ROMÂNIA
MINISTERUL APĂRĂRII NAŢIONALE
COMANDAMENTUL APĂRĂRII CIBERNETICE
Nr. BA-1245 din 26.05.2026
-Bucureşti-

NECLASIFICAT
Exemplarul unic
Dosar nr. ___
Termen de păstrare: 5 ani

SPECIFICAȚIE TEHNICĂ PENTRU ACHIZIȚIE

"Soluție pentru protecția aplicațiilor web"

Revizuită în urma avizului conform condiționat nr. 5815/21.05.2026/DGEDACMISP

BUCUREȘTI
2026

Pagină albă

CUPRINS

1. SCOP

Prezenta specificație stabilește cerințele tehnice pentru achiziționarea unui complet software al cărui componente să asigure un nivel de protecție unificată la nivelul traficului de rețea, traficului web, sa optimizeze controlul asupra aplicațiilor, să permită gestionarea securizată a conexiunilor VPN, să integreze funcționalități avansate, tip ML/AI și funcționalități de detecție și prevenire a amenințărilor.

2. CERINŢE

2.1 Cerinţe privind configuraţia completului

<table>
<tr><th>Nr. cerință</th><th>CERINŢA</th></tr>
<tr><td>C1.</td><td>Completul trebuie să aibă compunerea din tabelul următor:
<table>
<tr><th>Nr. crt.</th><th>Tip componentă</th><th>UM</th><th>Cantitate</th></tr>
<tr><td>1.</td><td>Aplicație software (VM) de tip firewall NGFW</td><td>Lic.</td><td>1</td></tr>
<tr><td>2.</td><td>Aplicație software (VM) de tip web si API firewall</td><td>Lic.</td><td>1</td></tr>
</table></td></tr>
</table>

2.2 Cerinţe de performanţă şi specifice *aplicației software (VM) de tip firewall NGFW*

Nr. cerință	CERINŢA
C2.	Soluția trebuie să asigure îmbunătățirea vizibilității și controlului asupra traficului intern și extern.
C3.	Soluția trebuie să asigure consolidarea politicilor de securitate printr-o platformă centralizată și ușor de administrat.
C4.	Soluția trebuie să asigure un nivel ridicat de disponibilitate și redundanță.
C5.	Soluția trebuie să asigure implementarea unor măsuri pro active împotriva amenințărilor cibernetice, inclusiv cele de tip zero-day.
C6.	Soluția trebuie să asigure crearea unui cadru flexibil care să permită adaptarea ulterioară la nevoile în schimbare ale instituției, inclusiv extinderea către cloud și rețele hibride.
C7.	Formatul soluției trebuie să fie de tip mașină virtuala(VM).
C8.	Soluția trebuie să dispună de un sistem de operare dedicat. Nu se acceptă sisteme de operare de uz general sau instalare de module gratuite/open source pentru asigurarea cerințelor solicitate.

C9.	Soluția trebuie să îndeplinească următoarele capabilități: • Funcționalitate firewall cu inspecție avansată a pachetelor (deep packet inspection); • Sistem de prevenire a intruziunilor (IPS) cu actualizări automate ale semnăturilor; • Suport VPN pentru acces securizat de la distanță și interconectare între sedii; • Control al aplicațiilor și filtrare web bazate pe categorii predefinite și personalizabile; • Protecție antivirus, anti-malware și anti-botnet integrată; • Capacitate de decriptare și inspecție a traficului SSL/TLS (atât pentru trafic de intrare, cât și de ieșire).
C10.	Soluția trebuie să permită configurare în mod high availability în variantele active-active, active-pasive, iar în varianta active-active.
C11.	Soluția trebuie să dispună de funcționalități de proxy atât explicit, cât și implicit.
C12.	Soluția permite colectarea informațiilor device-urilor conectate la rețea precum adresa MAC, adresa IP, sistem de operare, hostname, etc.
C13.	Soluția suportă hipervizoare private de tipul VMware, Hyper-V, KVM, Proxmox, OpenStack și hipervizoare publice: AWS, Azure, Oracle Cloud, Google Cloud, IBM Cloud, AliCloud.
C14.	Soluția trebuie să aibă următoarele capacități de throughput adecvate dimensiunii rețelei folosind KVM: • Firewall Throughput IPv4/IPv6 (packete UDP de 512 bytes): minim 19 Gbps fără accelerare, minim 36 Gbps cu accelerare; • IPSec VPN Throughput: minim 5.5 Gbps fără accelerare, minim 32 Gbps cu accelerare; • IPS Throughput (Enterprise Mix): minim 6 Gbps; • NGFW Throughput: minim 4.8 Gbps; • Sesiuni concurente (TCP): minim 6 M; • Sesiuni noi/sec: minim 250.000.
C15.	Soluția trebuie să identifice disponibilitatea serviciilor de tipul: • Link status monitor; • Link failover; • Server Load balancing.
C16.	Soluția trebuie să asigure segmentare avansată multi-tentant, prin implementarea de instanțe VRF(Virtual Routing and Forwarding) și suport pentru domenii de virtualizare.

C17.	Soluția trebuie să dispună de un sistem de prevenire a intruziunilor(IPS) cu următoarele capabilități: • Detectarea și blocarea proactivă a atacurilor cunoscute și necunoscute, prin analiza bazată pe semnături și comportament; • Actualizarea automată și frecventă a semnăturilor de atac dintr-o bază de date menținută de producător; • Capacitatea de a funcționa în mod inline fără degradarea semnificativă a performanței; • Posibilitatea de configurare a acțiunilor la detectarea unui atac (permitere, blocare, alertare, carantinare pe durată cconfigurabilă); • Protecție împotriva atacurilor de tip DoS/DDoS, port scanning, exploatarea vulnerabilităților din aplicații sau sisteme de operare; • Posibilitatea de a adăuga semnături noi personalizate; • Posibilitatea de a adăuga semnături SNORT (direct sau utilizând instrumente de conversie); • Detecție locală de atacuri de tip Zero-Day utilizând un engine de tip IPS care folosește AI/ML; • Identificarea atacurilor de tip login brute force prin configurarea numărului de încercări și a duratei de observabilitate; • Suport pentru IPv6.
C18.	Soluția trebuie să includă o funcționalități de inspecție detaliată a pachetelor – Deep Packet Inspection (DPI), permițând: • Analiza conținutului pachetelor de rețea în timp real, dincolo de antetele de rețea (L3/L4), cu identificarea aplicațiilor, protocoalelor și tipului de conținut; • Identificarea și clasificarea automată a aplicațiilor, indiferent de port (ex: Facebook, YouTube, Skype, Dropbox, aplicații de tip peer-to-peer, aplicații VPN, protocoale criptate etc.); • Inspecția traficului criptat SSL, TLS1.1, TLS1.2, TLS1.3.
C19.	Soluția trebuie să includă funcționalități de protecție Antivirus și Anti-Malware cu următoarele caracteristici: • Detectarea, blocarea și eliminarea virușilor, troienilor, spyware, ransomware și altor forme de cod malițios; • Scanarea traficului în timp real (inclusiv HTTP, HTTPS, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS, SSH) și a fișierelor descărcate; • Analiza comportamentală pentru identificarea codului malițios necunoscut; • Integrare cu funcționalitatea de sandboxing în cloud sau locala, daca este disponibila in soluție, pentru analiza avansata a fișierelor suspecte; • Detectare conținutului malițios folosind AI/ML; • Suport pentru IPv6.

C20.	Soluția trebuie să includă funcționalitatea de Filtrare Web (Web Filtering) cu următoarele capabilități: • Clasificarea automată a site-urilor web în categorii (ex: social media, jocuri, streaming, pornografie, phishing etc.); • Posibilitatea de a permite, bloca sau monitoriza accesul la diferite categorii de site-uri; • Suport pentru filtrarea conținutului atât pentru traficul HTTP, cât și HTTPS; • Posibilitatea de a defini reguli pe bază de utilizator, grup sau IP; • Posibilitatea definirii de liste statice cu URL-uri permise/blocate; • Posibilitatea de configurare a categoriilor globale prin suprascriere; • Alerte și rapoarte pentru încercările de acces la conținut restricționat.
C21.	Soluția trebuie să includă următoarele funcționalități de VPN: • Suport pentru conexiuni VPN site-to-site și client-to-site (remote access); • Compatibilitate cu standardele IPSec (IKEv1 și IKEv2), cu algoritmi de criptare și autentificare puternici (AES-256, SHA-2, DH Group 14+); • Posibilitatea de definire a politicilor de criptare per tunel, cu opțiuni de failover automat; • Suport pentru autentificare pe bază de pre-shared key (PSK) și certificate digitale; • Integrare cu sisteme de autentificare externă (ex: LDAP, RADIUS, Active Directory); • Posibilitatea de limitare a accesului în funcție de IP sursă, utilizator sau grup; • Monitorizare în timp real a tunelurilor VPN active; • Suport pentru reconectare automată în cazul pierderii temporare a conexiunii; • Interoperabilitate cu alte soluții VPN de la terți (comunicare cu echipamente de la alți producători); • Posibilitatea de limitare a accesului în funcție de IP sursă al stațiilor, daca acestea sunt înregistrate în platforma de management a clientului de; • Asigurarea accesului la diverse resurse de rețea în funcție de îndeplinirea anumitor criterii de compliantă de securitate;

C22.	Soluția trebuie să includă funcționalități de rutare inteligentă a traficului cu următoarele caracteristici: • Agregare inteligentă a legăturilor WAN: posibilitatea de a utiliza simultan mai multe conexiuni WAN (furnizori diferiți, tipuri diferite – ex. MPLS, broadband, LTE/5G); • Seamless failover: comutare automată între conexiuni WAN în cazul pierderii sau degradării performanței, fără întreruperea sesiunilor active; • Selectarea dinamică a rutelor (Dynamic Path Selection): rutare a traficului pe baza performanței în timp real (jitter, pierderi de pachete, latență) în funcție de aplicație, destinație sau utilizator; • Optimizare pentru aplicații critice: prioritizarea aplicațiilor esențiale (VoIP, videoconferințe, aplicații ERP etc.) prin politici QoS (Quality of Service) configurabile; • Vizibilitate completă asupra traficului: interfața grafică pentru monitorizarea performanței legăturilor și a rutelor utilizate; • Suport pentru criptarea traficului între sedii: tuneluri securizate între puncte cu criptare IPSec; • Administrare centralizată a politicilor de rutare cu posibilitatea de definire a rutelor logice, a regulilor de comutare și a priorităților per aplicație; • Compatibilitate cu IPv4 și IPv6.
C23.	Soluția trebuie să includă funcționalități de filtrare de tipul: • Video Filtering; • File Filtering; • DNS Filtering.
C24.	Soluția trebuie să includă funcționalități de control asupra aplicațiilor cu următoarele capabilități: • Identificarea și clasificarea automată a aplicațiilor, indiferent de port (ex: Facebook, YouTube, Skype, Dropbox, aplicații de tip peer-to-peer, aplicații VPN, protocoale criptate etc.); • Controlul la nivel de aplicație; • Traffic shaping per aplicație; • Diff Serv per aplicație.
C25.	Soluția trebuie să includă suport pentru protocoale și standarde de rețea uzuale: • IPv4/IPv6; • VLAN; • OSPF; • BGP; • ISIS; • BFD; • PBR (policy-based routing); • NAT/PAT; • Multicast; • Link aggregation (802.3ad).
C26.	Soluția trebuie să includă suport pentru session helpers: SIP, SIP-ALG, DNS, alte protocoale.
C27.	Soluția trebuie să includă suport DHCP: DHCP server, DHCP relay și servere multiple pentru DHCP relay.

C28.	Soluția trebuie să permită administrarea interfeței de management prin următoarele metode: • Interfața centralizata, accesibila prin web, pentru configurare, monitorizare și raportare; • SSH; • Consolă.
C29.	Soluția trebuie să dispună de interfață suplimentară de management prin API.
C30.	Soluția trebuie să dispună de o platformă de management centralizat.
C31.	Soluția trebuie să suporte următoarele protocoale de monitorizare: • SNMP v1/v2; • SNMP v3; • Syslog.
C32.	Soluția trebuie să suporte mecanisme de notificare prin e-mail.
C33.	Pentru autentificarea administratorului soluția trebuie să dispună de: • Bază de date locală; • Integrare Active Directory; • Integrare LDAP/RADIUS/Tacacs+; • Restricționare acces de la anumite IP; • Suport pentru autentificare MFA.
C34.	Soluția trebuie să implementeze mecanisme de control al accesului pe baza de roluri (RBAC) pentru utilizatorii cu privilegii administrative.
C35.	Soluția trebuie să dispună de o interfață grafică de analiză în timp real și istorică a traficului și a evenimentelor de securitate.
C36.	Soluția trebuie să dispună de funcționalități de automatizare a răspunsului la incidente printr-o interfață grafică de tip flow-base și să permită: • Configurarea logicii de automatizare cu reguli de tip trigger-action; • Monitorizarea și auditarea execuției acțiunilor automate, cu înregistrarea completă a contextului și deciziilor aplicate; • Capacitatea de a extinde fluxurile automate către alte echipamente din rețea (prin API-uri, webhook-uri sau protocoale standard).
C37.	Soluția trebuie să permită definirea de politici automate de răspuns, declanșate de evenimente sau alerte generate de componentele de securitate ale sistemului (IPS, antivirus, filtrare web etc.).Exemple de acțiuni automate care pot fi configurate: • Blocarea automată a unei adrese IP sursă după detectarea unei încercări de atac; • Izolarea automata a unui dispozitiv compromis în rețea (prin schimbare de VLAN sau aplicare de politici restrictive); • Dezactivarea temporară a accesului unui utilizator în urma detectării unei scurgeri de date; • Notificare automată prin email sau integrare cu sisteme externe (ex. ticketing, SIEM).

C38.	Soluția trebuie să ofere posibilitatea de a permite actualizări dinamice de pachete de semnături, furnizate dintr-o bază de date globală, actualizată permanent: • Control aplicații; • IPS; • Anti-malware; • Antivirus; • Filtrare Web; • Firewall; • Routing; • PBR.
C39.	Soluția dispune de licențe suplimentare care vor asigura funcționarea următoarelor: • Access remote VPN (inclusiv client); • Rutare inteligenta a traficului; • Posibilitatea de a utiliza minim 8 vCPU.

2.3 Cerințe de performanță și specifice *aplicației software(VM) de tip web si API firewall*

Nr. cerință	CERINȚA
C40.	Formatul soluției trebuie să fie de tip mașină virtuala (VM).
C41.	Soluția trebuie să dispună de un sistem de operare dedicat. Nu se acceptă sisteme de operare de uz general sau instalare de module gratuite/open source pentru asigurarea cerințelor solicitate.
C42.	Soluția trebuie să permită configurare în mod high availability în variantele active-pasive și active-active pentru volum mare de trafic.
C43.	Soluția trebuie să permită implementarea în următoarelor scenarii arhitecturale: • Reverse proxy; • Inline transparent; • Proxy în mod transparent; • Offline sniffing.
C44.	Soluția trebuie să suporte următoarele hipervizoare: • Private: VMware, Hyper-V, KVM, OpenStack • Publice: AWS, Azure, Oracle Cloud, Google Cloud, Alibaba
C45.	Soluția trebuie să aibă capacitate de throughput adecvata dimensiunii rețelei (folosind KVM): • Trafic HTTP : minim 3 Gbps; • Trafic HTTPS: minim 1 Gbps; • Fără licențiere pentru numărul aplicațiilor web protejate.

C46.	Soluția trebuie să dispună de opțiuni de definire a politicilor și profilelor de securizare prin: • Politici de securitate predefinite; • Opțiune de partajare al accesului administrativ pentru configurația profilelor și politicilor de securizare pentru aplicațiile web protejate, prin utilizarea de domenii administrative.
C47.	Soluția trebuie să dispună de o opțiunea de autentificare a utilizatorilor care să poată verifica credențialele prin verificare locală sau externă prin protocoalele RADIUS (inclusiv autentificare prin doi factori), LDAP.
C48.	Soluția trebuie să ofere suport pentru Single Sign On a utilizatorilor pe aplicațiile Microsoft protejate (Outlook Web Access, Sharepoint).
C49.	Soluția trebuie să permită autentificare adițională a clienților prin certificate digitale X.509 (pentru aplicații HTTPS) – validare locala a certificatului (folosind un certificat importat al CA-ului semnatar) și posibilitate de trimitere a informațiilor legate de acesta către aplicația protejata.
C50.	Soluția trebuie să aibă posibilitate de a verifica validitatea certificatelor digitale X.509 ale clienților.
C51.	Soluția trebuie să asigure protecție la nivel de aplicație împotriva atacurilor de tip: • Browser Exploits; • Brute Force Login; • Buffer Overflows; • Command Injection; • Cookie Tampering/Poisoning; • Cross Site Request Forgery; • Cross Site Scripting; • Denial Of Service; • Directory Traversal; • Forms Tampering; • Hidden Field Manipulation; • HTTP Header overflow; • Outbound Data Leakage; • Local file Inclusion; • Man in the Middle attacks; • Remote File Inclusion; • Session Hijacking; • Site Reconnaissance; • SQL Injection; • XML Intrusion Prevention.
C52.	Soluția trebuie să ofere protecție DLP cu reguli predefinite și reguli configurabile cu suport pentru expresii de tip Regex.
C53.	Soluția trebuie să ofere posibilitatea de a defini manual semnături de atac noi.
C54.	Soluția trebuie să ofere posibilitatea de a bloca pe bază de reputație sursele cu potențial malițios.
C55.	Soluția trebuie să ofere protecție împotriva botnet, crawler, search engine.
C56.	Soluția trebuie să ofere posibilitatea de a monitoriza și bloca traficul provenit dintr-o anumită regiune geografică sau țară.
C57.	Soluția trebuie să ofere protecție împotriva scanării fișierelor de conținut malițios (scanare antivirus).

C58.	Soluția trebuie să ofere protecție DoS pentru atacuri la nivel rețea și aplicație și să permită: • limitare pentru numărul de cereri HTTP /secundă de la o singură sursă IP; • limitare a numărului de conexiuni TCP concurente per adresă IP sursă ce folosesc același cookie HTTP; • protecție pentru HTTP request flood făcut de o sursă IP pentru același URL; • protecție împotriva cererilor HTTP generate de posibile scripturi (prin validarea browserului client); • blocare a atacurilor de tip TCP SYN flood; • limitare a numărului de conexiuni TCP concurente per adresă IP sursă.
C59.	Soluția trebuie să ofere mecanisme pentru controlul accesului clienților de aplicație HTTP după blacklist-uri și whitelist-uri configurabile de adrese IP sau folosind Geolocații.
C60.	Soluția trebuie să ofere suport pentru redirectarea cererilor HTTP și modificarea URL-ului și a headerelor, Host și Referer din cereri.
C61.	Soluția trebuie să ofere suport pentru modificarea răspunsurilor HTTP – headerul Location și întregul corp al răspunsului.
C62.	Soluția trebuie să ofere posibilitatea de a impune clienților accesul într-o anumită ordine a paginilor aplicației HTTP protejate – cererile unui client ce nu respectă această ordine trebuie să poată fi blocate.
C63.	Soluția trebuie să ofere protecție Anti Web Defacement – restaurarea conținutului original al unei aplicații web protejate în cazul modificării malițioase al acestuia.
C64.	Soluția trebuie să ofere protecție prin validarea complianței RFC HTTP a traficului procesat.
C65.	Soluția trebuie să asigure protecție la nivel de aplicație prin o funcționalitate de scanare programabilă și raportare automată a vulnerabilităților aplicațiilor web protejate.
C66.	Soluția trebuie să asigure protecție la nivel de aplicație prin control asupra parametrilor protocolului HTTP
C67.	Soluția trebuie să asigure protecție la nivel de aplicație prin posibilitatea de a include header pentru HTTP Strict Transport Security(HSTS) în răspunsul serverului de aplicație web către client.
C68.	Soluția trebuie să asigure protecție la nivel de aplicație prin posibilitatea de a scana atașamentele pentru aplicațiile ActiveSync/MAPI, OWA și FTP.

C69.	Soluția trebuie să asigure protecție folosind ML și să îndeplinească următoarele caracteristici: • Soluția trebuie să includă un modul de detectare anomalii și sa dispună de botneți care să analizeze automat traficul HTTP/HTTPS pentru a identifica comportamente neobișnuite care pot indica atacuri; • Sistemul trebuie să construiască matematic un model al traficului normal (URL, parametri, metode HTTP) și să detecteze deviații față de acesta pentru a determina dacă cererile sunt potențial malițioase sau legitime; • Sistemul trebuie să colecteze eșantioane relevante de trafic pentru construirea modelelor inițiale și standard; • Sistemul trebuie să permită configurarea parametrilor de detectare, în special nivelurile de strictness pentru anomalii, astfel încât devierea față de normal să fie definită conform cerințelor de risc ale organizației; • Să existe opțiuni de configurare a acțiunilor la detectarea unei anomalii (Ex: alertare, blocare, blocare temporară etc.); • Să existe un panou de control centralizat unde se pot vizualiza: o Starea procesului de învățare ML și progresul învățării pentru fiecare domeniu/URL; o Numărul de anomalii detectate, împărțite pe tipuri și acțiuni aplicate (alertă/deny); o Loguri detaliate privind evenimentele de anomalii și detalii de context pentru audit și investigații ulterioare.
C70.	Soluția trebuie să ofere protecție de tip Client Side (nu se acceptă soluții de protecție client side în cloud).
C71.	Soluția trebuie să ofere monitorizare și control al scripturilor și conținutului terț încărcate în paginile web la nivel de browser pentru a identifica și securiza riscurile post-livrare.
C72.	Soluția trebuie sa includă identificare automată a serviciilor externe și domeniilor terțe, clasificarea resurselor (script, iframe, form etc.) și evaluarea riscului asociat fiecărui serviciu.
C73.	Soluția trebuie sa permită configurarea flexibilă a politicilor client-side, incluzând cel puțin două moduri: • Monitor — colectează date și rapoarte fără a bloca traficul, pe baza Content-Security-Policy-Report-Only; • Block — aplică politici stricte de securitate (CSP și SRI) pentru a preveni executarea conținutului neautorizat.
C74.	Soluția trebuie sa permită ca politicile să poată fi aplicate granular pentru anumite gazde (hosts), pattern-uri URL sau intervale de IP-uri client.
C75.	Soluția trebuie să asigure o interfață de tip dashboard pentru vizualizare în timp real a telemetriei și a deciziilor de securitate.
C76.	Soluția trebuie să ofere: • Vizualizare centralizată a serviciilor descoperite, cu domenii externe, tipuri de resurse și scoruri de risc; • Trenduri și statistici de rapoarte CSP pe tipuri de browsere accesate; • Export de date (ex. CSV) pentru audit, raportare și analiză ulterioară.

C77.	Soluția trebuie să permită administrarea interfeței de management prin următoarele metode: • Interfață centralizată, accesibilă prin web, pentru configurare, monitorizare și raportare; • SSH; • Consolă.
C78.	Soluția trebuie să dispună de o interfață suplimentară de management prin API.
C79.	Soluția trebuie să dispună de o platforma de management centralizat.
C80.	Soluția trebuie să suporte protocoale de monitorizare SNMP, Syslog.
C81.	Soluția trebuie să permită notificarea prin Email.
C82.	Pentru autentificarea administratorului soluția va dispune de: • Bază de date locală; • Integrare Active Directory; • Integrare LDAP/RADIUS; • Restricționare acces de la anumite IP.
C83.	Soluția trebuie să implementeze mecanisme de control al accesului pe baza de roluri (RBAC) pentru utilizatorii administratori.
C84.	Soluția trebuie să dispună de o interfață grafică de analiză în timp real și istorică a traficului și a evenimentelor de securitate.
C85.	Soluția dispune de actualizări dinamice de pachete de semnături, furnizate dintr-o bază de date globală, actualizată permanent: • Machine Learning; • Web security; • IP reputation; • Antimalware.
C86.	Soluția dispune de licențe suplimentare care vor asigura funcționarea următoarelor: • Suport pentru minim 4 interfețe configurabile; • Suport pentru minim 8vCPU; • Suport pentru minim 32 GB RAM (creșterea capacității RAM se va face fără licențiere suplimentară).

2.4. Cerințe privind licențierea produsului

C87.	Licenţele componentelor software ale produsului ofertat trebuie să fie de tip subscripție, cu o perioadă de valabilitate de minim 36 de luni, calculată de la data recepției

2.5. Cerințe privind garanția și suportul tehnic al produsului

C88.	Garanţia produsului trebuie să fie de minim 36 de luni de la data finalizării recepției. Garanția va acoperi orice defect de funcționare apărut în condiții normale de utilizare.
C89.	Suportul software pentru produsul ofertat va fi de minim 36 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar.
C90.	Ofertantul trebuie să detalieze în propunerea tehnică modul în care va asigura acest serviciu (personal tehnic, puncte de intervenție, suport logistic, etc.).

C91.	Suportul software aferent produselor livrate trebuie să fie asigurat de ofertant, pe întreaga perioadă de suport solicitată. Aceasta are responsabilitatea de a furniza, prin resurse proprii sau prin rețeaua autorizată de suport a producătorului, acces 24/7 la suportul tehnic necesar, inclusiv posibilitatea raportării incidentelor critice, acces la patch-uri, precum și actualizări de software.
C92.	În cazul în care suportul este asigurat prin implicarea producătorului, ofertantul trebuie să prezinte documente justificative (ex. scrisoare de suport, certificat de partener autorizat sau acord de suport) care să confirme că poate activa serviciile de suport necesare. Responsabilitatea față de autoritatea contractantă pentru întreaga prestație revine ofertantului.
C93.	Nu se acceptă condiționarea acordării garanției soluției de acordarea accesului ofertantului la soluția instalată în rețele private ale beneficiarului.

2.6. Cerinţe privind condiţiile de livrare

C94.	Termenul de livrare trebuie să fie de maxim 60 de zile de la data semnării contractului subsecvent de către ambele părți.
C95.	Livrarea produsului ofertat trebuie să se realizeze electronic, la adresa electronică comunicată de beneficiar în cadrul contractului subsecvent.
C96.	O dată cu livrarea produselor, ofertantul trebuie să transmită documentația de însoțire, care va cuprinde: • avizul de însoțire a mărfii; • inventarul cantitativ-valoric, în limba română, care trebuie să coincidă cu prețul unitar al produsului ofertat cu TVA; • certificatul de garanție al produsului; • certificatul/documentul de licențiere; • documentația de exploatare, cunoaștere și întreținere, în format electronic sau prin specificarea link-ului din internet unde se regăsește.
C97.	Ofertantul este responsabil pentru livrarea în termenul agreat soluției și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu trebuie să invoce nici un motiv de întârziere sau costuri suplimentare.

2.7. Cerințe privind instalarea, punerea în funcțiune, testarea

C98.	Instalarea, punerea în funcțiune și testarea produsului se va realiza de către personalul de specialitate al beneficiarului.

2.8. Cerințe privind recepția produsului

C99.	Recepția produsului se va desfășura în acord cu prevederilor contractuale și va conține o recepție cantitativă și calitativă. Activitatea de recepție se va realiza în termen de maxim 10 zile de la data primirii produselor. Recepția cantitativă și calitativă a produsului se va executa la sediul beneficiarului din București, în prezența reprezentanților beneficiarului și ai furnizorului. În cadrul activității de recepție se vor parcurge următoarele etape: - verificarea livrării cantitative a produselor;

	- verificarea livrării documentelor prevăzute la pct. 4 din prezentul Caiet de sarcini; - verificarea funcționării produselor în acord cu prevederile cerințelor tehnice prevăzute în anexa nr. 1 la Caietul de sarcini, de către o comisie de recepție formata din angajați ai beneficiarului. Activitatea de recepție se va finaliza prin consemnarea în Procesul verbal de recepție cantitativă și calitativă a activului fix, de către o echipă formată din membrii de la furnizor și o comisie de recepție formată din angajați ai beneficiarului, a rezultatelor evaluării produsului, în modalitatea descrisă mai sus.

2.8. Alte cerințe

C100.	Specificațiile tehnice și de calitate ale soluției oferit trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog sau documentații în format electronic.
C101.	Toate cerințele enumerate sunt considerate ca având mențiunea «sau echivalent» și vor fi considerate specificații minimale din punct de vedere al performanței, indiferent de marcă sau producător.
C102.	Produsele software ofertate nu trebuie declarate de producător ca fiind EoL (End of Life), EoS (End of Sale), End of Support la data depunerii ofertei.
C103.	Ofertantul trebuie să precizeze detaliat în oferta tehnică modul de îndeplinire concretă a cerințelor tehnice software pentru toate componentele, indicând pagina și paragraful din documentația oficială detaliată a produsului emis de producătorul acestuia, unde se găsesc informațiile legate de îndeplinirea cerinței respective. Nu sunt luate în considerare ofertele care prezintă simpla confirmare a îndeplinirii cerinței, sau numai copierea acesteia, fără a fi detaliată modalitatea de îndeplinire.

Toate cerințele definite în cadrul prezentei specificații tehnice sunt obligatorii. Nerespectarea lor va conduce la respingerea ofertei.

Cristian Agapi
Digitally signed by Cristian Agapi
Date: 2026.05.28 21:40:43 +03'00'