4. Echipamente de comunicații date, tip router

Instalarea, punerea în funcțiune, testarea se vor realiza conform unui *”Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție”* propus de către Contractant și agreat cu Autoritatea contractantă la încheierea contractului.

Serviciile de instalare, configurare, testare și punere în funcțiune se vor realiza cu îndeplinirea următoarelor cerințe (minime și obligatorii):

– Conectarea echipamentelor la rețeaua electrică și efectuarea testelor funcționale;

- Contractantul va instala licențele, conform drepturilor acordate Autorității contractante, va documenta procesul de instalare, configurare și va genera din sistem lista prin care să fie indicată totalitatea software-ului livrat, solicitată la cap.3.6 și care va fi verificată în cadrul recepției calitative, conform cap.5.2.;
- Instalarea, configurarea și punerea în funcțiune a produselor se va realiza de către personalul Autorității contractante, în locațiile finale, respectiv sediile birourilor vamale și direcțiilor regionale vamale, conform specificațiilor producătorului și a documentaţiei de instalare, configurare şi utilizare livrată de Contractant.

Contractantul rămâne responsabil pentru protejarea produselor luând toate masurile adecvate pentru a preveni lovituri, zgârieturi și alte deteriorări, până la acceptarea de către Autoritatea contractantă.

Pe perioada executării activităţilor de instalare, configurare, punere în funcțiune și testare a produselor, Contractantul are următoarele obligaţii:

- să nu afecteze serviciile existente în reţeaua de comunicaţii a MFP;
- să respecte toate regulile privind confidenţialitatea informaţiilor, accesul în locaţii şi protecţia muncii;
- să nu afecteze prin activităţile desfăşurate buna funcţionare a echipamentelor existente în locaţii, precum şi mediul de comunicaţii pus la dispoziţie.

Soluţionarea eventualelor probleme de natură tehnică apărute pe parcursul derulării Contractului referitoare la soluția livrată cade în sarcina exclusivă a Contractantului

3.5.3.2 Instruirea personalului pentru utilizare:

Pentru loturile 1, 3 si 4 nu se solicita instruire.

Lot 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții:

Contractantul este responsabil pentru instruirea personalului desemnat de Autoritatea Contractantă. Scopul instruirii este de a pregati personalul desemnat al autoritatii contractante pentru a configure/administra produsele livrate și instalate.

Instruirea se va realiza conform unui *“Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție”* care va fi propus de Contractant și va fi agreat cu Autoritatea contractantă.

- Contractantul va asigura instruirea personalului desemnat de Autoritatea Contractantă pentru exploatarea/administrarea soluției oferite și instalate.

În cadrul Propunerii tehnice se va detalia modul în care Contractantul va asigura instruirea pentru minim 2 persoane.

Cursul va cuprinde atât partea teoretică cât și practică, și va fi însoțit și de suport de curs printat pentru fiecare participant.

Contractantul poate să propună orice subiect suplimentar care ar putea fi necesar pentru a se asigura că personalul Autorității contractante este pe deplin instruit pentru a asigura utilizarea corespunzătoare a produsului.

În cadrul Propunerii tehnice, Contractantul va detalia nivelul de instruire avut în vedere, nivel care trebuie sa fie direct corelat cu scopul achiziției, cu obiectivul proiectului, cu tipul de soluție propusă din punct de vedere al noutății tehnologice astfel încât să permită personalului care va fi instruit să administreze eficient si la un nivel adecvat soluțiile furnizate. Propunerile privind nivelul de instruire, suportul de curs și programa de instruire, coordonatele activităților de instruire, incluzând datele cursurilor, durata acestora și detaliile cu privire la locul de desfășurare, vor fi incluse în *Planul de livrare, instalare, punere în funcțiune, testare, instruire și recepție* care va fi propus de Contractant și agreat cu Autoritatea contractantă, în vederea satisfacerii nevoii de instruire la nivelul așteptat.

3.5.3.3 Mentenanța preventiva in perioada de garanție

Nu se solicită.

3.5.3.4 Mentenanța corectiva in perioada post-garanție

Nu se solicită.

3.5.3.5 Suport tehnic

Loturile 1, 2, 3 și 4 - Cerințe generale

Contractantul va asigura suport tehnic, inclusiv subscripții si suport tehnic de la Producător, perioada fiind cea solicitată la cap. 3.4.1. pentru fiecare produs hardware/software și serviciu ofertat.

Pe toata durata contractului, în perioada de garanție, Contractantul va asigura accesul garantat al Autorității contractante, fără costuri suplimentare, la servicii de suport tehnic pentru produsele livrate, constând în:

- înștiințarea autorității contractante de apariția unor îmbunătățiri sau modificări aplicabile echipamentelor livrate și software-ului aferent, pentru o posibilă aplicare a acestora;
- înștiințarea autorității contractante privind încetarea producției oricăruia din tipurile de echipamente livrate în baza Contractului, modificări în politica de licențiere a producătorului sau alte modificări privind produsele software livrate care pot afecta drepturile și/ sau modul de utilizare a produselor de către Autoritatea contractantă sau privind încetarea suportului oferit de producător.
- accesul la resursele de update și upgrade firmware/software oferite de producător;
- informarea Autorității Contractante cu privire la orice modificări în politica de licențiere a Producătorului sau alte modificări privind produsele software livrate care pot afecta drepturile și/ sau modul de utilizare a produselor de către Autoritatea contractantă.

Contractantul va asigura un punct de contact dedicat personalului autorizat al Autorității contractante unde se poate semnala orice problemă/defecțiune care necesită solicită suport tehnic Contractantului în gestionarea unui incident, disponibil, pentru a se asigura că orice situație semnalată este tratată cu promptitudine.

Contractantul va răspunde în timp util la orice incident semnalat de Autoritatea contractantă.

Contractantul trebuie să asigure disponibilitatea serviciilor de suport tehnic 24x7, din momentul primirii sesizării și până la remedierea definitivă a problemei și asigurarea funcționalității integrale a produsului.

Contractantul va trebui să respecte următorii timpi de intervenție:

Timp de răspuns	***Timp de implementare soluție provizorie***	***Timp de rezolvare***
4 ore	*24 ore*	*48 ore*

Nerespectarea timpilor de mai sus dă dreptul Autorității contractante de a solicita penalități/daune interese în conformitate cu clauzele Contractului.

Cerințe specifice

Lot 1. Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal

Contractantul va asigura suport tehnic, inclusiv subscripții si suport tehnic de la Producător, care va include cel puțin:

- Actualizări de programe (incluzând noi versiuni, ediţii, patch-uri), pe măsură ce ele devin disponibile comercial şi dacă ofertantul le recomandă sau beneficiarul le solicită;
- Accesul la site-ul de suport al producătorului pentru descărcarea tuturor noilor versiuni, ediţii şi patch-uri, precum şi a documentaţiei aferente serviciilor care fac obiectul contractului;
- Asistenţă tehnică şi suport, ca răspuns la solicitările beneficiarului, care se referă la diagnosticarea și izolarea cauzei problemelor apărute în funcţionare;
- Mentenanță corectivă şi patch-uri de programe, conform nivelului de suport achiziționat, pentru orice probleme identificate de către beneficiar sau ofertant;

Pentru rezolvarea incidentelor, serviciile de suport tehnic vor fi prestate de către personalul tehnic al ofertantului, în limba română, în locația în care sunt instalate echipamentele.

Contractantul va prezenta lista persoanelor abilitate să asigure serviciile de suport tehnic, ce va cuprinde minim următoarele informații: nume și prenume, telefon mobil, e-mail. Contractantul va notifica Autoritatea contractantă despre eventuale schimbări în structura persoanelor abilitate, iar acestea se vor face numai cu acordul Autorității contractante. Contractantul poate înlocui persoanele respective doar cu personal propriu, cu calificare egală sau superioară persoanelor înlocuite, fără costuri suplimentare.

Persoanele abilitate să asigure serviciile de suport tehnic vor fi autorizate/certificate în administrarea/configurarea soluției și vor semna o declarație de confidențialitate.

Orice intervenție la sediile Beneficiarului se va încheia prin semnarea Procesului verbal de intervenție, care va descrie natura problemei, modul și timpii de intervenție.

Lot 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții

Contractantul va asigura suport tehnic, inclusiv subscripții si suport tehnic de la Producător, care va include cel puțin:

- Actualizări de programe (incluzând noi versiuni, ediţii, patch-uri), pe măsura ce ele devin disponibile comercial şi dacă ofertantul le recomandă sau beneficiarul le solicită;
- Asigurarea accesului la site-ul de suport al producătorului pentru descărcarea tuturor noilor versiuni, ediţii şi patch-uri, precum şi a documentaţiei pentru produsele care fac obiectul contractului;
- Acces nelimitat la servicii de suport online;
- Asistenţă tehnică şi suport, ca răspuns la solicitările beneficiarului, care se referă la:
    a. Probleme legate de instalare, utilizare şi configurare;
    b. Întrebări cu privire la documentaţii şi publicaţii despre produsele respective;
- Asistenţă pentru diagnosticarea și izolarea cauzei problemelor apărute în funcţionare (de ex. asistenţă în interpretarea rapoartelor problemelor de instalare sau referitoare la documentaţiile produselor software eligibile);
- Mentenanță corectivă şi patch-uri de programe pe care beneficiarul are dreptul să le primească conform nivelului de suport achiziționat;
- Instalarea, fără costuri suplimentare, a versiunilor noi de software apărute pe perioada contractului la producatorul de software;

Serviciile de suport tehnic vor fi prestate de către persoanele prezentate în ofertă. Persoanele menționate în ofertă vor fi autorizate/certificate în administrarea/configurarea soluției ofertate și vor semna o declarație de confidențialitate. Ofertantul poate înlocui persoanele respective doar cu personal cu calificare egală sau superioară persoanelor înlocuite, fără costuri suplimentare.

Contractantul va asigura asistenţă tehnică şi suport, remote şi on-site la sediile beneficiarului, telefonic şi prin e-mail, în limba română.

Lot 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero

Contractantul va asigura suport tehnic, inclusiv subscripții si suport tehnic de la Producător, care va include cel puțin:

- Actualizări de programe (incluzând noi versiuni, ediţii, patch-uri), pe măsura ce ele devin disponibile comercial şi dacă ofertantul le recomandă sau beneficiarul le solicită;
- Asigurarea accesului la site-ul de suport al producătorului pentru descărcarea tuturor noilor versiuni, ediţii şi patch-uri, precum şi a documentaţiei pentru produsele care fac obiectul contractului;
- Acces nelimitat la servicii de suport online;
- Asistenţă tehnică şi suport, ca răspuns la solicitările beneficiarului, care se referă la:
    a. probleme legate de instalare, utilizare şi configurare;

b. întrebări cu privire la documentaţii şi publicaţii despre produsele respective;
c. asistență pentru diagnosticarea și izolarea cauzei problemelor apărute în funcţionare (de ex. asistenţă în interpretarea rapoartelor problemelor de instalare sau referitoare la documentaţiile produselor software eligibile, cum ar fi trace-uri și dump-uri);
d. pentru defecte identificate de către beneficiar sau ofertant, service corectiv şi patch-uri de programe pe care beneficiarul are dreptul să le primească conform nivelului de suport achiziționat.

Contractantul va asigura asistenţă tehnică şi suport remote şi on-site la sediile beneficiarului, telefonic şi prin e-mail, în limba română.

Lot 4. Echipamente de comunicații date, tip router

Nu este cazul.

3.5.3.6 Piese de schimb și materiale consumabile pentru activitățile din programul de mentenanță corectiva după expirarea garanției

Nu este cazul

3.5.4 Mediul in care este operat produsul

Mediul în care se utilizează produsele este descris la cap.3.1.

3.5.5 Constrângeri privind locația unde se va efectua livrarea/instalarea

Locațiile de livrare/instalare sunt în București și Brașov. Adresele exacte vor fi precizate ofertantului devenit Contractant, în cadrul Contractului.

Locațiile de livrare/instalare aferente loturilor sunt următoarele:

LOT 1 - Centrul Primar de Date – București

LOT 2 - Centrul Primar de Date – București și Centrul Secundar de Date – Brașov

LOT 3 - Centrul Primar de Date – București

LOT 4 - Sediile Autorității contractante – București

3.6 Atribuțiile și responsabilitățile Părților:

3.6.1 Pentru achiziție de software separat, sau de hardware și software inclus, Contractantul va utiliza în proiectare/configurare/dezvoltare etc. produse software sau tehnologii hardware care înglobează tehnologii software, doar a acelor produse ce beneficiază de suport pe termen lung (de tip Long-term support – LTS), ca intenție a Autorității contractante de asigurare a unei politici de management a ciclului de viața al produsului prin adoptarea de versiuni stabile care sunt menținute pe perioade mai lungi de timp decât versiunile standard. Justificarea se poate face prin prezentarea de Roadmap (foaie de parcurs privind ciclul de viață al produsului) sau alte documente echivalente disponibile publicului larg, elaborate de către producători, declarații semnate ale acestora.

3.6.2 Contractantul va avea obligația ca, pentru componentele livrate, ori va obține din timp în numele Autorității contractante, ori va transfera acestuia, prin documente cu caracter juridic, licențele necesare pentru utilizarea lor conform cu scopul prezentului contract. Aceasta prevedere se aplică tuturor componentelor/resurselor licențiate și/sau sub licențiate, componentelor software comercializate de contractant, componentelor software ale unor terți, componentelor pre-existente, uneltelor software necesare livrării, monitorizării și mentenanței ș.a.m.d.

3.6.3 Contractantul va oferi licențele pentru cumulul total al tehnologiilor HW și SW (atât cele proprii cât și ale terților, indiferent că sunt OEM, distincte, orice altă metodă) înglobate în echipamentele livrate funcționale. Aceeași cerință este valabilă inclusiv pentru utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată.

3.6.4 Contractantul va prezenta documente care dovedesc faptul că software-ul în ansamblul său este supus sau nu unor politici de licențiere (inclusiv se vor avea în vedere utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată). Documentele justificative trebuie să fie clare, să permită identificarea tipului de licențiere, metodele de calcul (fie virtual, fizic, grad de încărcare, număr de utilizatori etc.), condițiile de utilizare, perioada de timp precum și orice altă informație valabilă la momentul contractării). Orice diferend juridic ulterior cu un terț pe subiectul drepturilor de proprietate intelectuală va cădea în sarcina și responsabilitatea Contractantului.

3.6.5 Contractantul va avea obligația ca transferul drepturilor de proprietate și/sau folosință, și al oricăror drepturi conexe către Autoritatea contractantă va avea loc de la data recepției finale.

3.6.6 Contractantul va avea obligația să despăgubească Autoritatea contractantă împotriva oricăror: a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.) și b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea caietului de sarcini întocmit de către Autoritatea contractantă.

3.6.7 Contractantul trebuie să aibă în vedere că după livrare și instalare se va întocmi un Raport de livrare și instalare, pentru numărul total al licențelor care acoperă integral, distinct, licențele furnizate . Este obligatoriu ca la întocmirea acestui Raport de livrare și instalare a licențelor aferente softului să se țină seama de împerecherea datelor din lista generată de către sistemul funcțional propus pentru livrare finală (lista prin care este indicată de sistemul conceput toate software-urile utilizate și livrate), cu documentele în original (documente care să indice clar numărul licențelor, felul acestora, durata (nelimitată/ perpetuă sau limitată) etc. într-o formă care să permită înregistrarea în patrimoniul/contabilitatea Autorității contractante) prin care se atestă și se transmit drepturile de proprietate/folosință, după caz, condițiile de utilizare etc. astfel încât la finalizarea recepției calitative Autoritatea contractantă să dețină toate documentele privind licențele proprii sau cele din partea terților.

3.6.8 Contractantul va avea în vedere, ca obligație, la recepție, că Autoritatea contractantă va proceda la preluarea tuturor licențelor livrate și instalate, doar prin întocmirea Proceselor verbale de recepție cantitativă și calitativă a licențelor, ca documente necesare în implementarea Contractului, care se vor întocmi pe baza constatării existenței tuturor documentelor în original privind drepturile de proprietate acordate și condițiile utilizării acestora, drepturile de folosință și condițiile acestora, identificarea clară (distinctă) a fiecărei tehnologii supuse licențierii/sub licențierii, a existenței listei de software/hardware generate de către sistemul propus pentru livrare.

3.6.9 Contractantul va garanta faptul că toate suporturile ce conțin software vor fi livrate fără viruși informatici, viermi informatici sau cod periculos, care pot distruge sau altera software, firmware sau hardware și care, prin orice metodă, pot colecta, distruge sau altera orice dată sau informație accesată sau procesată de software. Contractantul va anunța imediat Autoritatea contractantă în scris, dacă există suspiciunea sau are cunoștință că software-ul livrat poate provoca neajunsuri de tipul celor enunțate mai sus.

3.6.10 Contractantul va avea obligația ca, la transferul documentelor privind licențele, ca drepturi de proprietate intelectuală/folosință, să facă transferul către Autoritatea contractantă a unor documente în original, atât pentru propriile produse cât și pentru toate cele ale unor terți pe care le-a înglobat, adaptat, modificat, îmbunătățit, ș.a.m.d. și simultan să aibă în vedere că orice reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), în legătură cu produsele achiziționate, montate și puse în funcțiune, vor fi în sarcina și responsabilitatea sa.

3.6.11 Contractantul are obligația de a garanta că produsele software furnizate prin Contract sunt noi, de ultimă generație, şi încorporează toate îmbunătățirile recente în proiectare şi din ultima versiune, inclusiv din punct de vedere al securității. Contractantul are obligația de a garanta că toate produsele furnizate prin Contract sunt livrate pe canalul oficial al producătorului, acoperind zona Uniunii Europene.

3.6.12 Contractantul va avea în vedere obligația de a deschide sau, după caz, de a actualiza un cont de identificare deschis pe numele/seama Autorității contractante la producător. Această cerință poate să nu fie aplicabilă în situația în care producătorul nu are o astfel de politică.

4 Documentații ce trebuie furnizate Autorității contractante în legătură cu produsul

Pentru serviciile aferente lotului 1 și 3 Contractantul va prezenta documente din care sa reiasă perioada de valabilitate a serviciilor achiziționate și sistemul pe care au fost activate.

Pentru produsele aferente loturilor 2 și 4, Contractantul va prezenta următoarele documente în legătură cu produsul:

- Documentele de însoțire a mărfii;
- Documentație tehnică(*), respectiv:
    - descrierea tehnică;
    - documentația de instalare, configurare și utilizare (inclusiv documentația de network engineering - capabilități hardware-software);
    - documentația de întreținere și remediere a defecțiunilor;
- Certificate de garanție producător/ furnizor/ distribuitor ;
- Certificate de calitate/conformitate;
- Roadmap (foaie de parcurs privind ciclul de viață al produsului) sau alte documente echivalente disponibile publicului larg, elaborate de către producători, declarații semnate ale acestora;
- Documente care dovedesc faptul că software-ul în ansamblul său este supus sau nu unor politici de licențiere (inclusiv se vor avea în vedere utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată);
- Documentele de licențiere pentru produsele software ofertate;
- Politica de licențiere stabilită de producător pentru produsele software ofertate;
- Orice alt document solicitat în celelalte capitole din Caietul de Sarcini și nespecificat explicit în acest capitol.

(*) *Documentația tehnică va fi pusă la dispoziție și în format electronic digital agreat de Autoritatea contractantă*.

Documentele justificative trebuie să fie clare, să permită identificarea tipului de licențiere, metodele de calcul (fie virtual, fizic, grad de încărcare, număr de utilizatori etc.), condițiile de utilizare, perioada de timp precum și orice altă informație valabilă la momentul contractării. Orice diferend juridic ulterior cu un terț, pe subiectul drepturilor de proprietate intelectuală, va cădea în sarcina și responsabilitatea Contractantului.

5 Recepția produselor/serviciilor

Lot 1. Servicii de suport destinate produselor de securitate informatică pentru Sistemul Informatic Integrat Vamal

Recepția serviciilor se va efectua pe baza de proces verbal semnat de contractant și Autoritatea contractantă.

Recepția calitativă a serviciilor se va realiza astfel:

- Verificarea documentelor din care sa reiasă perioada de valabilitate a serviciilor achiziționate și sistemul pe care au fost activate serviciile;
- Verificarea în consola de administrare a sistemului, a actualizării perioadei contractului de suport;

- Verificarea pe site-ul producătorului în contul alocat Autorității contractante, a perioadei de valabilitate a serviciilor de suport, pentru fiecare serviciu achiziționat.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

a. acceptat;
b. acceptat cu observații minore;
c. acceptat cu rezerve;
d. refuzat.

Lot 2. Echipamente de securitate informatică, cluster Intranet și Internet, inclusiv suport și subscripții

Recepția produselor se va realiza conform unui *"Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție"* propus de către contractant și agreat cu Autoritatea contractantă la încheierea Contractului.

Dreptul Autorității contractante de a inspecta, testa și, dacă este necesar, de a respinge produsele, nu va fi limitat sau amânat din cauza faptului că produsele au fost inspectate și testate de contractant, anterior furnizării acestora la locația de livrare/instalare.

Transferul drepturilor de proprietate și/sau folosința, și al oricăror drepturi conexe către Autoritatea contractantă va avea loc de la data recepției calitative.

Recepția produselor se va efectua pe baza de proces verbal semnat de Contractant și Autoritatea contractantă. Recepția produselor se va realiza în mai multe etape, în funcție de progresul Contractului, respectiv:

a. recepția cantitativă se va realiza după livrarea produselor în cantitatea solicitată la locația indicată de Autoritatea contractantă și va consta în efectuarea următoarelor operațiuni:
   - Numărarea bucată cu bucată;
   - Verificarea aspectului exterior, a integrității fizice și a caracteristicilor constructive pentru echipamentele livrate;
   - Verificarea existenței documentelor de însoțire a mărfii (aviz de însoțire a mărfii/ aviz de expediție etc.);
   - Verificarea existenței documentației tehnice aferente fiecărui tip de echipament;
   - Verificarea existenței certificatelor de garanție, calitate/ conformitate;
   - Verificarea existenței documentelor de licențiere pentru software-ul livrat;
   - Verificarea existenței documentațiilor privind produsele software pe care Contractantul trebuie să le furnizeze Autorității contractante conform Caietului de sarcini
   - Întocmirea unui proces verbal de recepție cantitativă *($PVR_{cant.}$)* în fiecare locație între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus.

b. recepția calitativă va consta în efectuarea următoarelor operațiuni:
   - verificarea instalării și electroalimentării echipamentelor livrate;
   - verificarea configurării hardware-software a echipamentelor livrate;
   - verificarea punerii în funcțiune a echipamentelor livrate;

- verificarea conformității componentelor livrate cu specificațiile tehnice din caietul de sarcini și din propunerea tehnică, prin efectuarea de inspecții și teste funcționale. Inspecțiile și testele funcționale din cadrul recepției vizează respectarea cerințelor caietului de sarcini și a specificațiilor producătorului (caracteristici tehnice, constructive, electrice, cerințele funcționale etc.);
- testările funcționale din cadrul recepției se vor efectua pe baza unui set de teste, teste care vor fi propuse de către contractant în *Planul de livrare, instalare, punere în funcțiune, testare, instruire și recepție* și agreate de Autoritatea contractantă ;
- generarea unei liste de către sistem prin care să fie indicată totalitatea software-ului livrat și împerecherea acestei liste cu documentele juridice în original prin care se transmit drepturile de proprietate/folosință, după caz, verificarea versiunii codurilor software instalate, a licențelor corespunzătoare acestora, astfel încât la finalizarea recepției calitative Autoritatea contractantă să se asigure că va deține toate documentele juridice privind licențele;
- Întocmirea unui Proces Verbal de Recepție Calitativă *(PVR$_{cal.}$)* în fiecare locație între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

a. acceptat;
b. acceptat cu observații minore;
c. acceptat cu rezerve;
d. refuzat.

Lot 3. Servicii de suport și licență pentru soluția de prevenire a atacurilor de tip ziua zero

Recepția serviciilor se va efectua pe baza de proces verbal semnat de contractant și Autoritatea contractantă.

Recepția calitativă a serviciilor se va realiza astfel:

- Verificarea documentelor din care sa reiasă perioada de valabilitate a serviciilor achiziționate și sistemul pe care au fost activate serviciile;
- Verificarea în consola de administrare a sistemului, a actualizării perioadei contractului de suport;
- Verificarea pe site-ul producătorului în contul alocat Autorității contractante, a perioadei de valabilitate a serviciilor de suport, pentru fiecare serviciu achiziționat.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

a. acceptat;
b. acceptat cu observații minore;
c. acceptat cu rezerve;
d. refuzat.

Lot 4. Echipamente de comunicații date, tip router

Recepția produselor se va realiza conform unui ”Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție” propus de către Contractant și agreat cu Autoritatea contractantă la încheierea contractului.

Dreptul Autorității contractante de a inspecta, testa și, dacă este necesar, de a respinge produsele, nu va fi limitat sau amânat din cauza faptului că produsele au fost inspectate și testate de Contractant, anterior furnizării acestora la locația de livrare/instalare.

Transferul drepturilor de proprietate și/sau folosință, și al oricăror drepturi conexe către Autoritatea contractantă va avea loc de la data recepției calitative.

Recepția produselor se va efectua pe baza de proces verbal semnat de Contractant și Autoritatea contractantă. Recepția produselor se va realiza în mai multe etape, în funcție de progresul contractului, respectiv:

- recepția cantitativă se va realiza după livrarea produselor în cantitatea solicitată la locația indicată de Autoritatea contractantă și va consta în efectuarea următoarelor operațiuni:
    - numărarea bucată cu bucată;
    - verificarea aspectului exterior, a integrității fizice și a caracteristicilor constructive pentru echipamentele livrate;
    - verificarea existenței documentelor de însoțire a mărfii (aviz de însoțire a mărfii/ aviz de expediție etc.);
    - verificarea existenței documentației tehnice aferente fiecărui tip de echipament;
    - verificarea existenței certificatelor de garanție, calitate/ conformitate;
    - întocmirea unui Proces Verbal de Recepție Cantitativă *(PVR$_{cant.}$)* între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus.

- recepția calitativă va consta în efectuarea următoarelor operațiuni:
    - verificarea instalării și electroalimentării echipamentelor livrate;
    - verificarea configurării hardware-software a echipamentelor livrate;
    - verificarea conformității componentelor livrate cu specificațiile tehnice din Caietul de sarcini și din Propunerea tehnică, prin efectuarea de inspecții și teste funcționale. Inspecțiile și testele funcționale din cadrul recepției vizează respectarea cerințelor Caietului de sarcini și a specificațiilor Producătorului (caracteristici tehnice, constructive, electrice, cerințele funcționale etc.);
    - verificarea integrării funcționale a componentelor livrate conform specificațiilor din Caietul de sarcini/Propunerea tehnică prin efectuarea de inspecții și teste funcționale pe baza unui set de teste care vor fi propuse de către Contractant în *„Planul de livrare, instalare, punere în funcțiune, testare, instruire și recepție”* și agreate în prealabil de către Autoritatea contractantă.
    - întocmirea unui Proces Verbal de Recepție Calitativă între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

a. acceptat;
b. acceptat cu observații minore;
c. acceptat cu rezerve;
d. refuzat.

6 Modalități si condiții de plata

Contractantul va emite factura pentru produsele livrate. Factura va avea menționat numărul contractului, datele de emitere și de scadența ale facturii respective. Factura va detalia cantitativ/ valoric produsele furnizate și va prezenta prețul unitar al acestora. Factura va fi trimisă în original la adresa specificata de Autoritatea contractantă.

Factura va fi emisă după semnarea de către Autoritatea contractantă a procesului verbal de recepție calitativă, acceptat, după livrare. Procesul verbal de recepție calitativă va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

a) certificatul de calitate și garanție;

b) declarația de conformitate;

c) documentele de livrare;

d) procesul verbal de recepție cantitativă;

Plata se va efectua în lei, în contul Contractantului, în baza facturii fiscale însoțite de procesul-verbal de recepție calitativă, semnat de reprezentanții ambelor părți, astfel cum este prevăzut în contract (Secțiunea IV a Documentației de atribuire).

7 Cadrul legal care guvernează relația dintre Autoritatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii.

Actele normative și standardele indicate mai jos sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă:

- Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare
- Normele metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică /acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, aprobate prin HG nr. 395/2016, cu modificările și completările ulterioare
- Legea nr. 8/1996 privind dreptul de autor şi drepturile conexe cu completările și modificările ulterioare.

8 Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

8.1 Activitățile în cadrul contractului se vor desfășura:

- Conform unui ”Plan de livrare, instalare, punere în funcțiune, testare, instruire și recepție” propus de către Contractant și agreat împreună cu Autoritatea contractantă la încheierea contractului.

8.2 Evaluarea performanței Contractantului

Performanța Contractantului va fi evaluată luându-se în considerare:

- respectarea termenelor de livrare/ instalare/ configurare/ testare/ instruire în raport cu prevederile contractuale și Planul de livrare, instalare, punere în funcțiune, testare, instruire și recepție propus de Contractant și agreat împreună cu Autoritatea contractantă

- eventuale abateri de la calitatea produselor și a serviciilor contractate.

9 Cerințe privind personalul de specialitate:

Specificații generale pentru toate loturile (LOT 1, 2, 3 și 4)

Ofertantul va nominaliza specialiștii proprii care vor asigura pe parcursul contractului serviciile de instalare, configurare, punere în funcțiune și testare, cât și cele de înlocuire a componentelor în perioada de suport/garanție.

Specialiștii propuși trebuie să dețină calificarea și experiența specifică tipului de produs/serviciu achiziționat, necesară pentru prestarea serviciilor solicitate prin Caietul de sarcini.

Pentru aceștia se vor prezenta următoarele documente:

- CV actualizat, semnat de către titular;
- documente suport (diplome, atestate, acreditări, certificări) din care să rezulte pregătirea și competențele/calificările profesionale pentru îndeplinirea serviciilor solicitate prin prezentul Caiet de sarcini;
- experiența generală sau specifică în domeniu demonstrată prin copii ale unor documente precum: contracte de muncă, contracte de colaborare, contracte de prestări servicii, fișe de post, adeverințe, recomandări sau altele similare;
- declarație de disponibilitate pentru perioada implicării efective în derularea contractului.

Prin aceste cerințe se urmărește protejarea integrității echipamentelor complexe și de valoare ale Autorității contractante și implicit obținerea unei garanții minime că scopul și obiectivele achiziției vor fi îndeplinite iar disponibilitatea Sistemului Informatic Integrat Vamal(SIIV) nu va fi afectată. Ca urmare, Ofertantul trebuie să dovedească faptul că dispune de personal calificat corespunzător și cu experiență în asigurarea serviciilor de instalare, configurare, punere în funcțiune și testare, cât și cele de înlocuire a componentelor în perioada de garanție.

10 Modul de întocmire a Propunerii tehnice

Toate specificațiile tehnice din prezentul Caiet de sarcini sunt obligatorii și minimale pentru toți ofertanții.

Propunerea tehnică va răspunde punct cu punct cerințelor Caietului de sarcini, va prezenta detaliat produsele ofertate și modul de îndeplinire a cerințelor, și va asigura, obligatoriu, posibilitatea verificării facile a corespondenței cu specificațiile tehnice.

Propunerea tehnică trebuie întocmită în limba română și va fi însoțită de un format editabil (.odt/ .doc / .docx/ nu se va accepta propunerea tehnică scanată)

Propunerea tehnică constă în Formularul de Propunere tehnică din secțiunea Formulare a Documentației de atribuire, în care se va prezenta descrierea detaliată a produselor, a componentelor, accesoriilor și produselor software, după caz, ce compun Oferta și dacă este cazul modul de integrare funcțională a acestora conform cerințelor Caietului de sarcini, cu referire clară la specificațiile tehnice ale Producătorului, la standardele aplicabile și la Politica de licențiere a producătorului pentru produsele software ofertate.

Formularul de Propunere tehnică va avea următorul format:

Echipament: Producător și Model			
Cerință solicitată	**Conformitate (mod de îndeplinire)**	**Pagină din datasheet-ul oficial**	**Link valid site oficial producător. Se va preciza data ultimei accesări***

Pentru fiecare produs ofertat se vor prezenta:

a. Producătorul;
b. denumirea comercială, tipul/versiunea;
c. configurația hardware detaliată pe subansamble/componente/module;
d. versiunea de firmware;
e. pachetele software;
f. licențele ofertate (proprii și ale terților) și condițiile acestora; Contractantul va prezenta în formă scrisă, printr-o adresă oficială semnată, datată și ștampilată, un exemplar tipărit după politica de licențiere a producătorului, valabil la momentul semnării contactului
g. accesoriile ofertate/servicii asociate;
h. specificațiile tehnice emise de Producător pentru fiecare subansamblu / componentă / modul / întregul echipament;
i. standardele / protocoalele respectate;
j. rolul și facilitățile funcționale.
k. modul de integrare funcțională a fiecărui produs ofertat, conform cerințelor Caietului de sarcini.

Formularul de Propunere tehnică din secțiunea Formulare a Documentației de atribuire va conține, la rubricile dedicate:

- pentru specificațiile tehnice ale fiecărui produs în parte se va indica **pagina din datasheet-ul oficial și link-ul valid al site-ului oficial al producătorului. Se va preciza data ultimei accesări***.

- informații privind livrarea, modul de asigurare a serviciilor asociate de instalare, configurare, testare, instruire, garanție și suport tehnic incluzând: detalierea resurselor și mijloacelor pe care Ofertantul le va angaja pentru îndeplinirea Contractului, obligaţiile asumate referitoare la modul de asigurare a garanției și suportului tehnic, responsabilităţi ale personalului Contractantului implicat pentru îndeplinirea Contractului de furnizare;

- trimiteri la documentația tehnică / documentele suport, anexate la Formularul de Propunere tehnică.

**** se atașează, în format hârtie, extrasele la data ultimei accesări de pe site-urile indicate, relevante pentru demonstrarea conformității cu cerințele din Caietul de sarcini.***

Formularul de Propunere tehnică va fi însoțit de anexe:

- documentația tehnică și documentele suport necesare pentru identificarea produselor ofertate și a specificațiilor tehnice și funcționale ale acestora. Documentația tehnică și documentele suport se prezintă structurat, pe tipuri de componente/echipamente, respectând ordinea de prezentare a acestora înscrisă în Formularul de propunere tehnică.

- documentele doveditoare ale calificării și experienței specialiștilor desemnați de Contractant conform cap.9.

Toate echipamentele ofertate, sau după caz, configuraţia hardware-software a unui echipament, respectiv toate componentele şi licenţele software sau firmware care au un suport fizic vor fi prezentate cantitativ în Propunerea tehnică şi cantitativ-valoric în Propunerea financiară, specificându-se prețul unitar al fiecărui produs ofertat.

În cazul constatării unor neconcordanțe, specificațiile oficiale ale Producătorului echipamentului (valabile la data limită de depunere a ofertelor), vor fi considerate ca referință, conținutul acestora primând asupra specificațiilor tehnice prezentate de ofertant.

Marius Daniel PEȘTINĂ

Director general adjunct

Întocmit: Liviu Ilaș, expert superior, DTICSV-CACSSISV

Gabriela Mitroi, consilier superior DTICSV-CACSSISV

Dorin Cinieru, inspector superior, DTICSV-SITPAI