Finanțat de Uniunea Europeană NextGenerationEU

Planul Național de Redresare și Reziliență

România explorați Grădina Carpaților

Ursu Nicolae

Digitally signed by Ursu Nicolae
Date: 2026.03.05 12:57:28 +02'00'

CAIET DE SARCINI

privind achiziția publică soluție virtuală Next Generation Firewall

1. Introducere

Ministerul Economiei, Digitalizării, Antreprenoriatului și Turismului funcționează ca organ de specialitate al administrației publice centrale, în subordinea Guvernului, care aplică strategia și Programul de guvernare în domeniile antreprenoriatului, întreprinderilor mici și mijlocii, mediului de afaceri și turismului. Totodată, Ministerul Economiei, Digitalizării, Antreprenoriatului și Turismului inițiază, propune, implementează, coordonează și monitorizează acțiuni în domeniul reducerii barierelor administrative în domeniul său de activitate, asigură elaborarea, gestionarea și monitorizarea implementării elor și programelor pentru stimularea înființării și dezvoltării întreprinderilor mici și mijlocii și a societăților cooperative, precum și pentru creșterea competitivității și eficienței acestora în condițiile mediului concurențial și ale fenomenelor specifice economiei de piață.

Caietul de sarcini 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 Economiei, Digitalizării, Antreprenoriatului și Turismului 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 pentru produse echivalente

2. **Obiectul procedurii**:

Echipamente virtuale Next Generation Firewall 2 buc.

3. **Scopul achiziției:**

Implementarea în condiții optime a jalonului 246, "Investiția 1. Platforme digitale Privind transparentizarea legislativă, debirocratizarea și simplificarea procedurală destinate mediului de afaceri", din Planul Național de Redresare și Reziliență.

4. **Cerințe minimale și obligatorii**:

Soluția ofertată va fi în totalitate conformă cu detaliile tehnice specificate;
Soluția va fi pusă în funcțiune la sediul achizitorului;
Recepția cantitativă și calitativă se va realiza după punerea în funcțiune, conform cerințelor.

5. **Specificațiile tehnice și /sau cerințele funcționale minime sunt următoarele:**

Echipamente virtuale Next Generation Firewall

Se vor livra toate licentele / subscriptiile de la producator necesare asigurarii pentru o perioada de minim 5 ani a urmatoarelor funcționalități și capabilități avansate de securitate: protecție antivirus, detecția și controlul aplicațiilor (la nivelul OSI 7), prevenirea intruziunilor (IPS), filtrare URL, securitate DNS si Sanboxing

Solutia de securitate NGFW va asigura urmatoarele capabilitati tehnice si functionale minim obligatorii:

- ✓ Solutia implementeaza simultan, printr-un singur proces de inspectie a traficului mecanisme de protectie la nivel de retea (filtru de pachete), firewall de aplicatie, mecanisme anti-intruziune (IPS), filtrare anti malware, mecanisme de protectie impotriva exfiltrarii datelor (anti spyware), identificare de utilizator si de terminal, servicii de concentare VPN IPSec si SSL, decriptare SSL de tip inbound si outbound (forward proxy), decriptare SSH, inspectie tunele GRE, IPsec non-criptate.

- ✓ Soluția trebuie să suporte separarea unui management plane (care se ocupă de GUI-ul firewall-ului și de configurația firewall-ului) și a unui data plane (care se ocupă de traficul care trece prin firewall).
- ✓ Soluția suporta agregarea interfețelor utilizând protocolul LACP (802.3ad);
- ✓ Interfetele pot fi configurate mod Layer3, TAP, Virtual Wire (Transparent Mode);
- ✓ Sunt suportate subintefete 802.1Q (VLAN tag 1-4093 / interfata);
- ✓ Soluția va fi de tipul masina virtuala si va permite instalarea cel putin pe urmatoarele tipuri de hipervizoare: ESXi, Hyper-V, KVM precum si instante de cloud on-premise, cel putin: Azure, Google Cloud Platform, Red Hat OpenStack Platform (RHOSP), Red Hat OpenShift Container Platform(Red Hat OCP).
- ✓ Fiecare soluție in parte va rula un sistem de operare dedicat, dezvoltat de către producător. Nu este permisă folosirea unui sistem de operare comercial, pentru uz general.
- ✓ Modelul de licentiere va permite instalarea unui firewall de tipul masina virtuala cu urmatorii parametrii de performanta:

- „Firewall Throughput”
  - minim 2 Gbps utilizand un patern de trafic mix, avand jurnalizarea evenimentelor activata (“logging enabled”) si identificarea aplicatiilor in traficul monitorizat;
- „Threat Prevention throughput”:
  - minim 1,2 Gbps utilizand un patern de trafic mix pentru care se aplica inspectie IPS, antivirus, file blocking, anti-malware, filtrare aplicatie si cu „logging enabled”;
- “IPSec VPN Throughput”
  - minim 1 Gbps

- ✓ Este obligatoriu ca stocarea datelor transmise în cloud (pentru analiză amenințări informatice, fișiere sau aplicații suspicioase, loguri necesare suportului extern pentru remedierea unor defecțiuni etc.) se va face pe teritoriul UE, cu respectarea prevederilor Regulamentului UE nr. 679, iar acest aspect trebuie certificat și/sau garantat explicit de către producătorul soluției.
- ✓ Solutia asigura pe baza de subscriptie de tip „threat inteligence” , subscriptie valida pe durata periodei de garantie, informatii puse la dispozitie de catre producatorul sistemului NGFW urmatoarele capabilitati minime obligatorii:

- Sa asigure, fara a fi necesara instalarea de module sau platforme suplimentare in infrastructura clientului, implementarea de mecanisme de protectie activa a traficului DNS, protectie asigurata prin utilizarea de categorii si tehnici specifice: „C&C domains”, „DGA detection”, „NXNSAttack”, „DNS rebinding”, „Malware domains”, „Newly Registered Domains”, „Phishing Domains”, „Parked domains”, „Proxy avoidance”, „Ad tracking domains.” Aceasta protectie trebuie sa fie implementata fara reconfigurarea "DNS resolver" din infrastructura Beneficiarului si va inspecta inline in timp real traficul DNS, atat cererile cat si raspunsurile , pentru a opri atacuri de tipul DNS hijacking.
- Trebuie să conțină o soluție avansată de analiză a malware-ului oferita din cloud-ul producatorului (malware sandboxing) și trebuie să aibă în mod implicit suport și pentru scanarea executabilelor MacOS și Linux.
- Sa asigure funcționalități pentru filtrare a trafic WEB:
  - pe baza de filtrare site-uri și adrese URL cu conținut rău intenționat sau nedorit, folosind o bază globală de cunoștințe, actualizată la zi.
  - Solutia va permite definire de liste statice cu URL-uri permise/blocate respectiv personalizarea categorii filtrare;
  - Analiza in timp real a URL-urilor ce nu au o categorie existenta, fara intreruperea comunicatiei de acces, cu scopul de a preveni amenintari configurate recent, cu obtinerea unui verdict/ in timp real.
  - Capacitatea de a crea politici de securitate pentru a preveni furtul de acreditări (combinatia valida de utilizator si parola) și pentru a preveni scurgerea acreditărilor corporative către site-uri web terțe
- Să asigure analiza in timp real a comunicațiilor spyware si de tip C2 (comandă și control) necunoscute, pe baza algoritmilor de tip Deep Learning implementati în cloud-ul producătorului. Solutia trebuie sa permita implementarea functionalitatii cel putin pentru trafic de tip HTTP, HTTP/2, TLS si aplicatii neidentificate de platforma in trafic TCP si UDP si sa permita blocarea comunicatiei malitioase analizate in cloud in timp real la nivelul echipamentului de tip next generation firewall
- Componenta IPS asigura pe baza de semnaturi:
  - actualizări automate ale semnăturilor de tip IPS;
  - protectia împotriva atacurilor de tip DoS (Denial of Service);

- detectare anomalii utilizare protocoale de comunicații;
- detectarea si sa blocarea incercarilor de exploatare, tehnicilor evazive atat la nivel de retea cat si la nivel de aplicatie, inclusiv atacuri de tip port scan, buffer overflow, remote code execution si command injection;
- detectare atacuri de tip "port scan" si "host sweeping";
- asigură inspecția fișierelor arhivate fără parolă;
- suportă semnături definite de catre administratori.

✓ Solutia permite functionarea in infrastructuri izolate, avand posibilitatea desfasurarii activitatilor de actualizare semnaturi IPS si imagini ale sistemului de operare offline, fara a fi necesara o conexiune activa la portalul de suport al producatorului.

✓ Solutia asigura funcționalități pentru controlul aplicațiilor:

- Identificare și control pentru cel puțin 4800 de aplicații uzuale (control la nivelul OSI layer 7, inclusiv pentru cele existente în cloud – de exemplu suita Microsoft 365 și altele)
- utilizează tehnici multiple de identificare pentru a determina tipul de aplicațiilor care traversează echipamentele firewall, indiferent de port, protocol, tactici evazive sau criptare.
- permite definirea unor politici de securitate pentru anumite aplicatii care sa permita activarea unora dintre funcționalitatile aplicației în timp ce blochează altele. De ex. se vor configura o politica care permit utilizarea aplicatiei WebEx dar nu permite transferul de fisiere, politica care permite „file downloading” dar nu „file uploading” sau „file sharing”;
- limitare de bandă („traffic shaping”) per aplicație
- analiza aplicațiilor care au ratele cele mai mari de consum de bandă
- decriptare si inspectie a traficului criptat TLS1.2 / TLS1.3;

✓ Solutia asigura minim urmatoarele funcționalități la nivel retea:

- Suportă IPv4 și IPv6 pentru toate serviciile oferite;
- NAT („Network Address Translation”) / NAT 1 la 1 /PAT („Port Address Translation”);
- Rutare statica / rutare dinamică OSPF, BGP, Multicast;
- Rutare bazată pe politici („policy-based routing”);

- Funcționalități management lărgime de bandă („traffic shaping”): asigură limitarea / garantarea lărgimii de bandă în funcție de politici / adrese IP / aplicații

✓ Solutia permite definirea unor politici de securitate bazate pe identitatea utilizatorilor

✓ Solutia programarea în timp (scheduling) a politicilor de firewall

✓ Solutia trebuie să ofere posibilitatea de a solicita re-categorizarea URL-ului din interiorul firewall-ului prin intermediul WebGUI.

✓ Soluția trebuie să ofere funcționalitatea accesului de la distanță la resursele organizației pentru utilizatorii finali pentru sisteme de tip Windows, MacOS, Android si iOS.

✓ Functionalitaea de acces la distanta prin VPN trebuie sa permita conectarea atat prin intermediului clientului furnizat de producator, cat si fara client (Clientless VPN)

✓ Functionalitatea de acces la distanta prin VPN trebuie sa permita trecerea automata la SSL VPN de la IPSec VPN

✓ Funcționalitatea de acces la distanță VPN trebuie să fie integrată cu recunoașterea utilizatorului si sa permita implementarea de controale bazate pe profilul hostului (HIP Profile).

✓ Funcționalitatea de acces la distanță VPN trebuie să fie integrată cu recunoașterea utilizatorului.

✓ Adresele IP selectate trebuie să poată ocoli tunelul de acces la distanță VPN și să direcționeze traficul direct către destinația publica.

✓ Solutia trebuie să permita scalarea pe orizontală a numărului de utilizatori VPN, în cazul în care este necesar, utilizând dispozitive NGFW suplimentare într-o configurație fără disponibilitate ridicată (adică autonomă)

✓ Solutia trebuie sa ofere functionalitatea de definire a tunelurilor de tip site-to-site VPN

✓ Solutia trebuie sa ofere suport pentru Post Quantum Hybrid Key Exchange VPN pentru extinderea securității VPN prin functionalitatea de a crea chei hibride de tip PQC (Post Quantum Cryptographic) folosind suitele criptografice NIST round 3 si round 4 (RFC 9242 si RFC 9370). Acest lucru are rolul de a proteja împotriva atacurilor de top “harvest now, decrypt later).

✓ Solutia va oferi o platforma de management centralizat livrata ca masina virtuala pentru administrarea masinilor virtuale de tipul next generation firewall, care va oferi urmatoarele functionalitati:

- Solutia trebuie sa permita integrarea si configurarea echipamentelor FW noi prin tehnologia Zero Touch Provisioning
- Solutia trebuie sa permita actualizarea de software si continut de Securitate a echipamentelor FW in mod centralizat
- Solutia trebuie sa permită gruparea firewall-urilor și sistemelor din firewall-uri individuale în containere logice sau grupuri logice de dispozitive care să permită managementul comun (configurarea politicilor de securitate, configurarea setărilor de rețea, folosind aceleași obiecte).
- Solutia trebuie sa permită crearea unei ierarhii de setări pentru grupuri de dispozitive, astfel încât setările pentru un anumit grup să fie moștenite de la grupurile părinte. Sistemul ar trebui să permită cel puțin patru niveluri de moștenire.
- Solutia trebuie sa permită crearea și utilizarea unor roluri administrative care diferă în ceea ce privește nivelul de acces la un anumit dispozitiv sau grup de dispozitive. Trebuie să fie posibil să se restricționeze accesul la dispozitivele sau grupurile de dispozitive selectate.
- Solutia trebuie sa ofere funcția de a trimite automat configurația pregătită și acceptată către dispozitivele gestionate conform programului. Acest lucru este pentru a reduce costurile de operare și pentru a utiliza eficient ferestrele de service programate pentru implementarea nesupravegheată a modificărilor planificate, de rutină ale configurației.
- Solutia trebuie să permită colectarea jurnalelor de evenimente de pe dispozitivele firewall administrate. Datele colectate ar trebui să includă informații despre cel puțin: trafic de rețea, utilizatori, aplicații, amenințări și site-uri web filtrate
- Solutia trebuie să fie capabil să coreleze jurnalele de evenimente de la firewall-urile gestionate. De asemenea, trebuie să ofere o căutare ușoară a jurnalelor corelate colectate de la firewall-urile gestionate.
- Solutia trebuie să ofere instrumente pentru analiza rapidă și eficientă a informațiilor, inclusiv cel puțin să permită crearea, salvarea și reutilizarea filtrelor pentru căutarea informațiilor în datele colectate.
- Solutia trebuie sa permită crearea de rapoarte statice adaptate cerințelor utilizatorului.
- Solutia trebuie sa permită salvarea rapoartelor create și rularea acestora manual sau automat la anumite intervale de timp și trimiterea lor sub formă de mesaje de e-mail către persoanele selectate.
- Solutia trebuie sa ofere instrumente de inventariere și audit central, precum și managementul configurației, inclusiv cel puțin:

- să permită distribuirea și instalarea de la distanță a noilor versiuni și actualizări de sistem
- să permită crearea de copii de rezervă ale firewall-urilor gestionate
- să permită distribuirea și instalarea de la distanță a actualizărilor de semnături
- permite auditarea/validarea configurației dispozitivului înainte de aprobarea acestuia - permite salvarea diferitelor versiuni de configurare ale firewall-urilor gestionate
- permite procedura de înlocuire a unui dispozitiv deteriorat cu unul nou, astfel încât gestionarea, înregistrarea și sistemul de raportare înțelege că noul dispozitiv înlocuiește dispozitivul deteriorat
- informați despre modificările aduse configurației sistemului.

6. Livrare, ambalare, etichetare, transport și asigurare pe durata transportului

În cadrul prezentei achiziții, produsele și materialele încorporate ce urmează a fi achiziționate trebuie să fie noi, nefolosite, de asemenea, vor fi oferite cele mai recente modele. Produsele și materialele încorporate ce urmează a fi achiziționate ar trebui să încorporeze cele mai recente îmbunătățiri în proiectare și materiale. Orice referire la standarde va fi însoțită de mențiunea "sau echivalent", fiind în sarcina ofertantului de a demonstra echivalența în cazul în care produsele furnizate sunt conforme cu un standard echivalent celui menționat în Caietul de sarcini.

Specificațiile tehnice cuprinse în acest caiet de sarcini sunt cerințe minimale și obligatorii și trebuie îndeplinite în acest sens, sau în mecanisme echivalente ce îndeplinesc în mod minimal cerințele și funcționalitățile specificate. În acest sens, oferta de bază prezentată care se abate de la prevederile Caietului de sarcini va fi luată în considerare, dar numai în măsură în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerințelor minimale din Caietul de sarcini.

Propunerea tehnica va fi elaborată astfel încât să reflecte asumarea de către ofertant a îndeplinirii fără echivoc a tuturor cerințelor și obligațiilor prevăzute în Caietul de sarcini.

Specificațiile tehnice care indică o anumită origine, sursă, producție, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație, sunt menționate doar pentru identificarea cu ușurință a tipului de produs și nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produs; aceste specificații vor fi considerate ca având mențiunea "sau echivalent".

Având în vedere prevederile Directivei 18/2004 și Directivelor 2014/24/UE, respectiv 2014/25/UE, specificațiile tehnice care fac trimitere la standarde naționale sau la transpunerile unor standarde europene se vor citi "sau echivalent".

Orice referire la standarde va fi considerată ca având mențiunea “sau echivalent”, fiind în sarcina ofertantului de a demonstra echivalența în cazul în care produsele fumizate sunt conforme cu un standard echivalent celui menționat în Caietul de sarcini.

În cadrul ofertei tehnice, pentru fiecare produs, se va preciza în mod clar marca, denumire produs, nume, model, producător.

Prezentul caiet de sarcini conține specificații tehnice și face parte integrantă din documentația de atribuire în vederea participării la licitația deschisă în vederea încheierii unui contract privind achiziția de echipamente virtuale NGFW.

Achiziția de echipamente Virtuale NGFW se va face conform celor precizate.

Toate produsele vor avea certificat de calitate și / sau conformitate care includ detaliile și certificatele.

La depunerea ofertei, produsele nu trebuie să aibă anunțat sfârșitul perioadei de vânzare sau de suport (EOL -End of Life/ EOS - End of Sale/Support). Ofertantul va prezenta o declarație pe proprie răspundere prin care își vă asumă livrarea pentru toate pozițiile de echipamente noi și că nu este anunțat sfârsitul perioadei de vânzare sau de suport.

Produsele ofertate vor fi certificate pentru conformitate CE și vor respecta toate cerințele impuse de legislația, standardele și reglementările aplicabile în România, inclusiv cele cu privire la Protecția Mediului și principiile DNSH, Asigurarea Calității, PSI, Securitate și Sănătate în Muncii.

7. Garanție/Termen de valabilitate

Garanția este obligația contractuală a vânzătorului față de cumpărător, fără solicitarea unor costuri suplimentare, de restituire a prețului plătit de cumpărător/de reparare sau de înlocuire a produsului cumpărat, dacă acesta nu corespunde condițiilor enunțate în declarațiile referitoare la garanție. Garanția trebuie să precizeze elementele de identificare a produsului, termenul de garanție, modalitățile de asigurare a garanției - întreținere, reparare, înlocuire - inclusiv denumirea și adresa vânzătorului și ale locației unde se prestează serviciile de mentenanță. În concordanță cu dispozițiile art. 1.716 - 1.718 Cod civil, care reglementează garanția pentru buna funcționare a bunurilor, în practica contractelor de furnizare sunt practicate 2 concepte:

- garanția legală - este obligatorie din punct de vedere juridic pentru ofertant și reprezintă perioada în care produsul trebuie să respecte specificațiile sale inițiale, să aibă proprietățile pentru care a fost cumpărat; uzual, răspunderea vânzătorului este angajată dacă lipsa de conformitate apare într-un anumit termen, calculat de la livrarea produsului;

- garanția tehnică/comercială - garanția solicitată prin documentația de atribuire și/sau cea oferită/decisă de distribuitor sau producător - în acest termen, distribuitorul sau producătorul se angajează ca, în cazul în care produsul se defectează/nu funcționează în parametrii să aducă produsul în parametrii de conformitate; costul acestei garanții intră în prețul produsului respectiv atunci când garanția tehnică este egală cu garanția legală (intră în prețul produsului respectiv) sau presupune costuri suplimentare față de prețul produsului, atunci când este mai mare decât garanția legală (aceste costuri suplimentare urmează a fi incluse în estimarea valorii achiziției).

Toate produsele trebuie să fie acoperite de garanție. Perioada de garanție începe de la data [ex.: data acceptării produselor]. Cerințele privind garanția pot acoperi: durata garanției, termenul de la care începe să curgă perioada de garanție, condițiile de acoperire, precum și operațiunile accesorii pe care furnizorul trebuie să le asigure în perioada de garanție. Dacă există cerințe privind o perioada de garanție extinsă, autoritatea/entitatea contractantă va introduce informații referitoarele la garanția extinsă. Garanția trebuie să acopere toate costurile rezultate din remedierea defectelor în perioada de garanție

Pentru scopul acestei proceduri, noțiunea de “defect” trebuie interpretată ca un comportament al produsului diferit de [ex: parametrii agreați de părți, etc.] având ca referință pentru determinarea defectelor [specificațiile tehnice SAU cerințe funcționale] din caietul de sarcini.

Termenul de livrare este cel menționat pentru fiecare produs în parte, respectiv 30 de zile calendaristice. Produsele vor fi livrate cu respectarea tuturor cerințelor cantitative și calitative, la locul de livrare indicat de autoritatea/entitatea contractantă.

Destinația de livrare este Calea Victoriei, nr. 152, sector 1, București, cod poștal 010096.

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

8. Instalare, punere în funcțiune, testare

După instalare și punere în funcțiune, autoritatea/entitatea contractantă și/sau contractantul va efectua teste funcționale ale produsului.

Testarea produsului va avea în vedere următoarele elemente:
autoritatea/entitatea contractantă poate să introducă informații despre activitățile

realizate pentru testarea echipamentului, care pot include următoarele, după caz la cele ce urmează: ex. testare în condiții de utilizare "reală"; metode de testare; funcționalități care trebuie testate; criterii de succes/eșec ale testelor; calendar/interval de testare, etc.

Pentru a asigura funcționarea produsului la parametri agreați, contractantul va efectua testarea pe cheltuiala sa și fără nici un fel de costuri din partea autorității/entității contractante.

9. Mentenanța corectivă în perioada de garanție

Serviciile de mentenanță corectivă din perioada de garanție sunt incluse în prețul bunului. În cazul în care echipamentul/produsul respectiv funcționează pe perioada de garanție fără defecțiuni sau funcționează în parametrii optimi stabiliți se poate ca aceste servicii să nu fie solicitate de autoritatea/entitatea contractantă. Mentenanța corectivă reprezintă totalitatea operațiunilor de intervenție la un echipament/produs care se efectuează ca urmare a unor defecțiuni sau funcționării în afara parametrilor optimi cu scopul de a restabili capacitatea de funcționare optimă a echipamentului/produsului.

Mentenanța corectivă include localizarea, diagnosticarea defectelor, inclusiv intervenția pentru restabilirea bunei funcționari și trebuie efectuată pentru toate părțile componente ale produsului atunci când autoritatea/entitatea contractantă semnalează un incident.

Contractantul trebuie să includă în costurile mentenanței corectivă toate costurile aferente intervenției, cum ar fi, dar fără a se limita la: forța de muncă, piesele de schimb, alte materiale sau consumabile, costurile cu transportul echipamentului/produsului de la sediul beneficiarului la locul efectuării operațiilor de mentenanță corectivă, dacă este cazul.

Activitățile de mentenanță corectivă se vor realiza, de regulă remote exceptând cazul în care soluția ofertată este total nefuncțională definită ca "worst case scenario". În acest caz activitățile de mentenanță corectivă necesită operații tehnologice mai complicate, acestea se vor executa la sediul contractantului, caz în care se întocmește un proces-verbal de intervenție.

După fiecare intervenție corectivă, contractantul trebuie să se efectueze teste de funcționare care să demonstreze că echipamentul/produsul funcționează în parametrii optimi și să prezinte un raport care să includă activitățile realizate, precum și rezultatele testelor de funcționare.

10. Mentenanța preventivă în perioada de garanție

Contractantul trebuie să efectueze mentenanță preventivă a produsului anual/an (o data pe an) în perioada de garanție. Operațiunile care trebuie efectuate de contractant pentru fiecare intervenție sunt: cele stabilite de către Contractant de comun acord cu autoritatea/entitatea contractantă.

Contractantul este responsabil pentru realizarea operațiunilor de mentenanță preventivă. Înainte de efectuarea operațiunilor de mentenanță preventivă, contractantul comunică autorității/entității contractante lista operațiunilor de mentenanță care trebuie efectuate. Operațiuniile de mentenanță preventivă se vor realiza remote, este posibil ca mentenanță preventivă să trebuiască a fi realizată în afara orelor normale de lucru sau la sfârșit de săptămână sau în sărbători legale. Orele de lucru normale ale autorității/entității contractante sunt de luni pana joi intervalul orar 08:30 – 17:00, iar vineri intervalul orar 08:30 – 14:30.

Operațiunile de mentenanță preventivă care necesită o oprire a produsului se efectuează în afara orelor normale de activitate. Datele exacte vor fi agreate cu autoritatea/entitatea contractantă. Mentenanța preventivă trebuie să acopere toate costurile aferente intervenției. Operațiunile de mentenanța preventivă trebuie efectuate în condiții de securitate. După fiecare intervenție preventivă, contractantul trebuie efectueze teste de funcționare ale produsului și să prezinte un raport care să includă activitățile realizate.

11. Suport tehnic

Pe toată durata contractului, atât în perioada de garanție cât și după expirarea perioadei de garanție, după caz, Contractantul va asigura suport tehnic Contractantul va asigura un punct de contact dedicat personalului autorizat al autorității/entității 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.

Contractantul va răspunde în timp util la orice incident semnalat de autoritatea/entitatea contractantă, în funcție de nivelul incidentului. Fiecare incident este caracterizat de un nivel de prioritate, care va evidenția impactul acestuia asupra funcționalităților produsului.

Nivelele de prioritate sunt:

i. Urgent - incidentul are impact major asupra funcționarii produsului. Problema împiedică desfășurarea activității Autorității/entității contractante.

ii. Critic - impact semnificativ asupra funcționarii produsului. Problema împiedică desfășurarea în condiții normale a activității Autorității/entității contractante. Nici o soluție alternativa nu este disponibilă, însă activitatea Autorității/entității contractante poate totuși continua, însă într-un mod restrictiv.

iii. Major - impact mediu asupra desfășurării activității autorității/entității contractante. Problema afectează minor funcționalitățile produsului. Impactul reprezintă un inconvenient care necesita soluții alternative pentru refacerea funcționalităților.

iv. Minor - impact minim asupra desfășurării activității Autorității/entității contractante. Problema nu afectează funcționalitățile produsului. Rezultatul este o eroare minora care nu împiedică desfășurarea în bune condiții a activității Autorității/entității contractante.

Contractantul trebuie să asigure disponibilitatea serviciilor de suport tehnic. În cazul incidentelor cu prioritate "urgent" intervenția va fi asigurată 24x7, din momentul primirii sesizării și până la remedierea definitiva a problemei și asigurarea funcționalității integrale a produsului. Contractantul va trebui să respecte următorii timpi de răspuns, corelați cu nivelul de prioritate a incidentului - aceștia se vor particulariza în funcție de specificul obiectul contractului, cei de mai jos fiind cu caracter orientativ:

Nivel prioritate	Timp de răspuns	Timp de implementare soluție provizorie	Timp de rezolvare*
Urgent	2 ore	24 ore	4 zile
Critic	4 ore	48 ore	7 zile
Major	8 ore	4 zile	14 zile
Minor	24 ore	8 zile	30 zile

**În cazul în care software-ul de bază, aplicațiile sau tehnologiile folosite necesită corectarea unui bug și/sau construcția unui patch de la producător, timpul de remediere se va modifica cu timpul necesar producătorului să construiască patch-ul și/sau să corecteze bug-ul.*

Legendă:

- Timp de răspuns: timpul scurs de la anunțul inițial înregistrat de client prin metodele de comunicare stabilite în procedura de suport tehnic (stabilită de comun acord ulterior semnării contractului de furnizare) și răspunsul primit de la echipa de suport tehnic a furnizorului către client. Răspunsul va conține termenul până la care incidentul va fi remediat, cel puțin printr-o soluție alternativă temporară. Timpul de remediere menționat în tabel se va prelungi cu durata de timp necesară pentru clarificarea incidentului.
- Timp de remediere: durata de timp de la constatarea de către furnizor a defecțiunii până la implementarea soluției finale.

- Remediere provizorie/temporară: o modificare în cadrul procedurilor sau datelor care permite desfășurarea activității utilizatorului, ca soluție care evită temporar manifestarea defectului reclamat.

Timpii prezentați în tabelul de mai sus sunt calculați din momentul în care furnizorul a fost înștiințat de apariția problemelor.

Nerespectarea timpilor de mai sus da dreptul Autorității/entității contractante de a solicita penalități/daune interese în conformitate cu clauzele contractului de achiziție publică/sectorială de produse.

12. Atribuțiile și responsabilitățile părților

În raport cu produsele solicitate și cu cerințele stipulate în prezentul Caiet de Sarcini, responsabilitățile și atribuțiile părților sunt:

Ofertantul are următoarele obligații principale:

a. mobilizarea de resurse suficiente și cu expertiză adecvată pentru a asigura gestionarea contractului, astfel cum este solicitat la nivelul Caietului de Sarcini;

b. îndeplinirea obligațiilor contractuale, cu respectarea bunelor practici din domeniu, a prevederilor legale și contractuale relevante, astfel încât să se asigure că obligațiile sunt îndeplinite la parametrii solicitați;

c. asigurarea unui grad de flexibilitate în planificarea modalității de gestionare a contractului, pe toată durata de derulare a contractului;

d. transmiterea datelor de identificare și de contact ale personalului alocat pentru executarea contractului;

e. colaborarea cu personalul autorității/entității contractante alocat pentru verificarea produselor livrate și realizarea recepțiilor;

f. reducerea, în măsura posibilă, la minim, a situațiilor de întârzieri în efectuarea livrărilor, minimizând astfel impactul negativ asupra activității autorității/entității contractante;

g. asigurarea că orice documente, documentații și/sau instrucțiuni furnizate către personalul autorității/entității contractante sunt exacte și elaborate în conformitate cu bunele practici specifice în domeniu;

h. prezentarea rapoartelor solicitate de personalul autorității/entității contractante, potrivit cerințelor de raportare stabilite prin Contract;

i. colaborarea cu personalul autorității/entității contractante alocat pentru furnizarea produselor care fac obiectul contractului și pentru asigurarea serviciilor accesorii.

Autoritatea/entitatea contractantă are următoarele obligații principale:

a. desemnarea unei persoane sau a unei echipe pentru monitorizarea contractului;

b. punerea la dispoziția Contractantului a tuturor informațiilor disponibile și necesare pentru derularea contractului în timpul stabilit și la nivelul de calitate prevăzut în Caietul de Sarcini;

c. asigurarea accesului în spațiile în care urmează a se realiza livrarea, după caz instalarea produselor;

d. mobilizarea tuturor resurselor care sunt în sarcina sa, pentru buna derulare a contractului;

e. colaborarea cu Contractantul pentru a identifica în timp util orice eventuale probleme care ar putea apărea pe parcursul derulării contractului;

f. asigurarea acurateței oricăror informații puse la dispoziția Contractantului pe durata derulării contractului;

g. monitorizarea îndeplinirii tuturor cerințelor din Caietul de Sarcini și a oricăror elemente ale Propunerii Tehnice și Financiare pe durata derulării contractului;

h. notificarea Contractantului prin canalele de comunicație puse la dispoziție de acesta privind orice incidente sau disfuncționalități care intervin pe perioada de derulare a contractului;

i. verificarea tuturor documentelor asociate recepției produselor și serviciilor suport care fac obiectul contractului, respectiv care confirmă furnizarea produselor potrivit condițiilor de calitate stabilite în Caietul de sarcini.

13. Documentații ce trebuie furnizate autorității/entității contractante în legătură cu produsul

Toate produsele incluse în prezentul contract vor fi furnizate împreună cu documentația adecvată, în limba română.

Documentațiile obligatorii pe care Contractantul trebuie să le livreze autorității/entității contractante în cadrul contractului sunt:

- Declarația sau certificatul de conformitate;
- Garanția produselor emisă de furnizor sau de producător;
- Certificat de calibrare;
- Manualele de folosire;

14. Recepția produselor

Recepția produselor se va efectua pe baza de proces verbal semnat de contractant și reprezentanții autorității/entității contractante.

Recepția produselor se poate 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 Ministerul Economiei, Digitalizării, Antreprenoriatului și Turismului din Calea Victoriei, nr. 152, sector 1, Bucureşti, cod 010096;
b) recepția calitativă se va realiza după instalare, punere în funcțiune și testare a produselor și, după caz, toate defectele au fost remediate.
Procesul verbal de recepție calitativă și cantitativă va include unul din următoarele rezultate:
a) admiterea recepției cu sau fără obiecții;
b) suspendarea recepției;

Comisia de recepție recomandă suspendare recepției când:

i. se constată existența unor neconformități, neconcordanțe, defecte ori deficiențe care sunt de natură să afecteze utilizarea produsului/produselor conform destinației sale/lor, dar care pot fi remediate;

ii. se constată existența unor produse realizate necorespunzător sau nefinalizate, care pot afecta cerințele fundamentale aplicabile, dar care pot fi remediate;

iii. se constată existența, în mod justificat, a unor suspiciuni rezonabile cu privire la calitatea produselor și este necesară realizarea unor expertize tehnice, încercări și teste suplimentare pentru a le clarifica;

iv. Contractantul nu pune la dispoziția comisiei de recepție documentele prevăzute în contract și caietul de sarcini (dacă este cazul).

În cazul în care comisia de recepție decide suspendarea procesului de recepție, aceasta încheie un proces-verbal de suspendare a procesului de recepție în care consemnează decizia de suspendare, măsurile recomandate în scopul remedierii aspectelor constatate, precum și termenul de remediere, iar autoritatea/entitatea contractantă comunică Contractantului decizia comisiei în maximum 3 zile lucrătoare de la luarea la cunoștință a procesului- verbal de suspendare a procesului de recepție, împreună cu un exemplar al acestuia. Termenul de remediere nu poate depăși 90 de zile de la data încheierii procesului-verbal de suspendare a procesului de recepție. În cazul în care Contractantul nu remediază aspectele constatate și nu adoptă măsurile recomandate în cadrul procesului- verbal de suspendare a procesului de recepție în termenul stabilit, comisia de recepție va decide respingerea recepției.
c) respingerea recepției (dacă se constată vicii care nu pot fi remediate și care, prin natura lor, împiedică realizarea uneia sau a mai multor exigențe esențiale).

15. Modalități și condiții de plată

Contractantul va emite factura pentru produsele livrate și acceptate [conform prevederilor contractuale/conform graficului de plăți, anexă la contract]. Plățile în favoarea contractantului se vor efectua [conform graficului de plăți] în termen de maxim 30 de zile de la momentul semnării procesului-verbal de recepție cantitativă și calitativă, conform prevederilor OMFP nr. 1792/2002. Fiecare factură va avea

menționat numărul contractului, datele de emitere și de scadența ale facturii respective. Factura va fi emisă după semnarea de către autoritatea/entitatea contractantă a procesului verbal de recepție calitativă și cantitativă, acceptat, după livrare, instalare și punere în funcțiune. Procesul verbal de recepție calitativă și cantitativă va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute la "5. Documentații ce trebuie furnizate autorității/entității contractante în legătură cu produsul".

Cadrul legal care guvernează relația dintre autoritatea/entitatea contractantă și contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă).

Ofertantul devenit contractant are obligația de a respecta 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 enumerate în anexa X la Directiva 2014/24, respectiv:

i. Convenția nr. 29 a OIM privind munca forțată;

Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului, dacă este cazul.

Pe parcursul derulării Contractului, Autoritatea/entitatea contractantă verifică la intervale stabilite și comunicate prin Caietul de sarcini dacă toate activitățile planificate au fost realizate conform cerințelor și că produsele au fost livrate și acceptate

Elaborat,

Adrian STĂNILOIU