ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
COMANDAMENTUL APĂRĂRII CIBERNETICE
Nr.3A-1197 din 20.05.2026
București

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

SPECIFICAȚIE TEHNICĂ
PENTRU ACHIZIȚIE

Revizuită în data de 20.05.2026

„Soluție integrată de protecție a rețelei"

BUCUREȘTI
2026

21 din 68

1. SCOP

Prezenţa specificaţie stabileşte cerinţele tehnice pentru achiziţionarea unei *Soluţii integrate de protecţie a reţelei* destinată filtrării traficului unei reţele conectată la Internet.

2. CERINŢE

Ofertantul va furniza o serie de instrumente în vederea realizării filtrării traficului dintr-o reţea de calculatoare conectată la Internet din infrastructurile beneficiarului.

Nr. cerinţă	CERINŢA
C1.	Soluţia ofertată trebuie să aibă în compunere: - 2 x Echipament fizic de tip next generation firewall sau echivalent cu licenţă de funcţionare în regim de înaltă disponibilitate - HA (High Availability).
C2.	Toate specificaţiile de mai jos fac referire la 1 (unu) echipament fizic.
2.1 Cerinţe generale	
C3.	Soluţia ofertată trebuie să ofere protecţie unificată la nivelul traficului de reţea, să optimizeze controlul asupra aplicaţiilor şi să integreze funcţionalităţi avansate de detecţie şi prevenire a ameninţărilor.
C4.	Soluţia ofertată trebuie să îndeplinească cumulativ următoarele specificaţii hardware: - Minim 16 interfeţe GE RJ-45; - Minim 8 sloturi GE SFP; - Minim 12 sloturi 25GE SFP28/ 10GE SFP+/ GE SFP; - Minim 4 sloturi 100 GE QSFP28/ 40 GE QSFP+; - Minim 2 interfeţe management GE RJ-45; - Minim 2 sloturi HA 10 GE SFP+/ GE SFP; - Minim 1 port consola RJ-45; - Minim 1 port USB 3.0; - Dimensiune de maxim 2RU; - TPM (Trusted Platform Module); - Minim 12 transceivere incluse SFP+ (SR 10 GE); - Minim 2 module NVMe SSD de minim 960GB fiecare.
C5.	Soluţia ofertată trebuie să îndeplinească cumulativ următoarele caracteristici: - Minim 198/197/140 Gbps trafic firewall (1518/512/64 bytes pachete UDP); - Minim 3.22 µs latenta Firewall; - Minim 210 Mpps trafic firewall măsurat în pachete per secundă; - Minim 22 Gbps trafic IPS; - Minim 17 Gbps trafic NGFW; - Minim 15 Gbps trafic Threat Protection; - Minim 12 Gbps performanta SSL Inspection (IPS, HTTPS); - Minim 20.000 de tunele IPSec VPN site-to-site; - Minim 100.000 de clienţi IPSec VPN; - Minim 12.000.000 sesiuni concurente TCP; - Minim 750.000 sesiuni noi pe secundă TCP.
C6.	Soluţia ofertată trebuie să ofere un număr minim de 10 instanţe virtuale incluse.
C7.	Soluţia ofertată trebuie să fie un echipament integrat de securitate cu funcţionalităţi simultane de: - Firewall de tip stateful; - Router cu suport pentru protocoale de rutare dinamice; - Posibilitate de instalare in mod bridge Ethernet;

	- Protecţie Antivirus; - Criptare de date: IPSec VPN; - Suport pentru QoS si Traffic Shaping; - Detecţia si prevenirea intruziunilor – IDS/IPS; - Scanare si filtrare WEB; - Blocarea si controlul traficului din reţea generat de aplicaţii: - Protecţie Antispam: - Protecţie împotriva scurgerii de informaţii confidenţiale: - Update-uri automate şi în timp real; - Suport pentru IPv6 UTM; - Funcţionalitate de proxy SSL – posibilitatea inspecţiei traficului criptat.
C8.	Toate funcţionalităţile de securitate menţionate anterior, tehnologiile incluse, sistemul de operare precum şi platforma hardware trebuie să aparţină aceluiaşi producător.
C9.	Soluţia ofertată trebuie să fie în conformitate cu Certificarea de Conformitate Europeană (CE) şi Certificarea de Securitate Cibernetică (CB)
C10.	Soluţia ofertată trebuie să fie compusă din: - echipament hardware dedicat care are instalat un sistem de operare dedicat, dezvoltat de către producător. Nu este permisă folosirea unui sistem de operare comercial (cu scopul de a realiza o integrare nativă cu platforma hardware pentru a evita orice problemă de compatibilitate sau performanţă); - licenţele/subscripţiile necesare pentru asigurarea funcţionării simultane a tuturor componentelor solicitate.
2.2 Cerinţe tehnice şi funcţionale	
C11.	Soluţia ofertată trebuie să asigure funcţionalităţi NAT, PAT, Transparent Bridge.
C12.	Soluţia ofertată trebuie să asigure opţiunea de a aplica NAT per politică.
C13.	Soluţia ofertată trebuie să suporte VLAN Tagging 802.1Q.
C14.	Soluţia ofertată trebuie să permită autentificarea utilizatorilor pe grupuri.
C15.	Soluţia ofertată trebuie să asigure funcţionalităţi proxy explicit HTTP/HTTPS şi FTP.
C16.	Soluţia ofertată trebuie să asigure suport pentru proxy chaining cu balansare de sesiuni prin proxy-uri multiple pentru funcţionalitatea proxy explicit.
C17.	Soluţia ofertată trebuie să asigure suport pentru TCP MSS clamping.
C18.	Soluţia ofertată trebuie să aibă capabilitatea de a rescrie câmpul Class of Service.
C19.	Soluţia ofertată trebuie să ofere suport IPv6 (NAT/mod Transparent).
C20.	Soluţia ofertată trebuie să permită crearea de politici de securitate bazate pe identitatea utilizatorului/servicii folosite/tipul device-ului sau al sistemului de operare folosit.
C21.	Soluţia ofertată trebuie să deţină opţiune "Scheduling" pentru politicile de firewall.
C22.	Soluţia ofertată trebuie să aibă posibilitatea de a bloca traficul după ţara de origine a sursei sau destinaţiei (Geo IP).
C23.	Soluţia ofertată trebuie să includă un mecanism de calcul şi afişare al reputaţiei utilizatorilor din reţea pe baza de scor dedus în mod configurabil din activitatea detectată prin mecanismele de inspecţie de blocarea a atacurilor, blocare malware, filtrare web, firewall şi inspecţie a traficului de aplicaţii.
C24.	Soluţia ofertată trebuie să ofere suport pentru protocoalele VPN PPTP, L2TP, IPSec, L2TP over IPSec.
C25.	Soluţia ofertată trebuie să ofere suport pentru protocoalele de monitorizare SNMP v1/v2/v3, Syslog
C26.	Soluţia ofertată trebuie să asigure criptarea traficului VPN utilizând algoritmi de criptare DES, 3DES, AES 128, AES 192, AES 256.

C27.	Soluția ofertată trebuie să permită autentificarea utilizând algoritmi hash precum: MD5, SHA-1, SHA-256, SHA-384, SHA-512.
C28.	Soluția ofertată trebuie să ofere suport pentru PPTP și L2TP VPN Client Pass Through.
C29.	Soluția ofertată trebuie să ofere funcționalități de tip "Hub and Spoke" pentru conexiuni VPN de tip IPSec.
C30.	Soluția ofertată trebuie să suporte autentificare IKE prin certificate X.509 - suport pentru RSA și ECDSA.
C31.	Soluția ofertată trebuie să suporte IPSec Xauth NAT Traversal.
C32.	Soluția ofertată trebuie să ofere suport pentru configurare IPSec automată.
C33.	Soluția ofertată trebuie să integreze functionalitate IKE Dead Peer Detection.
C34.	Soluția ofertată trebuie să aibă suport pentru RSA SecureID.
C35.	Soluția ofertată trebuie să ofere funcționalități de monitorizare a tunelelor VPN.
C36.	Producătorul trebuie să aibă în portofoliu un client de VPN IPSec propriu, care are și funcționalități de: antivirus, filtrare web, filtrare a traficului de aplicații.
C37.	Soluția ofertată trebuie să ofere protecție anti-malware (virus, troian, worm, spyware, grayware).
C38.	Soluția ofertată trebuie să suporte minim protocoalele: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP.
C39.	Soluția ofertată trebuie să dispună de update-uri automate ale listei cu semnături malware.
C40.	Soluția ofertată trebuie să ofere protecție împotriva rețelelor botnet și site-urilor de tip phishing pe bază de reputație a adreselor IP si a URL-urilor accesate de utilizatori.
C41.	Soluția ofertată trebuie să permită filtrare pentru protocoalele HTTP si HTTPS.
C42.	Soluția ofertată trebuie să permită filtrare după categorii site-uri/URL- uri.
C43.	Soluția ofertată trebuie să aibă funcționalitatea de a contoriza timpul de acces sau a volumul de trafic pentru utilizatori, cu posibilitatea de a defini cote de utilizare.
C44.	Soluția ofertată trebuie să permită blocarea conexiunilor în funcție de URL/cuvânt cheie sau expresie în conținutul paginilor web.
C45.	Soluția ofertată trebuie să poată bloca conexiunile în funcție de URL-ul din header-ul Referer al cererii HTTP.
C46.	Soluția ofertată trebuie să permită filtrare pentru Java Applet, Cookies, scripturi Active X.
C47.	Soluția ofertată trebuie să ofere posibilitatea de activare forțată a opțiunii „Safe Search" pentru motoare de căutare web.
C48.	Soluția ofertată trebuie să ofere posibilitatea de a modifica header-ele HTTP din cererile generate de utilizatori.
C49.	Soluția ofertată trebuie să dispună de o funcționalitate de monitorizare a activității web a utilizatorilor.
C50.	Soluția ofertată trebuie să ofere posibilitatea de a înștiința utilizatorii, prin afișarea informațiilor în cadrul unui browser web, privind paginile web blocate.
C51.	Soluția ofertată trebuie să permită identificarea și controlul a minim 5000 de aplicații.
C52.	Soluția ofertată trebuie și ofere opțiunea de Traffic-Shaping per aplicație.
C53.	Soluția ofertată trebuie să dispună de control specific pentru aplicațiile de tip IM/P2P.
C54.	Soluția ofertată trebuie să permită clasificarea granulară a aplicațiilor după criterii multiple precum: categorii de aplicații, popularitate, tehnologie și risc.
C55.	Soluția ofertată trebuie să asigure funcționalități pentru monitorizarea aplicațiilor care au rata cea mai mari de consum de bandă.
C56.	Soluția ofertată trebuie să asigure funcționalități pentru monitorizarea aplicațiilor pe baza IP/Utilizator.

C57.	Soluția ofertată trebuie să confere suport pentru decriptarea și inspectarea sesiunilor SSH.
C58.	Soluția ofertată trebuie să ofere suport pentru blocarea aplicațiilor utilizate în cadrul rețelelor de tip Botnet.
C59.	Soluția ofertată trebuie să ofere posibilitatea de a defini semnăturile de aplicație personalizate.
C60.	Soluția ofertată trebuie să ofere posibilitatea de înștiințare a utilizatorilor, prin afișarea informațiilor în cadrul unui browser web, privind traficul de aplicații blocat.
C61.	Componenta IPS a soluției ofertate trebuie să asigure, pe bază de subscripție validă, pe durata perioadei de garanție: - Protecție împotriva a minim 18.000 de semnături de atac; - Suport pentru inspecția traficului de aplicație criptat prin protocolul SSL; - Protecție pentru atacuri de tip brute force; - Detectarea anomaliilor de protocol; - Suport pentru semnături configurabile; - Update-uri automate pentru semnături; - Suport pentru IPv4 si IPv6 DoS/DDoS.
C62.	Componenta antispam a soluției ofertate trebuie să asigure, pe bază de subscripție validă, pe durata perioadei de garanție: - Scanare pentru protocoalele SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI; - Suport RBL/ORDBL; - Inspecție header MIME; - Filtrare după cuvinte cheie/expresie; - Filtrare după Black/White List pentru adrese IP si e-mail; - Update-uri automate si in timp real.
C63.	Soluția ofertată trebuie, în cazul scurgerilor de informații, să permită blocarea conversației pe protocoale de email, HTTP, FTP si variantele criptate SSL.
C64.	Soluția ofertată trebuie să permită blocarea fișierelor după tip și dimensiune.
C65.	Soluția ofertată trebuie să aibă fucționalități de DLP fingerprint și arhivare.
C66.	Soluția ofertată trebuie să permită integrarea cu o aplicație software pentru securitate ce rulează pe stații care sa permită: - Blocarea traficului de aplicații instalate pe stații; - Restricționarea/filtrarea accesului web; - Scanarea pentru vulnerabilități a stațiilor; - Scanare Antivirus; - Configurarea automata pentru tunele VPN.
C67.	Soluția ofertată trebuie să includă funcționalități SD-WAN pentru control inteligent al interfeței WAN, cu posibilitatea de direcționare dinamică a traficului pe baza politicilor configurabile.
C68.	Soluția ofertată trebuie să permită identificarea și controlul aplicațiilor și să ofere posibilitatea aplicării de politici diferențiate pe utilizatori și/sau grupuri de utilizatori.
C69.	Soluția ofertată trebuie să ofere suport pentru legături WAN multiple cu balansare a traficului după metodele Weighted round robin a sesiunilor, împărțire proporțională a volumului de trafic, prin limitarea per interfață a benzii maxime utilizabile, după calitatea conexiunii ISP (jitter sau latență).
C70.	Soluția ofertată trebuie să ofere suport PPPoE și DHCP Client/Server.
C71.	Soluția ofertată trebuie să aibă capabilități pentru rutare statică.
C72.	Soluția ofertată trebuie să aibă capabilități de rutare dinamică IPv4 cu suport minim pentru protocoalele: RIP, OSPF, BGP, Multicast (PIM–DM, PIM–SM, IGMP v1 v2 v3), IS-IS).

C73.	Soluția ofertată trebuie să aibă capabilități de rutare dinamică IPv6 cu suport minim pentru protocoalele: RIPng, OSPF v3, BGP 4+.
C74.	Soluția ofertată trebuie să permită gruparea interfețelor în zone de securitate.
C75.	Soluția ofertată trebuie să permită rutare între zonele de securitate.
C76.	Soluția ofertată trebuie să suporte rutare bazată pe politici (policy-based routing).
C77.	Soluția ofertată trebuie să ofere suport pentru VRRP și Link Failure Control.
C78.	Soluția ofertată trebuie să ofere suport pentru VLAN Tagging (802.1q).
C79.	Soluția ofertată trebuie să suporte rutare între VLAN-uri.
C80.	Soluția ofertată trebuie să ofere suport pentru IPv6 (Firewall, DNS, SIP).
C81.	Soluția ofertată trebuie să aibă posibilitatea de mapare(Binding) adrese IP – adrese MAC.
C82.	Soluția ofertată trebuie să suporte One-to-One NAT.
C83.	Soluția ofertată trebuie să fie capabil de tunelare IP în IP.
C84.	Soluția ofertată trebuie să suporte NAT64, DNS64, NAT46, NAT66.
C85.	Soluția ofertată trebuie să suporte LLDP.
C86.	Soluția ofertată trebuie să ofere funcționalități de limitare/garantare/prioritizare a benzii de trafic prin politici, traffic shaping per aplicație și adresă IP, suport pentru DSCP și ToS și limitarea cotei de trafic (per adresă IP).
C87.	Soluția ofertată trebuie să fie capabilă să funcționeze în mod Activ-Activ sau Activ-Pasiv pentru asigurarea unui nivel ridicat al disponibilității.
C88.	Soluția ofertată trebuie să dispună de funcționalitate Stateful Failover (Firewall și VPN).
C89.	Soluția ofertată trebuie să permită configurarea HA (High Avalability) în modurile: - Activ-Activ - Activ-Pasiv - Clustering
C90.	Soluția ofertată trebuie să includă funcționalități de detecție si notificare a stării de nefuncționare a unuia dintre echipamentele configurate în HA (High Availabiliy).
C91.	Soluția ofertată trebuie să fie capabilă de monitorizarea conexiunii la rețea.
C92.	Soluția ofertată trebuie să dispună de funcționalitate Link Failover.
C93.	Soluția ofertată trebuie să permită administrarea prin WEB UI, Secure Command Shell (SSH) și Command Line Interface (CLI).
C94.	Soluția ofertată trebuie să permită posibilitatea de administrare dintr-un portal cloud-based oferit de producător.
C95.	Soluția ofertată trebuie să permită crearea de utilizatori/administratori cu drepturi configurabile.
C96.	Soluția ofertată trebuie să permită exportul/importul configurației.
C97.	Soluția ofertată trebuie să dispună de o politica de control a parolelor.
C98.	Soluția ofertată trebuie să permită păstrare a log-urilor pe memoria internă.
C99.	Soluția ofertată trebuie să permită definirea locală a utilizatorilor.
C100.	Soluția ofertată trebuie să permită integrare cu Windows Active Directory (AD) pentru Single Sign On.
C101.	Soluția ofertată trebuie să permită integrare cu Citrix pentru autentificare SSO a utilizatorilor.
C102.	Soluția ofertată trebuie să permită integrare cu RADIUS/LDAP/TACACS+/POP3.
C103.	Soluția ofertată trebuie să suporte Xauth pentru IPSec VPN.

C104.	Soluția ofertată trebuie să ofere suport pentru autentificarea grupurilor de utilizatori prin LDAP.
C105.	Soluția ofertată trebuie să ofere suport pentru autentificare prin doi factori folosind OTP generate de token-uri fizice sau software ce pot fi trimise utilizatorilor prin Email sau SMS.
C106.	Soluția ofertată trebuie să ofere suport pentru autentificare prin certificate digitale PKI X.509.
C107.	Soluția ofertată trebuie să consume maxim 600 W, iar alimentarea să fie de la curent alternativ 200-250V, 47-52 Hz (conform standardelor din România).
C108.	Soluția ofertată trebuie să fie echipat cu surse de alimentare redundantă hot swappable.
2.3 Cerințe privind licențierea	
C109.	Licențele software trebuie să fie valabile pentru o perioadă de minim 36 de luni. În această perioadă, ofertantul trebuie să asigure accesul beneficiarului la toate actualizările software ale elementelor componente ale soluției.
C110.	Ofertantul trebuie să prezinte modul de licențiere a software-ului aferent soluției.
2.4 Cerințe privind garanția	
C111.	Garanția produsului trebuie să fie de minim 36 de luni de la data finalizării recepției produsului.
C112.	Nu se acceptă condiționarea acordării garanției produsului de acordarea accesului ofertantului la produsul instalat în rețele private ale beneficiarului.
C113.	În cazul defectării în perioada de garanție a unei componente/echipament ce conține un mediu de stocare a informațiilor, nevolatil la decuplarea alimentării (hard-disk, card, memorie etc.), ofertantul va primi echipamentul pentru diagnosticare și reparație fără mediul de stocare a informațiilor.
C114.	Soluția ofertată trebuie să beneficieze de minimum 36 de luni de suport care trebuie să includă: - Înlocuirea echipamentului în caz de defecțiune hardware, cu livrare în următoarea zi lucrătoare (NBD – Next Business Day); - Suport tehnic din partea producătorului 7 zile pe săptămână, 24 de ore pe zi; - Update firmware versiuni minore și majore.
C115.	Soluția ofertată trebuie să beneficieze de update-uri automate de semnături de securitate pentru îndeplinirea tuturor funcționalităților licențiate pe toată durata garanției acesteia.
C116.	Soluția ofertată trebuie să beneficieze de garanție hardware de minim 36 de luni, acordată de ofertant. Garanția trebuie să acopere orice defect de fabricație sau de funcționare apărut în condiții normale de utilizare.
C117.	În cazul în care, pe durata garanției, discurile SSD/Flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea trebuie să fie înlocuite de ofertant cu altele noi, funcționale. Costurile aferente acestor activități trebuie să fie incluse în ofertă.
C118.	Discurile de stocare defecte (SSD/Flash) rămân în posesia beneficiarului și nu vor fi returnate ofertantului sau producătorului, din considerente de securitate a informației.
C119.	În cazul în care suportul este asigurat prin implicarea producătorului, ofertantul va prezenta 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.
2.5 Cerințe privind livrarea, ambalarea, etichetarea, transportul și asigurarea pe durata transportului	

C120.	Termenul de livrare trebuie să fie de maxim 60 de zile de la data semnării contractului subsecvent de către ambele părți.
C121.	Livrarea produsului ofertat trebuie să se realizeze la sediul beneficiarului din str. Drumul Taberei 7-9, Sector 6, București.
C122.	Odată 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 pentru componenta/componentele software ale produsului; - documentația de exploatare, cunoaștere și întreținere, în format electronic sau prin specificarea link-ului din internet unde se regăsește.
C123.	Ofertantul 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 trebuie să invoce nici un motiv de întârziere sau costuri suplimentare.
2.6 Instalare, punere în funcțiune, testare	
C124.	Instalarea, punerea în funcțiune și testarea produsului se va realiza de către personalul de specialitate al beneficiarului.
2.7 Cerințe privind instruirea	
C125.	Ofertantul trebuie să ofere instruire pentru minim 8 reprezentanți ai beneficiarului, pe o durată de minim 5 (cinci) zile, câte 8 ore pe zi, pentru buna înțelegere a funcționării soluției ofertate.
C126.	Instruirea se va executa în termen de maxim 60 de zile de la semnarea contractului subsecvent de ambele părți și trebuie să permită personalului beneficiarului să opereze si să administreze soluția livrată.
C127.	Instruirea trebuie să se facă în București, într-o locație pusă la dispoziție de ofertant, cu acordul beneficiarului, care să ofere toate facilitățile necesare instruirii profesionale a personalului pentru administrarea și utilizarea soluției ofertate.
C128.	Ofertantul trebuie să asigure instructorul, sala de instruire, materialele didactice, infrastructura IT&C, (sisteme informatice, rețeaua și domeniul virtual al cursului, instrumente software), precum și suportul instruirii și multiplicarea acestuia.
C129.	Instructorul desemnat trebuie să dețină certificări tehnice valide aferente soluției ofertate, emise de producător sau de un centru autorizat de instruire al producătorului. Ofertantul va prezenta documente justificative privind certificările și acreditările instructorului propus.
C130.	Instruirea trebuie să se facă în limba română.
C131.	Instruirea trebuie să exemplifice modul practic prin care se verifică toate funcționalitățile solicitate prin caietul de sarcini.
C132.	Instruirea trebuie să fie de tip "hands-on" (implicarea participanților în mod direct în activitățile practice, crearea și testarea de exemple bazate pe noțiunile teoretice prezentate și accesul la resursele materiale corespunzătoare în timpul desfășurării cursului), cu activități practice în care cursanții utilizează, administrează și testează produsul ofertat, aplicând noțiunile specific privind integrarea software, configurarea, administrarea și exploatarea soluției ofertate.
C133.	Cheltuielile de instruire a personalului care care va utiliza produsul trebuie să fie incluse în prețul ofertei.

2.8 Cerințe privind recepția produsului	
C134.	Recepția produselor constă în recepția cantitativă și calitativă a produsului.
C135.	Recepția cantitativă și calitativă se va realiza la sediul beneficiarului din str. Drumul Taberei 7-9, Sector 6, București, în prezența reprezentanților beneficiarului și furnizorului.
C136.	Recepția se va realiza în termen de maxim 10 (zece) zile lucrătoare de la data livrării produsului și a activității de instruire a personalului descrisă la punctul 2.7 din prezenta specificație tehnică.
C137.	În cadrul activității de recepție se vor parcurge următoarele etape: - verificarea livrării cantitative a produsului; - verificarea livrării documentelor prevăzute la pct. 4 din caietul de sarcini; - verificarea funcționării produsului în acord cu prevederile cerințelor tehnice prevăzute în anexa nr. 1 la caietul de sarcini, de către o echipă formată din membrii de la furnizor și o comisie de recepție formată din angajați ai beneficiarului; - verificarea executării activității de instruire descrisă la punctul 2.7 din prezenta specificație tehnică.
C138.	La finalul activității de recepție se va întocmi un **proces verbal de recepție a activului fix** prin care se va finaliza activitatea de recepție.
C139.	Dacă în cadrul recepției se constată că unele produse nu corespund din punct de vedere cantitativ sau calitativ, beneficiarul are dreptul de a respinge produsele, iar furnizorul are obligația de a remedia neconformitățile constatate în decurs de 5 (cinci) zile lucrătoare de la constatarea lor.
C140.	Activitățile de recepție se consideră a fi finalizate la momentul semnării de către beneficiar a **procesului verbal de recepție a activului fix (dacă din acest document nu rezultă obiecțiuni).**
2.9 Alte cerințe	
C141.	Produsele livrate vor fi noi și nefolosite. Nu se acceptă echipamente remanufacturate și/sau care au în componență elemente care au fost folosite anterior.
C142.	Specificațiile tehnice și de calitate ale soluției ofertate trebuie, obligatoriu, susținute de documentații originale: prospecte, foi de catalog sau documentații în format electronic.
C143.	Soluției ofertată va fi livrată împreună cu toate accesoriile necesare punerii în funcțiune și funcționării în regim High Availability(HA), chiar dacă acestea nu au fost solicitate în mod expres.
C144.	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.
C145.	Produsele și accesoriile ofertate trebuie să fie noi și să nu fie declarate EoL (End of Life), EoS (End of Sale) sau End of Support de către producător.
C146.	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.

= PAGINA ALBĂ =