**Caiet de sarcini**

**Soluție unificată de detecție și mitigare a vulnerabilităților**

 **CUPRINS**

[**1** **Introducere** 4](#_Toc189206871)

[**2** **Contextul realizării acestei achiziții de produse** 4](#_Toc189206872)

[**2.1** **Informații despre Achizitor** 4](#_Toc189206873)

[**2.2** **Informații despre contextul care a determinat achiziționarea soluției** 5](#_Toc189206874)

[**2.3** **Informații despre beneficiile anticipate de către achizitor** 6](#_Toc189206875)

[**2.4** **Alte inițiative/proiecte/programe asociate cu această achiziție de produse** 7](#_Toc189206876)

[**2.5** **Cadrul general al sectorului în care achizitorul își desfășoară activitatea** 7](#_Toc189206877)

[**2.6** **Factori interesați și rolul acestora** 7](#_Toc189206878)

[**3** **Descrierea soluției solicitate** 7](#_Toc189206879)

[**3.1** **Obiectivul general la care contribuie furnizarea soluției** 7](#_Toc189206880)

[**3.2** **Obiectivul specific la care contribuie furnizarea soluției** 7](#_Toc189206881)

[**3.3** **Produsele solicitate și operațiunile cu titlu accesoriu (servicii asociate) necesar a fi realizate** 8](#_Toc189206882)

[**3.3.1** **Produse solicitate** 8](#_Toc189206883)

[**Detalierea ”Soluției unificată de detecție și mitigare a vulnerabilităților” pentru Ministerul Finanțelor:** 9](#_Toc189206884)

[**3.3.2** **Disponibilitatea și scalabilitatea soluției** 34](#_Toc189206885)

[**3.4** **Extensibilitate** 35](#_Toc189206886)

[**Nu este cazul.** 35](#_Toc189206887)

[3.5 Furnizarea de produse de generaţie superioară 35](#_Toc189206888)

[3.6 Garanție 35](#_Toc189206889)

[3.7 Livrare, ambalare, etichetare, transport și asigurare pe durata transportului 37](#_Toc189206890)

[3.8 Operațiuni cu titlu accesoriu (servicii asociate) 38](#_Toc189206891)

[**3.8.1** **Instalare, punere în funcțiune, testare** 38](#_Toc189206892)

[**3.8.2** **Instruirea personalului pentru utilizare** 39](#_Toc189206893)

[3.9 Servicii de mentenanţă 39](#_Toc189206894)

[**3.9.1** **Mentenanța preventivă în perioada de garanție** 39](#_Toc189206895)

[**3.9.2** **Mentenanța corectivă în perioada post-garanție** 40](#_Toc189206896)

[3.9.3 Mentenanța evolutivă în perioada post-garanție 40](#_Toc189206897)

[3.10 Suport tehnic 40](#_Toc189206898)

[3.11 Piese de schimb și materiale consumabile pentru activitățile din programul de mentenanță corectivă după expirarea garanției 42](#_Toc189206899)

[3.12 Mediul în care este operat produsul 42](#_Toc189206900)

[**3.12.1** **Constrângeri privind locația unde se va efectua livrarea/instalarea** 42](#_Toc189206901)

[**4** **Atribuțiile și responsabilitățile Părților** 42](#_Toc189206902)

[**5** **Documentații ce trebuie furnizate achizitorului în legătură cu produsul** 45](#_Toc189206903)

[**6** **Recepția soluției** 46](#_Toc189206904)

[**6.1** **Recepția cantitativă** 46](#_Toc189206905)

[**6.2** **Recepția calitativă** 47](#_Toc189206906)

[**7** **Modalități și condiții de plată** 47](#_Toc189206907)

[**8** **Cadrul legal care guvernează relația dintre Achizitor și Furnizor** 48](#_Toc189206908)

[**9** **Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului** 48](#_Toc189206909)

[**9.1** **Activitățile în cadrul Contractului** 48](#_Toc189206910)

[**9.2** **Evaluarea performanței furnizorului** 49](#_Toc189206911)

[**10** **Cerințe privind personalul de specialitate** 50](#_Toc189206912)

[**11 Modul de întocmire a Propunerii tehnice** 52](#_Toc189206913)

[**I.** **Îndeplinirea cerințelor Caietului de sarcini referitoare la:** 52](#_Toc189206914)

[**II.** **Factori de evaluare pentru componenta tehnică:** 53](#_Toc189206915)

[**III.** **Respectarea obligațiile relevante în domeniile mediului, social și al relațiilor de muncă:** 54](#_Toc189206916)

[**IV.** **Confidențialitatea propunerii tehnice:** 54](#_Toc189206917)

[12 Alocarea riscurilor în cadrul contractului, măsuri de gestionare a acestora 55](#_Toc189206918)

1. **Introducere**

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

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

În cadrul acestei proceduri, Ministerul Finanțelor (MF) îndeplinește rolul de Autoritate contractantă, respectiv achizitor 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 minime 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 va fi considerată admisibilă numai în condițiile în care aceasta asigură un nivel calitativ superior cerințelor minime solicitate prin prezenta documentație.

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

1. **Contextul realizării acestei achiziții de produse**
	1. **Informații despre Achizitor**

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

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

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

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

Informații suplimentare despre achizitor, Ministerul Finanțelor, se pot regăsi pe site-ul web oficial al instituției: [www.mfinante.gov.ro](http://www.mfinante.gov.ro).

* 1. **Informații despre contextul care a determinat achiziționarea soluției**

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

Din aceste motive, este necesar să fie asigurate continuitatea funcționării, securitatea, integritatea și disponibilitatea datelor/informațiilor, ce fac obiectul tranzacțiilor economice.

Modernizarea serviciilor de comunicație din rețeaua internă (Intranet) apare ca o necesitate de bază, indispensabilă pentru buna funcționare a serviciilor informatice suport pentru aplicațiile informatice accesibile din portal în contextul mai larg al infrastructurii MF/ANAF.

În acest sens este necesar ca infrastructura de securitate IT să fie în permanență actualizată în funcție de necesitățile de trafic, pentru a preîntâmpina atacuri cibernetice care ar putea afecta funcționarea în parametri optimi a Sistemului Informatic al Ministerului Finanțelor.

Informațiile de mai jos sunt prezentate cu următoarele scopuri:

1. Înțelegerea infrastructurii fizice în care va fi integrată soluția livrată;
2. Înțelegerea tehnologiilor cu care soluția ofertată trebuie să se interconecteze.

În prezent securizarea accesului din internet către Sistemul informatic MF/ANAF este realizată cu echipamente în tehnologie F5 Networks.

În cadrul Sistemului Informatic al MF/ANAF diferențiem următoarele categorii de acces la resursele informatice:

1. Acces public pentru toți utilizatorii din România și străinătate reprezentat de platforma internet;
2. Acces intern pentru utilizatorii interni ai MF și ANAF reprezentat de platforma intranet;
3. Acces privat pentru utilizatorii din instituțiile publice externe ANAF și MF reprezentat de platforma extranet.

după cum urmează:

1. Portal internet

<https://www.anaf.ro>

1. Portal internet

<http://www.mfinante.gov.ro>

1. Portal intranet

<https://www.fiscnet.ro>

1. Portal extranet

<https://extranet.fiscnet.ro>

1. Sistemul ARB

<https://extranet.fiscnet.ro/anaf/extranet/ARB>

1. Sistemul PATRIMVEN

<https://epatrim.fiscnet.ro>

1. Sistemul IFN

<https://financiar.anaf.ro>

1. Sistemul FOREXEBUG

<https://extranet.anaf.mfinante.gov.ro/anaf/extranet/Aplicatii>

1. Sistemul DEDOC, de depunere declarații

<https://www.e-guvernare.ro>

1. Declarație unică

<https://declunica.anaf.ro>

În cazul serviciilor **Spațiul Privat Virtual** - **SPV** din cadrul portalului internet, a serviciilor din cadrul platformelor **FOREXEBUG**, **ARB**, **PATRIMVEN**, **DEDOC**, platforma F5 Networks realizează suplimentar și autentificarea și preluarea sesiunilor active ale utilizatorilor.

De asemenea, contextele aferente serviciilor web oferite de MF/ANAF, disponibile prin intermediul adreselor: **webservice.anaf.ro, webserviced.anaf.ro, webservicedext, api.anaf.ro, webserviceapl.anaf.ro**, sunt configurate și deservite din punct de vedere al balansării traficului și sarcinii de procesare, politicilor de securitate, mecanismelor de autorizare și control al accesului, de către platforma F5 Networks, respectiv prin intermediul platformei se realizează și autentificarea utilizatorilor și preluarea sesiunii acestora.

* 1. **Informații despre beneficiile anticipate de către achizitor**

Achiziția soluției solicitate în prezentul Caiet de sarcini are în vedere menținerea în funcțiune a Sistemului Informatic MF/ANAF la nivelul utilizatorilor interni și externi prin asigurarea conectivității acestora la resursele centralizate din Centrele de date și contribuie astfel la:

* Asigurarea continuității și disponibilității utilizării Sistemului Informatic al MF;
* Protecția datelor gestionate în cadrul Sistemului Informatic al MF;
* Alinierea MF cu strategiile asumate și cu eforturile întreprinse la nivel național, în domeniul protecției infrastructurilor critice.
	1. **Alte inițiative/proiecte/programe asociate cu această achiziție de produse**

Nu este cazul

* 1. **Cadrul general al sectorului în care achizitorul își desfășoară activitatea**

Administrație publică centrală

* 1. **Factori interesați și rolul acestora**

Factorii interesați în implementarea Contractului sunt:

* Ministerul Finanțelor prin Centrul Național pentru Informații Financiare care:
* administrează și dezvoltă Sistemul Informatic al MF/ANAF;
* va implementa Contractul și va intra în relație directă cu Furnizorul pe perioada derulării acestuia;
* Angajații din Ministerul Finanțelor și Agenția Națională de Administrare Fiscală aparat central și instituții subordonate din teritoriu, care utilizează Sistemul Informatic al MF/ANAF.
1. **Descrierea soluției solicitate**
	1. **Obiectivul general la care contribuie furnizarea soluției**

Asigurarea funcționării sistemului informatic al MF în condiții de securitate, performanță și disponibilitate prin asigurarea siguranței în exploatare a zonei de aplicații web oferite de Sistemul Informatic MF/ANAF atât către utilizatorii interni cât și către utilizatorii externi.

* 1. **Obiectivul specific la care contribuie furnizarea soluției**

Scopul principal al achiziției „Soluție unificată de detecție și mitigare a vulnerabilităților” este de a asigura echipelor de utilizatori finali o majorare în termeni de calitate și performanță a nivelului de disponibilitate a aplicațiilor web expuse către zonele Internet/Intranet/Extranet.

Totodată se urmărește asigurarea funcționării sistemului informatic al MF în condiții de securitate, performanță și disponibilitate. În urma efectuării acestei achiziții se preconizează atingerea următoarelor obiective:

1. achiziționarea „Soluție unificată de detectie și mitigare a vulnerabilităților” în configurația precizată în prezentul Caiet de sarcini;
2. maximizarea valorii investiției în tehnologia aflată în producție, în directă corelație și cu celelalte tehnologii utilizate în funcționarea sistemului informatic al Autorității contractante, precum și a nivelului de pregătire a specialiștilor din cadrul Autorității contractante;
3. asigurarea de suport tehnic și servicii profesionale pentru 36 luni pentru soluția achiziționată.
	1. **Produsele solicitate și operațiunile cu titlu accesoriu (servicii asociate) necesar a fi realizate**
		1. **Produse solicitate**

*Soluție unificată de detecție și mitigare a vulnerabilitățiilor*

| Cantitate | Unitate de măsură | Loc de livrare\* | Data de livrare solicitată\*\* | Specificații tehnice SAU cerințe funcționale minime | Specificații tehnice SAU cerințe funcționale extinse | Durata minimă garanție/termen de valabilitate |
| --- | --- | --- | --- | --- | --- | --- |
| 1. | 2. | 3. | 4. | 5. | 6. | 7. |
| 1 | Soluție | La sediul Autorității contractante din București, conform precizărilor Autorității contractante | 90 zile de la intrarea în vigoare a contractului | conform precizărilor de mai jos\*\*\* | - | 36 luni |

*\** ***Locațiile exacte*** *la care vor fi livrate componentele soluției achiziționate vor fi precizate Contractantului declarat câștigător, în cadrul Contractului.*

 *\*\** ***Data de livrare*** *a soluției include și acceptarea de către Achizitor (recepția cantitativă și calitativă)*

 *Furnizorul va fi responsabil de livrarea soluției în termen de 90 de zile de la semnarea contractului, termen în cadrul căruia se vor efectua livrarea tuturor componentelor acesteia și toate serviciile cu titlu accesoriu de instalare, punere în funcțiune, testare (cap.3.8.1) și instruirea (cap.3.8.2), precum și recepția cantitativă și calitativă (cap.6). Achizitorul își rezervă un termen de 3 zile lucrătoare de la livrare pentru realizarea recepției cantitative a componentelor soluției și un termen de 5 zile lucrătoare de la finalizarea serviciilor cu titlu accesoriu și a instruirii, pentru realizarea recepției calitative.*

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

***”Soluția unificată de detecție și mitigare a vulnerabilităților” pentru Ministerul Finanțelor, trebuie să asigure integrarea hardware și software minim a următoarelor componente:***

| **Poz.** | **Denumire reper** | **UM** | **Cantitate** |
| --- | --- | --- | --- |
| A | Soluție unificată de detecție și mitigare a vulnerabilităților | buc. | 1 |
| B | Infrastructura IT dedicată | buc. | 1 |

| **Nr. crt.** | **Cerința solicitată** |
| --- | --- |
| ***A. Specificații tehnice și cerințele funcționale minime pentru*** ***Soluție unificată de detecție și mitigare a vulnerabilităților*** |
| **A.1** | **Funcționalități de tip managementul vulnerabilitatilor:** * Funcționalitate de inventariere a activelor IT;
* Funcționalitate de detecție și remediere a vulnerabilităților;
* Funcționalitate de detecție și mitigare a amenințărilor de securitate;
* Funcționalitate de detecție a vulnerabilităților la nivelul aplicațiilor web.
 |
| ***B. Specificații tehnice și cerințele funcționale minime pentru*** ***Infrastructura IT dedicată*** |
| **B.1** | **Suport de procesare virtualizată de tip HCI:**1. cluster de echipamente de tip Server, în arhitectură HCI scalabilă, pentru procesare și stocare virtualizată;
2. arhitectură de tip cluster HCI (Hyper-Converged Infrastructure), pentru suportul componentelor software de management, cu minim 4 noduri tip server, fiecare nod fiind echipat cel puțin cu 2 procesoare fizice multi-core, 1TB RAM și minim 6x 6.4TB SSD pentru fiecare nod.
 |

**Detalierea ”Soluției unificată de detecție și mitigare a vulnerabilităților” pentru Ministerul Finanțelor:**

1. **Soluție unificată de detecție și mitigare a vulnerabilităților**

**A.1 Funcționalități de tip managementul vulnerabilităților**

Soluția ofertată trebuie să includă o soluție unificată de detecție și mitigare a vulnerabilităților, ce trebuie să fie complet localizată în Centrul Primar de Date, fără a avea componente localizate în locații de tip „cloud public”. Platforma trebuie să respecte următoarele cerințe tehnice minimale:

|  |  |
| --- | --- |
| **Funcționalitate** | **Descriere** |
| **Funcționalități Generale** | 1. Trebuie să ofere o interfață HTML ce reunește în elemente dinamice, personalizabile de tip „dashboard” toate informațiile oferite de soluție, respectiv vizualizări complete și actualizate în mod continuu a tuturor activelor IT și a informațiilor de securitate și conformitate asociate acestora, precum și corelări între acestea;
2. Trebuie să permită construirea flexibilă de “dashboard”-uri, prin folosirea unor elemente de tip “widget”, elemente ce pot conține orice set de informații relative la activele IT și vulnerabilitățile asociate acestora. De asemenea trebuie să includă un “dashboard” disponibil inițial, pre-populat cu “widget”-uri rezultate în urma unor criterii de identificare uzuale a activelor IT;
3. Trebuie să permită crearea și salvarea de “dashboard”-uri în funcție de rolul utilizatorului și/sau a departamentului din care face parte, respectiv “widget”-urile trebuie să permită operațiuni de tip “drill-down” în scopul vizualizării de informații relevante asupra activelor IT investigate;
4. “Dashboard”-ul central trebuie să ofere, în mod complet personalizabil, acces la următoarele informații și acțiuni:
* Monitorizarea continuă a posturii de securitate, a problemelor de securitate identificate, respectiv a evoluției securității într-un interval de timp definibil;
* Crearea și personalizarea de vederi și rapoarte distincte;
* Posibilitatea de a identifica rapid zonele ce prezintă probleme de securitate;
* Căutarea și filtrarea incidentelor de securitate pentru a obține o vedere istorică a evenimentelor ce au condus către o anumită alertă de securitate;
* Afișarea granulară, detaliată a tuturor detaliilor legate de activele IT și de vulnerabilitățile identificate la nivelul acestora, astfel încât să se poată determina cu ușurință suita evenimentelor de securitate, când și unde au apărut acestea, ce schimbări au fost făcute în infrastructură, ce alte alerte corespondente de la nivelul acelorași active IT au fost generate etc;
1. Trebuie să permită centralizarea și organizarea flexibilă a activelor IT în funcție de structura organizațională, respectiv în funcție de drepturile utilizatorilor cu rol de administrator, definiți atât local cât și prin integrarea nativă cu sisteme de administrare a identităților de tip LDAP;
2. Trebuie să ofere interfețe apelabile în mod programatic (de tip REST API) pentru integrarea cu sisteme terțe de securitate (sisteme de agregare și corelare a jurnalelor de sistem, sisteme IDS/IPS, etc), sisteme de ticketing, sisteme de tip CI/CD etc;
3. Toate datele generate și accesate de platformă trebuie să fie stocate local, în nivelul de stocare asigurat de componenta software de stocare din nodurile platformei de procesare;
4. Trebuie să asigure un serviciu intern de criptare a tuturor datelor generate și stocate de platformă, respectiv trebuie să ofere un mecanism de gestionare a ciclului de viață al cheilor, mecanism validat FIPS 140-2.
 |
| **Funcționalități de inventariere a activelor IT** | 1. Trebuie să permită detecția, inventarierea și clasificarea atât în mod activ cât și în mod pasiv, respectiv prin intermediul unor agenți, dar și fără agenți dedicați, a tuturor activelor IT: servere fizice și virtuale, mașini virtuale, containere, echipamente de comunicație, echipamente de securitate, stații de lucru, dispozitive mobile, imprimante, sisteme IoT, baze de date, servere de aplicație etc. Detecția, inventarierea și clasificarea trebuie să se facă continuu, în mod automat și nu doar ca proces inițiat de administratorii soluției ofertate, respectiv trebuie să surprindă și modificările ulterioare făcute asupra activelor IT, de la momentul identificării inițiale;
2. La nivelul activelor IT hardware și software, cel puțin următoarele detalii trebuiesc colectate, inventariate și clasificate: detaliile hardware, serviciile ce rulează, porturile de comunicație deschise, software-ul instalat, conturile de utilizator asociate etc;
3. Procesul de detecție, inventariere și clasificare trebuie să se facă fără a aduce un impact de funcționare și de performanță asupra activelor IT, respectiv asupra mediului de comunicație;
4. Toate datele colectate trebuiesc stocate local, respectiv indexate pentru a facilita procesele de căutare și regăsire a activelor IT și a detaliilor asociate acestora;
5. Trebuie să ofere funcționalitate automată de normalizare și clasificare a detaliilor activelor IT, atât în baza unor reguli definibile de administratorul soluției, cât și în baza unui catalog permanent actualizat, oferit de producătorul soluției ofertate;
6. Procesul de normalizare și clasificare trebuie să permită standardizarea informațiilor activelor IT luând în considerare cel puțin: numele producătorului, numele produsului, specificațiile hardware detaliate, software-ul instalat (incluzând sistemul de operare, actualizările software, driver-ele, aplicațiile, utilitarele, plugin-urile), conexiunile de rețea, informațiile legate de utilizatori și contextul de securitate al acestora, servicii și procese ce rulează, sisteme de fișiere, zona geografică și de timp etc;
7. Trebuie să permită identificarea și catalogarea tuturor activelor IT de tip dispzitiv mobil, cu suport nativ pentru sisteme de operare Android și iOS/iPadOS, respectiv a informațiilor asociate acestora: tip de dispozitiv, informații de sistem, sistem de operare, configurare, aplicații instalate, certificate instalate, informații de localizare, servicii de comunicație active, stare dispozitiv (dispozitiv blocat, sistem de operare neactualizat/modificat) etc;
8. Trebuie să permită identificarea și catalogarea tuturor certificatelor digitale SSL/TLS folosite în infrastructură (atât pentru servicii expuse în exterior cât și pentru serviciile interne), respectiv a informațiilor asociate acestora: certificate expirate sau pe punctul de a expira, certificate ce nu respectă anumiți parametrii de securitate – lungimea cheilor, algoritmii de semnare, certificate emise de autorități de certificare ne-aprobate sau compromise etc;
9. Trebuie să permită identificarea și catalogarea tuturor activelor IT găzduite în instanțe de tip container, respectiv a artefactelor asociate (imagini de sistem, medii de construcție, medii de rulare, medii de tip registru etc);
10. Trebuie să permită identificarea și catalogarea tuturor meta-datelor asociate mediilor de rulare bazate pe container-e, incluzând, dar fără a se limita la: etichete aplicate la nivel de imagine sistem, software instalat în imaginea sistem, nivele de funcționare și informațiile de asociere între aceste nivele de funcționare, variabilele de sistem utilizate în mediul de rulare al container-elor, servicii ce rulează în container-e, utilizatori, accesul la sistemul de fișiere, informații legate de mediul de rețea, porturi de comunicație deschise, informații legate de asocierea cu alte container-e ce au la bază aceeași imagine de sistem comună, serverul pe care rulează etc;
11. Soluția trebuie să ofere funcționalitatea solicitată pentru medii de rulare de tip container, bazate pe Docker și gestionate prin Kubernetes, Docker Swarm sau medii de orchestrare echivalente;
12. În urma proceselor de detecție, inventariere, normalizare și clasificare, soluția ofertată trebuie să permită construirea unei hărți dinamice/multi-dimensionale a tuturor activelor IT, precum și a posturii de securitate a acestora, respectiv trebuie să evidențieze problemele de configurare, riscurile de securitate, violările politicilor de securitate și conformitate;
13. Trebuie să permită construcția unei hărți a mediului de rulare bazat pe container-e, folosind informații legate de imaginile de sistem, mediile de tip registru, mediile de rulare, mediile de construcție, container-ele în sine, serverele asociate etc;
14. Trebuie să ofere un motor inteligent de căutare, ce trebuie să permită construcția de interogări simple și complexe (ce combină multiple criterii de căutare) asupra tuturor activelor IT, respectiv să permită obținerea unor răspunsuri relevante în funcție de criteriile de căutare folosite (Ex.: toate serverele din infrastructură ce folosesc un sistem de operare ce nu mai este suportat de producător, toate bazele de date ce rulează în infrastructură și localizarea lor, toate sistemele ce au instalată o aplicație anume, toate sistemele ce folosesc certificate digitale expirate etc);
15. Motorul de căutare trebuie să permită sortarea, filtrarea și salvarea criteriilor de căutare, respectiv descărcarea rezultatelor căutărilor sub formă de fișiere pdf, csv, doc/docx și html. De asemenea trebuie să permită crearea de elemente de tip “widget” folosind criteriile de căutare salvate, respectiv construcția de “dashboard”-uri personalizate ce folosesc aceste “widget”-uri pentru a afișa active IT ce sunt des inspectate sau referențiate;
16. Trebuie să ofere posibilitatea de a adăuga etichete (manual și/sau automat în baza unor reguli bazate pe parametrii detectați) pe orice element de inventar al activelor IT și gruparea flexibilă a acestora în funcție de una sau mai multe etichete, respectiv adăugarea activelor IT în structuri ierarhice în baza etichetelor definite;
17. Trebuie să ofere un motor flexibil de raportare, permitțând construcția de rapoarte ce agregă informații despre orice tip de activ IT și/sau grupare de active IT, respectiv permite salvarea și partajarea rapoartelor. Nivelul de informație disponibil în rapoarte trebuie să poată fi configurat în funcție de audiență: sumar și detalii destinate elementelor de decizie, informații detaliate destinate administratorilor de sistem, informații legate doar de un anumit set de active IT destinate administratorilor respectivului tip de active IT etc.
 |
| **Funcționalități de detecție și remediere a vulnerabilităților** | 1. Trebuie să ofere un motor de detecție în timp real, atât în mod activ cât și în mod pasiv, respectiv prin intermediul unor agenți, dar și fără agenți dedicați, a tuturor vulnerabilităților asociate activelor IT (servere fizice și virtuale, mașini virtuale, containere, echipamente de comunicație, echipamente de securitate, stații de lucru, dispozitive mobile, imprimante, sisteme IoT, baze de date, servere de aplicație, certificate digitale SSL/TLS etc), folosind o bază globală, permanent actualizată, de informații legate de vulnerabilitaătți, respectiv folosind un mecanism de corelare a vulnerabilităților cu versiunile software ale activelor IT, pentru a crea și actualiza permanent harta vulnerabilităților din întreaga infrastructura IT. Motorul de detecție a vulnerabilităților trebuie să ofere o acuratețe de minim 99,99966% (“Six-Sigma”);
2. Trebuie să identifice, raporteze și monitorizeze greșelile de configurație pe baza criteriilor și bunelor practici definite de CIS (Center for Internet Security), permițând cel puțin următoarele:
* Importul politicilor CIS relevante și maparea acestora la activele IT identificate în infrastructură;
* Generarea de rapoarte ce evidențiază postura de securitate a activelor IT relativ la politicile CIS mapate, detalierea măsurilor de remediere ce trebuiesc luate pentru fiecare activ IT în parte și pentru fiecare element vulnerabil descoperit, respectiv referințele către politicile și standardele de conformitate ce sunt încălcate prin ne-aplicarea măsurilor de remediere;
1. Identificarea, raportarea și monitorizarea trebuie să se facă continuu, în mod automat și nu doar ca proces inițiat de administratorii soluției ofertate, respectiv trebuie să surpindă și modificările ulterioare făcute asupra activelor IT, de la momentul identificării inițiale;
2. La nivelul mediilor de rulare de tip container, motorul de detecție a vulnerabilităților trebuie să ofere suport pentru o paletă largă de sisteme de operare (distribuții Linux generale, distribuții specifice container-elor – CoreOS, Alpine, etc), aplicații (NGINX, PostGres, mySQL, Redis, MongoDB, etc), limbaje de programare (Python, NodeJS, RubyGems, GoLang, Java, etc), respectiv trebuie să detecteze vulnerabilitățile la toate nivelurile ce compun o imagine de container;
3. Tot la nivelul mediilor de rulare de tip container, motorul de detecție a vulnerabilităților trebuie să identifice granular deviațiile de la imaginile de sistem standard de la baza container-elor (modificări ale pachetelor software și ale configurațiilor, modificări ale accesului la sistemele de fișiere, modificări ale comunicației de rețea, modificări ale activității serviciilor și proceselor ce rulează în container-e, etc), evidențiind elementele de execuție neaprobate, respectiv evenimentele malițioase ce pot aparea în mediul de rulare al container-elor. După identificarea vulnerabilităților trebuie să permită acțiuni de monitorizare, blocare sau permitere a comportamentelor ce au fost clasificate ca devieri de la configurația de bază a imaginii de sistem, atât în mod manual cât și pe baza unor politici predefinite. Politicile trebuie să se poată genera automat pe baza activității observate la nivelul container-elor, trebuie să se poată selecta dintr-un catalog de politici uzuale și/sau trebuie să poată fi construite manual, respectiv trebuie să poată fi actualizate dinamic fără a fi necesară repornirea container-elor asupra cărora sunt aplicate;
4. Motorul de detecție a vulnerabilităților trebuie să ofere suport nativ pentru mediile DevOps de tip CI/CD (Jenkins, Bamboo, CircleCI etc) în scopul integrării directe cu pipeline-urile de dezvoltare, astfel încât vulnerabilitățile să poată fi identificate înainte de publicarea în infrastructură a unei noi versiuni de aplicație și/sau a unor aplicații nou dezvoltate. Prin această integrare trebuie să ofere dezvoltatorilor rapoarte detaliate privind măsurile ce trebuiesc luate pentru a remedia vulnerabilitățile identificate, respectiv trebuie să ofere administratorilor posibilitatea de a bloca publicarea unor aplicații vulnerabile sau a unei noi versiuni vulnerabile de aplicație, în baza severității vulnerabilității descoperite și/sau în baza identificatorului unic din catalogul global de vulnerabilități (QID, CVE ID, BugTraq ID etc);
5. La nivelul dispozitivelor mobile, motorul de detecție a vulnerabilităților trebuie să permită acțiuni de detecție și blocare de la distanță a activităților malițioase (Ex.: blocarea de la distanță a dispozitivului mobil, blocarea conectării la rețele wireless nesecurizate, resetarea dispozitivului mobil, dezinstalarea și actualizarea aplicațiilor, alertarea utilizatorilor, schimbarea parolelor/PIN-ului dispzitivului mobil etc);
6. Trebuie să permită integrarea nativă, bazată pe reguli definibile, cu unelte de tip ITSM (IT Service Management) în vederea deschiderii și alocării automate de tichete pentru a îmbunătății procesul de remediere a vulnerabilităților, respectiv pentru a scade timpul de remediere;
7. Trebuie să ofere un motor vizual, de tip “no-code” de creare a fluxurilor operaționale de remediere a vulnerabilităților, oferind pași predefiniți de remediere a unor riscuri globale de securitate ale întregii infrastructuri IT (riscuri ce pot îngloba multiple active IT/grupări de active IT, respectiv multiple vulnerabilități) fără a fi nevoie de remediere punctuală la nivelul fiecărui activ IT și/sau vulnerabilitate descoperită.
 |
| **Funcționalități de detecție și mitigare a amenințărilor de securitate** | 1. Trebuie să ofere un motor de identificare, monitorizare și alertare în timp real asupra amenințărilor de securitate survenite la nivelul activelor IT, motor integrat nativ cu funcționalitățile de detecție și remediere a vulnerabilităților;
2. Motorul de identificare, monitorizare și alertare trebuie să permită definirea de profile de monitorizare ce trebuie să specifice activele IT ce se doresc monitorizate (pe baza de IP-uri individuale sau pe baza unei game de adrese IP), definirea unor seturi de reguli granulare de monitorizare (evenimente de securitate), respectiv definirea notificărilor în cazul declanșării unei alerte (notificări afișate în “dashboard” și/sau notificări trimise pe e-mail către persoane individuale sau grupuri de distribuție, notificări sumarizate pentru un anumit interval de timp etc);
3. Motorul de identificare, monitorizare și alertare trebuie să adauge identificatori specifici de amenințare la vulnerabilitățile identificate, permițând astfel prioritizarea proceselor de remediere. Identificatorii specifici de amenințare trebuie să fie de minim următoarele tipuri:
* Zero Day (vulnerabilități pentru care nu există un remediu de la producător și pentru care au fost depistate atacuri);
* Public Expoit (vulnerabilități pentru care există mecanisme binecunoscute de exploatare, mecanisme ce sunt disponibile publicului larg);
* Actively Attacked (vulnerabilități ce sunt exploatate activ);
* High Lateral Movement (vulnerabilități ce, odată compromise, permit atacatorului exploatarea mai multor active IT, nu doar a celui ce a manifestat inițial vulnerabilitatea);
* Easy Exploit (vulnerabilități ce pot fi exploatate foarte ușor, fără cunoștințe avansate);
* High Data Loss (vulnerabilități a căror exploatare poate duce la pierderea masivă de date);
* Denial of Service (vulnerabilități ce pot suprasatura și întrerupe funcționarea temporară sau permanentă a activelor IT vizate);
* No Patch (vulnerabilități ce nu au disponibilă o remediere din partea producătorului);
* Malware (vulnerabilități asociate cu infecții malware);
* Exploit Kit (vulnerabilități pentru care există kit-uri de exploatare);
1. Motorul de identificare, monitorizare și alertare trebuie să folosească mecanisme de depistare în timp real a amenințărilor de securitate, mecanisme bazate atât pe o sursă de tip “Threat Intelligence” cât și pe inteligența artificială (“machine-learning”), asigurând astfel corelarea continuă a datelor externe legate de amenințările de securitate curente cu vulnerabilitățile identificate în infrastructura IT;
2. Sursa externă de tip “Threat Intelligence” trebuie să fie actualizată în permanență de producătorul soluției ofertate, oferind detalii și informații granulare despre fiecare vulnerabilitate/amenințare de securitate nou descoperită, atât la nivel de vulnerabilitate specifică cât și la nivel de activ IT asupra căruia a fost identificată vulnerabilitatea. De asemenea trebuie să permită sortarea, filtrarea, salvarea și partajarea doar a unui subset specific de vulnerabilități și nu a întregului “feed” de “Threat Intelligence”;
3. Motorul de identificare, monitorizare și alertare trebuie să coreleze vulnerabilitățile identificate cu actualizările software disponibile pentru activele IT, astfel încât să permită remedierea rapidă a respectivelor vulnerabilități, respectiv trebuie să ofere următoarele funcționalități integrate nativ la nivelul soluției ofertate:
* Trebuie să identifice actualizările ce lipsesc la nivelul sistemelor de operare, respectiv la nivelul aplicațiilor uzuale (Adobe, Google, Firefox, Apple, Microsoft, Linux etc);
* Trebuie să identifice actualizările de aplicații mobile ce sunt disponibile pentru dispozitive mobile cu sistem de operare Android;
* Trebuie să ofere vizualizări dinamice, personalizabile de stare a actualizărilor la nivelul activelor IT, respectiv să permită crearea de rapoarte personalizabile în funcție de audiența țintă;
* Trebuie să ofere corelarea vulnerabilităților cu toate actualizările disponibile la nivel de activ IT, astfel încât prin simpla introducere a unui identificator CVE, sistemul să afișeze toate actualizările necesare pentru remedierea respectivei vulnerabilități;
* Trebuie să permită crearea de acțiuni de remediere (actualizarea activelor IT) programabile conform unui orar, respectiv ce pot fi declanșate manual și/sau repetate la intervale de timp regulate;
* Trebuie să permită crearea de reguli și fluxuri de remediere, astfel încât actualizările să fie aplicate numai atunci când se îndeplinesc anumite criterii (severitatea vulnerabilității descoperite, scorul CVSS, denumirea produsului etc);
* Trebuie să permită actualizarea activelor IT ce sunt în afara rețelei interne, prin agent dedicat ce trebuie să aplice actualizările chiar dacă sistemul vizat se conectează foarte rar la rețeaua IT internă;
* Trebuie să permită notificarea utilizatorilor privind necesitatea instalării actualizărilor, respectiv asupra stării proceselor curente de actualizare;
* Trebuie să permită controlul operațiunilor de repornire a activelor IT, permițând instalarea subsecventă a cât mai multor actualizări fără a fi nevoie de restart, respectiv atunci când este nevoie de repornire, operațiunea de restart să poată fi lăsată la alegerea administratorilor/utilizatorilor activelor IT;
1. Trebuie să includă un motor intuitiv, cu funcție integrată de auto-completare a termenilor de căutare la nivelul vulnerabilităților identificate, motor ce trebuie să permită minim următoarele acțiuni:
* Construirea de căutari ad-hoc folosind multiple variabile și criterii de căutare (clasa de active IT, tipul de vulnerabilitate, etichete asociate, sistem de operare, intervalul de timp etc);
* Sortarea, filtrarea și rafinarea rezultatelor căutării;
* Salvarea, descărcarea și partajarea rezultatelor căutării;
* Crearea de elemente de tip “widget” folosind rezultatele căutărilor salvate, respectiv construcția de “dashboard”-uri personalizate ce folosesc aceste “widget”-uri pentru a afișa dinamic, în timp real, informațiile des inspectate sau referențiate;
1. Motorul de identificare, monitorizare și alertare trebuie să producă notificări cel puțin pentru următoarele evenimente de securitate:
* Active IT ce apar, dispar și/sau rulează sisteme de operare ce nu sunt recunoscute ca făcând parte din infrastructura IT;
* Certificate SSL identificate ca expirate, ce expiră în curând, necunoscute sau malițioase (emise de autorități de certificare compromise);
* Porturi de comunicație nou deschise, schimbate și/sau inchise, respectiv servicii nou apărute pe porturi de comunicație folosite în mod uzual de alte servicii;
* Vulnerabilități active, închise sau re-deschise pentru întreaga infrastructură IT;
* Software neautorizat nou instalat, actualizări neautorizate ale software-ului existent, dezinstalarea neautorizată a software-ului etc;
1. Notificările trebuie să poată fi trimise în intervale de timp definibile, astfel încât notificările asociate amenințărilor critice să poată fi trimise imediat și repetate la intervale de timp configurabile, respectiv notificările asociate amenințărilor cu risc redus să poată fi trimise o dată pe zi, o dată pe săptămână etc;
2. Notificările trebuie să includă minim următoarele informații legate de amenințările identificate: numărul total de alerte pentru categoria de amenințări vizată, activele IT afectate (adresa IP, hostname etc), vulnerabilitățile detectate, elementele software adăugate/schimbate în cadrul activelor IT, porturile de comunicație deschise etc;
3. Notificările trebuie să poată fi integrate prin intermediul unui API cu sistemele dedicate de agregare și corelare a jurnalelor (SIEM);
4. La nivelul “dashboard”-ului alertele trebuie să poată fi filtrate în funcție de categorie (Ex.: activ IT, vulnerabilitate, certificat etc), respectiv în funcție de intervalul de timp în care au fost declanșate.
 |
| **Functionalități de detecție a vulnerabilităților la nivelul aplicațiilor web** | 1. Trebuie să ofere un motor de detecție, inventariere și clasificare continuă a aplicațiilor web, motor ce trebuie să permită scanarea progresivă, în pași incrementali;
2. Trebuie să permită detecția tuturor vulnerabilităților specifice aplicațiilor web, conform cu Top 10 OWASP (SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), redirectări nevalidate etc);
3. Trebuie să permită scanarea endpoint-urilor de tip SOAP și REST API, API-uri folosite cu precădere pentru comunicația dispozitivelor IoT, a aplicațiilor mobile și a serviciilor de interfațare și schimb de date la nivel de API;
4. Trebuie să permită operațiuni de scanare autentificate, respectiv folosind un limbaj de scripting deschis/larg utilizat pentru automatizarea interacțiunii cu aplicațiile la nivel de browser web;
5. Trebuie să permită programarea operațiunilor de scanare, cu posibilitatea specificării timpului de începere, respectiv a duratei de scanare;
6. Trebuie să permită distribuția proceselor de scanare pe mai multe instanțe de scanare, diminuând astfel timpul necesar scanării a multiple aplicații web interconectate și/sau a aplicațiilor web foarte complexe;
7. Trebuie să permită identificarea și raportarea elementelor malware identificate la nivelul aplicațiilor web, inclusiv a celor ce evită detecția prin mecanismele obișnuite puse la dispoziție de soluțiile de tip anti-malware;
8. Trebuie să permită consolidarea și corelarea informațiilor obținute în urma proceselor de scanare cu informațiile obținute prin operațiuni manuale de testare de penetrare, obținând astfel o vedere completă asupra posturii de securitate a aplicațiilor web;
9. Trebuie să ofere suport nativ pentru mediile DevOps de tip CI/CD în scopul integrării directe cu pipeline-urile de dezvoltare, astfel încât vulnerabilitățile să poată fi identificate înainte de publicarea în infrastructură a unei noi versiuni de aplicație web și/sau a unor aplicații web nou dezvoltate. Prin această integrare trebuie să ofere dezvoltatorilor rapoarte detaliate privind măsurile ce trebuiesc luate pentru a remedia vulnerabilitățile identificate, respectiv trebuie să ofere administratorilor posibilitatea de a bloca publicarea unor aplicații web vulnerabile sau a unei noi versiuni vulnerabile de aplicație web;
10. Trebuie să permită prioritizarea operațiunilor de remediere asupra vulnerabilităților critice identificate;
11. Trebuie să permită definirea și aplicarea de etichete asupra tuturor elementelor identificate la nivelul aplicațiilor web;
12. Trebuie să includă un motor flexibil de raportare ce trebuie să permită atât o vzualizare globală a posturii de securitate a aplicațiilor web, cât și posibilitatea de a face “drill-down” asupra tuturor detaliilor disponibile în urma procesului de scanare;
13. Motorul de raportare trebuie să permită construcția de rapoarte ce agregă informații despre orice tip de aplicație web și/sau grupare de aplicații web, respectiv permite salvarea și partajarea rapoartelor. Nivelul de informație disponibil în rapoarte trebuie să poată fi configurat în funcție de audiență: sumar și detalii destinate elementelor de decizie, informații detaliate destinate administratorilor aplicațiilor web etc;
14. Trebuie să permită afișarea tuturor detaliilor legate de operațiunile de scanare, rapoarte și vulnerabilități identificate în panoul de tip “dashboard” disponibil pentru toate funcționalitățile oferite de soluție;
15. Trebuie să permită integrarea cu platforme de tip ADC pentru provizionarea automată a politicilor de securitate pentru WAF.
 |
|  **Dimensionare** | Oferta va fi licențiată pentru minim 1000 de active IT, minim 20 de medii de rulare de tip container, 100 de aplicații web, respectiv minim 1 centru integrat de management localizat în Centrul Primar de Date. |

1. **Infrastructura IT dedicată**

**B.1 Suport de procesare virtualizată de tip HCI (Hyper Convergent Infrastructure)**

Platforma de procesare hiperconvergentă, prin integrare nativă, va deservi nemijlocit soluția de management și mitigare a vulnerabilităților, alocând resursele fizice de procesare, stocare și comunicație către elementele funcționale ale soluției.

Toate nodurile de procesare vor implementa aceeaşi arhitectură internă de procesor şi aceeaşi platformă de operare.

Fiecare nod de procesare din cadrul soluției va indeplini următoarele cerințe tehnice minimale:

|  |  |
| --- | --- |
| **Funcționalitate** | **Descriere** |
| **Funcționalități de procesare** | 1. Minim 2 procesoare Intel Xeon (sau echivalent) cu cel puțin 28 nuclee/56 fire de execuție (exceptând funcționalitate de tip Hyper Threading) și frecvența minimă de 2.0 Ghz;
2. Minim 1 TB RAM DDR4-3200 cu suport pentru minim 4 TB de memorie RAM;
3. Minim 2 x 1Gbps Ethernet, 4 x 10/25Gbps Ethernet;
4. Capacitate de stocare formată din medii de tip SSD, echipare minimă de 2x450GB dedicat instalării hipervizorului dedicat funcționalităților de procesare virtualizată;
5. Capacitate de stocare formată din medii de tip NVMe, echipare minimă de 6x 6.4 TB, cu posibilitate de extensie până la 10 discuri SSD/NVMe interne;
6. Minim 3 slot-uri de extensie de tip PCI Express;
7. 2 x surse de alimentare de tip „hot-swap/hot-plug”, ce vor asigura alimentarea redundantă în condiții de încărcare maximă;
8. Sistem de ventilație de tip „hot-swap/hot-plug”, redundant;
9. Montabil în rack-uri standard de 19” cu o înălțime maximă de 1 RU;
10. Ofertantul trebuie să livreze un kit cu elementele de fixare/instalare în rack (suporți, șuruburi/captive);
11. Led integrat de localizare pentru controlul poziției în rack;
12. Panou frontal cu posibilitate de securizare echipament și ecran LCD pentru indicarea stării sistemului.
 |
| **Funcționalități de administrare** | 1. Procesor de management integrat, cu capabilități de monitorizare a componentelor critice local și de la distanță, respectiv cu posibilitatea de a genera analize predictive de eroare pentru respectivele componente;
2. Port dedicat 1 Gbps Ethernet ce va permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului;
3. Aplicație nativă de management ce va îndeplini următoarele cerințe tehnice minimale:
* Interfață securizată pentru identificarea resurselor hardware (inventar), configurare, monitorizare, alertare pentru server, respectiv toate modulele instalate în server;
* Funcții integrate de management de la distanță, redirectare interfață grafică - inclusiv sistemul de operare, tastatură și mouse, posibilitate de pornire/oprire de la distanță pentru fiecare server lamelar, suport pentru montarea de la distanță a unităților media;
* Suport pentru accesul securizat prin interfața web (SSL), respectiv prin linie de comandă (SSH);
* Suport pentru acces administrativ bazat pe roluri de utilizare, inclusiv prin integrarea Active Directory și LDAP;
* Suport pentru monitorizarea în timp real a consumului de energie electrică, a temperaturii și furnizarea unor grafice de evoluție pe diverse perioade de timp (minute, ore, zile);
* Sistem de alertare, diagnosticare și afișaj luminos cu LCD sau LED-uri pentru toate modulele instalate: procesoare, memorie, module de alimentare, module de ventilație, module de comunicație, module de management, module de stocare internă și module de expansiune.
 |
| **Funcționalități de securitate** | Trebuie să ofere suport pentru minim următoarele tehnologii de securitate:1. Blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate;
2. Utilizare de certificate digitale calificate pentru verificarea și validarea procesului de boot al sistemului de operare;
3. Suport hardware pentru verificarea și validarea la pornire a autenticității firmware-ului componentelor critice ale echipamentului (interfețe de rețea, adaptoare de tip HBA, controller RAID, discuri, surse de alimentare etc);
4. Actualizările de firmware trebuie să fie semnate criptografic de către producătorul echipamentului ofertat pentru a fi autentificate la instalare;
5. Toate componentele hardware și software care echipează soluția vor funcționa conform specificațiilor de securitate ale producătorului;
6. Firmware-ul instalat poate fi certificat de o entitate neutră, specializată în analiza, asigurarea și prevenirea riscurilor de securitate ale echipamentelor IT.
 |
| **Funcționalități de procesare virtualizată** | Soluția ofertată trebuie să includă o platformă de virtualizare dedicată, bazată pe hypervizor propriu, fără dependență de un sistem de operare anume, licențiată pentru totalitatea nucleelor de procesare, respectiv pentru întreaga funcționalitate solicitată. Această soluție trebuie să fie instalată direct în platforma de procesare și va beneficia de suportul acestei platforme atât la nivelul capacității de procesare, capacității de stocare cât și la nivelul opțiunilor de conectică și integrare cu restul elementelor fizice de infrastructură.Platforma de virtualizare trebuie să îndeplinească următoarele cerințe tehnice minimale:1. Hypervizor-ul trebuie să fie matur, testat și implementat în infrastructuri de producție complexe, respectiv trebuie să ofere performanță maximă pentru aplicațiile și serviciile instalate în mașini virtuale indiferent de complexitatea și natura acestora. Nivelul de abstractizare a componentelor fizice din platformele de procesare, stocare și comunicație nu trebuie să adauge complexitate și/sau penalizări de performanță sesizabile în funcționarea aplicațiilor și serviciilor deservite;
2. Hypervisor-ul platformei de virtualizare trebuie să fie independent de producătorul sau de metoda de stocare internă/externă disponibilă în platforma de procesare și stocare pe care rulează;
3. Amprenta pe disc a hypervizor-ului trebuie să fie cât mai mică astfel încât instalarea hypervizor-ului să poata fi facută foarte rapid, local și peste rețea, oferind totodată posibilitatea de pornire de pe stick USB dedicat și/sau direct dintr-o platformă de stocare externă (boot from SAN);
4. Trebuie să ofere scalabilitate crescută prin suport pentru configurarea în clustere de înaltă disponibilitate cu minim 64 de noduri de procesare;
5. Trebuie să ofere securitate crescută prin încărcarea proceselor importante la nivel de hypervizor în zone reziliente de memorie, respectiv prin utilizarea ultimelor functionalități de securitate disponibile în versiunile actuale ale procesoarelor (criptarea memoriei, protejarea redirectărilor în mediile virtuale de operare etc);
6. Platforma de virtualizare trebuie să ofere suport pentru următoarele sisteme de operare instalabile în mașina virtuală: Windows 10, 11, 2019, 2022; Linux Suse, Red Hat Enterprise Linux, CentOS; FreeBSD, Solaris, respectiv să permită adăugarea de spațiu de stocare pentru mașinile virtuale prin folosirea următoarelor protocoale: NAS – NFS; SAN – iSCSI/FC/FCoE, asigurând astfel compatibilitate cu majoritatea tehnologiilor implementate în mod uzual atât în platformele de procesare cât și în platformele de stocare;
7. Componentele virtuale ale platformei trebuie să poată fi modificate cu ușurință, permițând astfel crearea de configurații diferite pentru seturi comune de mașini virtuale, precum și crearea de configurații unitare la nivelul întregii infrastructuri virtuale, atât din prisma elementelor virtuale de procesare și stocare (integrate nativ în platformă sau prin integrarea nativă cu componente terțe ale respectivelor platforme de procesare și stocare), cât și din prisma elementelor de comunicație (posibilitatea integrării directe cu platforma de rețea aleasă prin intermediul unor conectori/componente proprietare sau de la producătorul platformei de rețea și asigurarea creării unei rețele virtuale unificate la nivelul întregii infrastructuri virtuale);
8. Trebuie să ofere mecanisme nativ integrate pentru adăugarea de resurse de procesare și memorie fără restartarea sistemului de operare din mașina virtuală, (în măsura în care sistemul de operare suportă aceste facilități), mecanisme ce pot fi independente de platformele de procesare/stocare/comunicație sau prin intermediul unor conectori/componente comune respectivelor platforme;
9. Prin integrarea nativă cu platformele de procesare, mașinile virtuale definite în platforma de virtualizare trebuie să beneficieze concomitent de suport de multiprocesare simetrică a minim 768 procesoare logice, minim 24 TB de RAM și acces la totalitatea porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile la nivelul nodurilor de procesare;
10. Trebuie să ofere suport pentru USB 3.0 și rularea de aplicații grafice (DirectX si/sau OpenGL) pe mașinile virtuale, respectiv suport pentru accelerare video hardware pentru mașinile virtuale cu sisteme de operare Linux și Windows;
11. Trebuie să permită configurarea și rularea unor mașini virtuale cu până la 256 procesoare virtuale și 6TB RAM;
12. Trebuie să permită prezentarea unui adaptor de rețea PCIe (PCI Express) ca mai multe adaptoare logice direct către mașinile virtuale, reducând astfel latența rețelei respectivelor mașini virtuale (I/O offload) și oferind performanțe ridicate;
13. Trebuie să ofere redundanță completă a arhitecturii, atât la nivelul elementelor virtuale distincte (procesoare, memorie, elemente de comunicație, mașini virtuale etc) cât și la nivelul unor seturi întregi de echipamente de infrastructură (platforma de procesare, platforma de stocare, platforma de comunicație etc) prin integrarea nativă cu mecanismele redundante existente în aceste platforme și prin folosirea unor tehnologii native de redundanță, balansare și fail-over aplicabile întregului spectru de funcționalitate asigurată (mașini virtuale, servicii, aplicații, platforme de procesare, platforme de stocare, platforme de comunicație);
14. Trebuie să permită identificarea și evitarea situațiilor de split-brain prin monitorizarea stării host-urilor atât la nivelul rețelei de management cât și la nivelul sistemului de stocare comun;
15. Trebuie să permită mutarea mașinilor virtuale peste rețele IP cu latențe ridicate, de până la 150ms (ex. rețele naționale sau continentale) dând astfel posibilitatea migrării mașinilor în funcționare între centre de date distante;
16. Pentru securitate sporită, trebuie să suporte în mod nativ criptarea mașinilor virtuale.
 |
| **Funcționalități de stocare virtualizată** | Toate funcționalitățile specifice pentru stocarea datelor trebuiesc implementate prin construirea unui sistem de stocare definit software, distribuit peste nodurile de procesare ale sistemului;Componenta de virtualizare a funcției de stocare trebuie să îndeplinească următoarele cerințe tehnice minimale: 1. Trebuie să fie distribuită pe fiecare nod al clusterului, rulând nativ în hypervizor, în vederea asigurării unor performanțe ridicate, respectiv a unui impact minim asupra procesorului și memoriei nodurilor de procesare;
2. Trebuie să ofere performanțe ridicate prin accelerarea citirilor și a scrierilor I/O folosind un mecanism de caching integrat, bazat pe dispozitive Flash de tip SSD/NVMe instalate în nodurile de procesare, marcate specific ca făcând parte din zona dedicată de tip cache;
3. Trebuie să fie compatibilă cu componentele de stocare integrate în nodurile de procesare ofertate și trebuie să prezinte către mașinile virtuale un singur set de resurse de stocare definite peste toate nodurile clusterului. Accesul nodurilor la resursele de stocare trebuie să se facă prin intermediul nivelului de stocare distribuit, iar accesul trebuie să fie de tip fișier, bloc, obiect, atât în mod direct cât și prin intermediul unor plug-in-uri de tip API;
4. Trebuie să permită definirea sistemului de stocare peste un cluster de minim 3 noduri pentru a implementa un sistem de fișiere distribuit;
5. Clusterul astfel construit trebuie să dețină capabilitatea de a crește liniar prin adăugarea de noduri noi până la cel puțin 64 de noduri, pentru a permite creșterea puterii de procesare a sistemului, a capacității de stocare a datelor și a performanței de citire/scriere pe sistemul de stocare;
6. Trebuie să suporte expansiunea dinamică a volumelor și LUN-urilor la capacități mai mari de 2TB, cu un minim de 60TB pentru fiecare volum exportat;
7. Trebuie să permită prezentarea unui sistem de stocare de tip block, folosind protocolul iSCSI, pentru accesul dinspre alte noduri de procesare disponibile în infrastructură;
8. Trebuie să gestioneze toate cererile de citire/scriere pentru volumele accesate de hypervizor, respectiv trebuie să intermedieze toate operațiunile I/O realizate de mașinile virtuale;
9. Trebuie să permită integrări prin intermediul unor API-uri dedicate cu sistemele de salvare și restaurare date specifice mediilor de virtualizare;
10. Trebuie să ofere posibilitatea executării operațiunilor de mentenanță și actualizare a componentelor de stocare fără afectarea funcționării mașinilor virtuale;
11. În scopul optimizării performanței trebuie să poată distribui datele mașinilor virtuale pe toate nodurile clusterului folosind un algoritm de distribuție uniformă a datelor;
12. Trebuie să permită managementul îmbunătățit al SLA-ului privind performanțele mașinilor virtuale, prin stabilirea de limite IOPS la nivel de mașină virtuală, eliminând astfel problemele de tip noisy neighbor, în care o mașină virtuală non-critică generează un număr foarte mare de IOPS, influențând negativ performanțele mașinilor virtuale critice/de producție;
13. Trebuie să utilizeze un mecanism ce va permite plasarea în mod dinamic a datelor pe diferitele niveluri de stocare din nodurile sistemului, în scopul optimizării performanței și disponibilității sistemului, respectiv rebalansarea clusterului și ajustarea distribuției datelor la adăugarea de noi noduri în cluster;
14. Trebuie să realizeze optimizarea spațiului ocupat pe disc în mod continuu atât prin deduplicare in-line precum și prin compresia datelor in-line cu bloc variabil. Aceste servicii trebuie să ruleze în mod continuu pe platformă fără a afecta în mod semnificativ performanța sistemului;
15. Trebuie să suporte nativ mecanisme de tip Thin Provisioning pentru alocarea dinamică de spațiu către mașinile virtuale, chiar dacă acel spațiu nu este fizic disponibil în nodurile de procesare, permițând funcționarea corectă a aplicațiilor și serviciilor ce necesită resurse stricte de spațiu de stocare, respectiv creșterea transparentă a volumelor de date prin adăugarea de resurse fizice de stocare (discuri) doar în momentul când acestea devin necesare;
16. Disponibilitatea și redundanța datelor trebuie asigurată prin replicarea datelor pe mai multe noduri de procesare ale clusterului. Trebuie să permită configurarea nivelului de toleranță la defecte și implicit numărul de replici ale datelor ce vor fi realizate în cadrul clusterului. Trebuie să poată tolera pierderea a până la trei noduri fără a exista riscul de pierdere a datelor;
17. Trebuie să asigure mecanisme de protecție a datelor la scriere, astfel confirmarea scrierii unui bloc de date trebuie transmisă către aplicație numai după ce datele au fost replicate pe unul sau mai multe discuri aflate pe noduri diferite ale clusterului;
18. La apariția unor probleme pe un nod al cluster-ului, toate cererile de citire/scriere ale aplicațiilor de pe nodul ce prezintă probleme trebuie să fie în mod automat transferate către alte noduri din cluster;
19. Trebuie să permită rebalansarea automată a clusterului, respectiv ajustarea automată a distribuției datelor pe nodurile sistemului la momentul adăugării și/sau scoaterii de noduri în/din cluster, fără a afecta operațiunile și funcționarea normală a clusterului;
20. Trebuie să permită toleranță la defectări prin tehnologie tip RAID cu unul și două discuri de paritate, pentru protecția volumelor de stocare, respectiv prin RAID de tip mirror pentru protecția zonei dedicate mecanismului de cache, asigurând astfel protecția datelor în cazul unor defectări la nivel de disk, nod de procesare și rețea de comunicație între nodurile de procesare;
21. Trebuie să asigure, în mod automat, integritatea datelor, prin verificarea automată a blocurilor de date stocate, pentru evitarea situațiilor de corupere prin erori de disc nedetectate;
22. Managementul zonei de stocare trebuie să fie integrat la nivelul funcționalităților de management al virtualizării, astfel încât toate operațiile de administrare să fie posibile din aceeași interfață grafică.
 |
| **Funcționalități de management al virtualizării** | Componenta de management trebuie să asigure administrarea și monitorizarea dedicată a tuturor componentelor, respectiv trebuie să fie disponibilă atât la nivelul echipamentelor fizice ce alcătuiesc platformele de procesare, stocare și comunicație cât și la nivelul mașinilor virtuale, ale resurselor virtualizate, aplicațiilor, serviciilor și protocoalelor însumate în infrastructură.Componenta de management al virtualizării trebuie să îndeplinească următoarele specificații tehnice minimale:1. În vederea accesului facil la funcțiile de administrare și monitorizare oferite, componenta trebuie să permită acces prin browser web;
2. Trebuie să fie disponibilă ca appliance virtual pentru simplificarea instalării, actualizării și administrării precum și pentru reducerea costurilor asociate (ex. licență Windows, licență bază de date etc);
3. Resursele virtuale (resurse de procesare, stocare și comunicație) disponibile la nivelul întregii componente de virtualizare (prin integrarea nativă cu echipamentele fizice de procesare, stocare și comunicație) trebuie să fie adresabile și configurabile în totalitatea lor prin intermediul unei singure interfețe de management și nu prin configurarea separată pentru fiecare echipament;
4. Trebuie să permită autentificarea utilizatorilor bazată pe roluri și privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director LDAP. De asemenea trebuie să permită crearea facilă de politici dinamice de acces la resursele de procesare, precum și de disponibilitate ale acestora;
5. Separarea privilegiilor administrative trebuie să se poată face pe orice element disponibil în interfața de administrare (server, utilizator, resursă de procesare, stocare, rețea etc), permițând astfel crearea de zone/domenii de securitate în funcție de aplicații și/sau roluri funcționale, nu în funcție de elementele disponibile în infrastructura de procesare, stocare și comunicație;
6. Trebuie să asigure mecanisme de definire și aplicare a profilelor standard de configurație pentru serverele ce fac parte din infrastructura virtuală. De asemenea trebuie să permită configurarea de politici de aplicare a acestor profile în funcție de necesitățile de moment sau în concordanță cu politica stabilită în prealabil;
7. Trebuie să permită agregarea tuturor resurselor fizice (plăci de rețea, switch-uri de comunicație integrate în nodurile de procesare) și virtuale de comunicație (switch-uri virtuale) într-un singur nivel unitar de comunicație, adresabil la nivelul întregii infrastructuri virtuale indiferent de complexitatea acesteia sau a echipamentelor de procesare și comunicație ce se integrează prin intermediul ei. De asemenea trebuie să ofere mecanisme automate de evaluare și prioritizare continuă a accesului mașinilor virtuale și aplicațiilor rezidente la resursele de comunicație disponibile, permițând alocarea și realocarea dinamică a acestor resurse în funcție de cerințele de moment sau conform unor politici prestabilite;
8. Trebuie să permită gruparea și organizarea logică a resurselor de procesare în funcție de necesități, precum și izolarea acestor grupări de resurse, respectiv trebuie să asigure flexibilitatea necesară măririi cantității de resurse disponibile într-o grupare prin extragerea de resurse din alte grupări. Accesul mașinilor virtuale și apartenența la aceste grupări de resurse trebuie să se facă atât în mod manual prin intervenția unui operator cât și pe baza unor politici dinamice de acces;
9. Trebuie să ofere functionalități integrate nativ de pornire/repornire a oricărei mașini virtuale (indiferent de aplicațiile și serviciile ce rulează pe respectivele mașini virtuale), în cadrul aceluiași server sau pe servere diferite, în cazul detectării nemijlocite a unei probleme de funcționare a mașinii virtuale au a aplicațiilor și serviciilor ce rulează pe aceste mașini virtuale. Scenarii posibile ce necesită implementarea nativă a unui astfel de mecanism de recuperare ar putea fi: blocarea sistemului de operare ce rulează în mașina virtuală, întreruperea căilor de comunicație către echipamentele de stocare, întreruperea căilor de comunicație către componenta de management etc;
10. Trebuie să ofere mecanisme integrate de balansare a încărcării resurselor fizice și virtuale disponibile în infrastructură și redistribuire a sarcinilor generate de utilizatori, servicii și aplicații, prin integrarea nativă cu echipamentele hardware, indiferent de producătorul respectivelor elemente de infrastructură. Aceste mecanisme trebuie să fie disponibile atât la comandă prin intervenția unui operator cât și prin operațiuni automate definite în funcție de necesități, gradul de ocupare al resurselor și/sau pe baza unor reguli/politici prestabilite;
11. Trebuie să permită configurarea spațiului de stocare virtual prin integrarea directă cu echipamentele de stocare alese prin intermediul unor conectori/componente native sau de la producătorul echipamentelor de stocare, mecanism ce va permite extinderea discurilor virtuale fără a fi necesară oprirea mașinilor virtuale ce au atașate aceste discuri. De asemenea prin integrare directă cu echipamentele de stocare, trebuie să ofere mecanisme automate de monitorizare a încărcării I/O și de alocare/realocare dinamică a resurselor I/O către mașinile virtuale în funcție de cerințele acestora (ad-hoc sau conform unei politici prestabilite), realizând astfel o prioritizare inteligentă a accesului aplicațiilor la resursele de stocare;
12. Prin aceleași mecanisme de integrare (inclusiv la nivelul componentelor apelabile și programabile din cadrul altor platforme, componente de tip API) cu echipamentele de stocare, trebuie să permită identificarea și folosirea optimă a mecanismelor de asigurare a căilor redundante de acces în echipamentele de stocare și a mecanismelor terțe de protecție a datelor stocate, incluzând volumele adresate direct de componenta de virtualizare, respectiv volumele de date folosite de aplicații, servicii și utilizatori;
13. Integrarea nativă cu echipamentele de stocare trebuie să permită alocarea dinamică de spațiu către mașinile virtuale, chiar dacă acel spațiu nu este fizic disponibil în aceste echipamente, permițând funcționarea corectă a aplicațiilor și serviciilor ce necesită resurse stricte de spațiu de stocare, respectiv creșterea transparentă a volumelor de date prin adăugarea de resurse fizice de stocare (discuri) doar în momentul când acestea devin necesare;
14. Trebuie să includă mecanisme de catalogare și grupare a resurselor disponibile în echipamentele de stocare, indiferent de tipul, producătorul și numărul acestora (tipuri de discuri, latența, tipul volumelor și metoda de export aplicată asupra lor), permițând astfel crearea de profile de stocare și asocierea acestor profile cu distribuirea/redistribuirea mașinilor virtuale în funcție de cereri temporare ale aplicațiilor sau în baza unor politici predefinite;
15. De asemenea trebuie să includă atât mecanisme automate de evaluare continuă a necesarului de resurse I/O cât și mecanisme de poziționare și repoziționare a mașinilor virtuale în grupările de resurse de stocare în funcție de cerințele inițiale ale aplicațiilor, respectiv în funcție de cerințele evaluate în mod continuu. Astfel se obține o balansare permanentă a distribuției mașinilor virtuale proporțional cu grupările de resurse de stocare, indiferent de cerințele de performanță și capacitate de stocare ale respectivelor mașini virtuale;
16. Trebuie să implementeze nativ mecanisme de asigurare dinamică a prioritizării accesului la aplicații și servicii, prin integrarea directă cu echipamentele de stocare și de comunicație, respectiv prin aplicarea de politici și profile asupra accesării datelor ce constituie mașinile virtuale respective și/sau sunt folosite de către respectivele aplicații, indiferent de locația respectivelor date (rezidente în echipamentele de stocare sau tranzitate prin mediile de comunicație fizice/virtuale). Se va obține astfel garantarea accesului prioritar la aplicațiile și serviciile critice din infrastructură;
17. Trebuie să asigure instalarea, configurarea și actualizarea automată a software-ului pentru virtualizarea serverelor fizice, a soluției de stocare definită software și a rețelei virtuale cu mecanisme de securitate definite software;
18. Trebuie să ofere instrumente care automatizează și simplifică procesul de implementare a stivei software de infrastructură pentru virtualizarea nodurilor de procesare, virtualizarea rețelei și crearea matricei de stocare definită software prin instalarea automată a pachetelor software, inclusiv pentru clusterele de procesare dedicate rulării de micro-servicii;
19. Trebuie să asigure mecanisme de actualizare a întregii stive software de virtualizare, respectiv trebuie să permită definirea programului și a domeniului de aplicare al acestor actualizări;
20. Trebuie să permită administrarea automată a configurației, respectiv a deviației de la anumite configurații monitorizând starea de sănătate a întregii componente;
21. Prin integrarea cu resursele de management, trebuie să permită mecanisme integrate de mutare a mașinilor virtuale de pe un server pe altul sau dintr-un datacenter în altul fără oprirea sistemului de operare ce rulează în mașina virtuală și fără întreruperea serviciului oferit de aplicația/aplicațiile din mașina virtuală. Acest lucru nu trebuie să se reflecte la nivelul utilizatorului final, astfel orice întrerupere de serviciu/mașină virtuală/sistem de operare, să nu afecteze serviciile oferite către utilizator. Aceleași mecanisme trebuie să permită atât mutarea întregului hard-disk virtual concomitent pentru oricare mașină virtuală în cadrul aceluiași datacenter sau între datacenter-e diferite, independent de echipamentul de stocare folosit și de mecanismele de replicare ale acestuia, precum și extinderea automată a harddisk-urilor virtuale pe măsură ce sistemul de operare și aplicațiile din mașinile virtuale o cer. În acest fel vor deveni posibile scenarii automate, prin politici pre-definite/definibile, de consolidare a mașinilor virtuale pe un număr prestabilit de servere și oprirea automată a serverelor fără activitate sau cu subutilizare a resurselor de procesare;
22. Tot prin integrarea cu resursele de management, trebuie să permită operațiuni automate, bazate pe politici pre-definite/definibile, de repornire (pe o altă platformă de procesare) a mașinilor virtuale individuale, precum și a seturilor de mașini virtuale ce au fost definite ca deservind o singură aplicație/serviciu sau un sub-set al unei aplicații/serviciu, în eventualitatea unei defecțiuni hardware majore la nivelul platformelor de procesare;
23. Trebuie să ofere funcționalitatea nativă de rulare în paralel a unei mașini virtuale sau a unui set de mașini virtuale ce deservesc o singură aplicație/serviciu, pe un număr de minim două echipamente distincte de procesare. Mecanismul trebuie să folosească tehnologii independente dar integrate cu echipamentele de procesare și de stocare, asigurând replicarea transparentă și sincronă a conținutului de memorie și a conținutului de disc asociat unei mașini virtuale, respectiv unui set de mașini virtuale, fără introducerea de latență semnificativă în respectivele echipamente sau în funcționarea mașinilor virtuale;
24. Trebuie să conțină funcționalitatea nativă de replicare a mașinilor virtuale către sisteme ce folosesc aceeași componentă de virtualizare, respectiv replicarea trebuie să fie posibilă atât sincron cât și asincron și trebuie să poată fi definită la nivel de mașină virtuală, cu granularitate până la nivel de disk;
25. În cazul detectării unor latențe mari, datorate unor probleme de conectivitate între cele două centre de date, replicarea trebuie să comute automat din modul sincron în modul asincron, pentru a nu impacta performanța mașinilor virtuale replicate;
26. Funcția de replicare trebuie să realizeze jurnalizarea tuturor operațiunilor de scriere, astfel încât să fie posibilă restaurarea datelor la momente de timp predefinite sau definibile de către utilizator, cu o granularitate mare;
27. Trebuie să ofere interfețe de programare pentru aplicații (API) în scopul integrării cu alte aplicații sau alte platforme de management, respectiv pentru crearea și managementul serviciilor fără restricții legate de structura/componența acestora.
 |
|  **Dimensionare** | Oferta va conține cel puțin 6 noduri de procesare în Centrul Primar de Date, toate în configurație identică, conform cu specificațiile tehnice minimale de mai sus;Oferta va conține un set de licențe ce va acoperi toate procesoarele fizice (socket echipat) ofertate (respectiv nu mai puțin de 12 de bucăți), fără limitări de capacitate de procesare, stocare, comunicație și număr de mașini virtuale funcționale;Oferta va conține un set de licențe ce va acoperi minim o instanță de management al virtualizării. |

* + 1. **Disponibilitatea și scalabilitatea soluției**

 Timp de funcționare (disponibilitate) a produsului. Produsele trebuie să fie disponibile 24 ore din 24, 7 zile din 7.

Dispozitivele hardware trebuie să fie astfel proiectate încât să poată asigura scalabilitatea sistemului în cazul creșterii ulterioare a necesarului de resurse de calcul.

* 1. **Extensibilitate**

**Nu este cazul.**

## Furnizarea de produse de generaţie superioară

Produsele software furnizate prin contract vor fi noi, de ultimă generație, nu vor fi „end of suport” în următorii 5 ani, încorporează toate îmbunătăţirile recente în proiectare, sunt din ultima generaţie / versiune (ultimul ”release” disponibil pe site-ul producătorului), inclusiv din punct de vedere al securităţii (sunt aplicate ultimele upgrade-uri/updare-uri/patch-uri).

## Garanție

Garanția soluției achiziționate va fi asigurată de către furnizor în condițiile politicii de garanție a producătorului cu acces în numele achizitorului la serviciile de garanție și suport ale acestuia, având în vedere prevederile Ordonanței de urgență a Guvernului nr. 140/2021 privind anumite aspecte referitoare la contractele de vânzare de bunuri precum și prevederile prezentului Caiet de sarcini.

Garanția tehnică oferită va fi pentru o perioadă minimă conform cap. 3.3.1, pentru întreaga soluție oferită, incluzând toate produsele și accesoriile componente, garanția începând din momentul recepției calitative.

În cazul în care perioada de garanție oferită de producătorii produselor este mai mare decât perioada minimă indicate de achizitor la cap.3.3.1, furnizorul va asigura o perioadă de garanție pentru produsele ofertate cel puțin egală cu cea oferită de producători.

Garanția tehnică a soluției asigurată de furnizor este distinctă de garanția de bună execuție a contractului și decurge de la data recepției calitative (data semnării procesului-verbal de recepție calitativă).

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

În perioada de garanție furnizorul va trebui să asigure:

1. garanția de bună funcționare, calitatea și performanțele tuturor produselor livrate în conformitate cu specificațiile producătorului acestora; acces la suportul oferit de producător pentru produsele livrate;
2. corectarea gratuită, pentru produsele livrate, a oricăror erori, defecte și neconformități constatate, cu excepția cazurilor în care defectele se datorează în mod exclusiv utilizării inadecvate/necorespunzătoare de către personalul achizitorului;
3. înștiințarea achizitorului de apariția unor îmbunătățiri sau modificări aplicabile produselor livrate, pentru o posibilă aplicare a acestora;
4. servicii de suport tehnic pentru produsele livrate conform cerințelor de la cap. 3.10.

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

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

În perioada de garanție, Furnizorul are obligația să asigure funcționarea produselor ce compun soluția, reparând sau înlocuind prin grija și pe cheltuiala lui orice componentă hardware sau accesoriu. Dacă durata de efectuare a reparației depășește un număr de 5 zile lucrătoare de la notificarea transmisă de Achizitor, produsul defect se va înlocui cu un alt produs nou, identic sau superior calitativ, compatibil din punct de vedere hardware și software.

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

După efectuarea reparației/înlocuirii și punerea în funcțiune a echipamentului/componentei defecte, între furnizor (partenerul de service acreditat al furnizorului, după caz) și achizitor se întocmește un proces-verbal de recepție.

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

Garanția trebuie să acopere toate costurile rezultate din remedierea defectelor în perioada de garanție, inclusiv, dar fără a se limita la:

1. diagnoza defectelor, inclusiv costurile de personal;
2. demontare, inclusiv închirierea de unelte speciale necesare pe durata intervenției;
3. înlocuirea/repararea tuturor produselor neconforme;
4. corectarea a oricăror erori, defecte și neconformități constatate;
5. testarea pentru a asigura funcționarea corectă a soluției;
6. repunerea în funcțiune a soluției;
7. transport prin intermediul transportatorului;
8. ambalaje, inclusiv furnizarea de material protector pentru transport (carton, cutii, lăzi etc.);
9. despachetarea, inclusiv preluarea ambalajelor și eliberarea tuturor spațiilor unde se efectuează intervenția.

Toate componentele/produsele care necesită înlocuire vor fi înlocuite de către furnizor cu componente/produse noi, identice sau superioare ca specificații tehnice, pe baza recomandărilor producătorului produselor ofertate.

## Livrare, ambalare, etichetare, transport și asigurare pe durata transportului

Livrarea soluției se va realiza conform unui ”Plan de execuție” propus de către furnizor și agreat cu achizitorul conform cap.9 din Caietul de sarcini.

Termenul de livrare este cel menționat la cap. 3.3.1. Soluția este considerată livrată când toate produsele componente ale acesteia au fost livrate, toate activitățile în cadrul contractului au fost realizate și soluția este acceptată de achizitor.

Produsele componente ale soluției vor fi livrate cantitativ și calitativ la locul indicat de achizitor pentru fiecare produs în parte. Fiecare produs va fi însoțit de toate subansamblele/părțile componente necesare punerii și menținerii în funcțiune.

Livrarea echipamentelor până la locul final al amplasării acestora cade în sarcina exclusivă a furnizorului, cu respectarea condițiilor de transport impuse de către producător pentru asigurarea garanției.

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

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

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

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

1. documentele de însoțire a mărfii (aviz de însoțire a mărfii/aviz de expediție etc.)
2. documentația tehnică***(\*)***, respectiv:
	* descrierea tehnică a echipamentelor;
	* documentația de instalare, configurare și utilizare;
	* documentația de întreținere și remediere a defecțiunilor;
3. documentele de licențiere pentru produsele software livrate;
4. documentațiile privind produsele software pe care furnizorul trebuie să le furnizeze achizitorului conform Caietului de sarcini;
5. certificat de garanție tehnică de la producător/furnizor/distribuitor;

***(\*)*** *Furnizorul va pune la dispoziția achizitorului, pentru fiecare echipament livrat, documentația tehnică prevăzută la alineatele de mai sus, în format electronic digital agreat de achizitor.*

Destinația de livrare este precizată la cap. 3.13. Furnizorul este responsabil pentru livrarea în termenul solicitat și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca niciun motiv de întârziere sau costuri suplimentare.

## Operațiuni cu titlu accesoriu (servicii asociate)

* + 1. **Instalare, testare punere** **în funcțiune**

Instalarea, testarea, punerea în funcțiune se vor realiza conform unui ”Plan de execuție” propus de către furnizor și agreat cu achizitorul conform cap.9 din Caietul de sarcini.

Furnizorul va detalia în cadrul soluției propuse strategia și modalitatea aleasă pentru îndeplinirea cerințelor achizitorului, fără perturbarea fluxului tehnologic.

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

Odată ce produsele sunt asamblate, furnizorul va realiza toate configurările/setările necesare pentru a pune produsele în funcțiune. Punerea în funcțiune include, de asemenea, toate ajustările și setările necesare pentru a asigura instalarea corespunzătoare în ceea ce privește performanța și calitatea, cu toate configurațiile necesare pentru o funcționare optimă și pentru a răspunde tuturor cerințelor funcționale și tehnice de la cap. 3.3 din Caietul de sarcini.

Furnizorul va efectua pe cheltuiala sa și fără niciun fel de costuri din partea achizitorului toate testele, pentru a asigura funcționarea produsului la parametri agreați.

Furnizorul rămâne responsabil pentru protejarea produselor luând toate măsurile adecvate pentru a preveni lovituri, zgârieturi și alte deteriorări, până la acceptare de către achizitor.

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

1. Furnizorul va asigura punerea în funcțiune a tuturor echipamentelor livrate;
2. Instalarea produselor componente ale soluției se va realiza conform specificațiilor producătorului, de comun acord cu achizitorul și conform *“Planului de execuție”* agreat;
3. Instalarea echipamentelor se va realiza în spațiile existente, în locațiile indicate de către achizitor;
4. Instalarea conectorilor, prizelor, unităților PDU, șinelor pentru montarea în rack a echipamentelor și a oricăror altor accesorii de montaj, în conformitate cu specificațiile producătorului, necesare punerii în funcțiune a echipamentelor livrate;
5. Conectarea echipamentelor la rețeaua electrică și interconectarea echipamentelor și accesoriilor necesare punerii în funcțiune a acestora;
6. Furnizorul va instala, configura, integra și testa produsele ofertate;
7. Furnizorul va instala licențele, conform drepturilor acordate achizitorului, va documenta procesul de instalare și punere în funcțiune și va genera din sistem lista prin care să fie indicată totalitatea software-ului livrat solicitată la cap.34 și care va fi verificată în cadrul recepției calitative, conform cap.56;
8. Furnizorul va întocmi un Raport de livrare și instalare a licențelor conform cap.3.4.
	* 1. **Instruirea personalului pentru utilizare**

Furnizorul este responsabil pentru instruirea personalului desemnat de achizitor. Scopul instruirii este de a transfera cunoștințele necesare personalului care va asigura operarea și administrarea soluției livrate și instalate.

Instruirea se va realiza conform „Planului de execuție” care va fi propus de furnizor și va fi agreat cu achizitorul conform cap.9 al Caietului de sarcini.

În cadrul Propunerii tehnice se va detalia modul în care furnizorul va asigura instruirea. Furnizorul va detalia nivelul de instruire avut în vedere, nivel care trebuie să fie direct corelat cu scopul achiziţiei, cu tipul de soluţie propusă din punct de vedere al noutăţii tehnologice, astfel încât să permită personalului care va fi instruit să se familiarizeze cu tehnologia respectivă la un nivel adecvat şi să administreze/ opereze eficient şi la un nivel adecvat produsele furnizate.

Instruirea:

1. va conține prezentarea generală a soluției,
2. va conține prezentarea schimbărilor ce au intervenit în infrastructura și arhitectura sistemului, ca urmare a implementării soluției propuse,
3. va fi axat pe soluția propusă,
4. va cuprinde atât partea teoretică cât și practică,
5. va fi însoțită de **material de curs** format digital, pentru fiecare participant,
6. va avea o durată de **3 zile** a câte **8 ore/zi,**
7. vor participa minim **5 persoane,**
8. se va finaliza prin completarea unei **fișe de prezență,**
9. va fi finalizată prin **acordarea de diplome** de participare semnate de către contractant,
10. se poate desfășura atât **on-line** cât și în sală fizică,
11. la finalizarea sesiunii de instruire, Furnizorul va întocmi un **Raport de instruire** care va conține lista persoanelor instruite, certificatele obținute și suportul de curs.

Furnizorul poate să propună orice subiect suplimentar care ar putea fi necesar pentru a se asigura că personalul achizitorului este pe deplin instruit pentru a asigura utilizarea corespunzătoare a soluției achiziționate.

Nivelul de instruire, suportul de curs și programa de instruire propuse, coordonatele activităților de instruire, incluzând datele cursurilor, durata acestora și detaliile cu privire la locul de desfășurare precum și orice alte aspecte legate de activitatea de instruire vor fi stabilite de comun acord între achizitor și furnizor în cadrul „***Planului de executie****”.*

## Servicii de mentenanţă

* + 1. **Mentenanța preventivă în perioada de garanție**

Nu se solicită.

* + 1. **Mentenanța corectivă în perioada post-garanție**

Nu se solicită

### Mentenanța evolutivă în perioada post-garanție

 Nu se solicită

## Suport tehnic

Pe toată perioada de garanție, furnizorul va asigura accesul garantat al achizitorului, fără costuri suplimentare, la servicii de suport tehnic constând în:

* + 1. acces la suportul oferit de producător pentru produsele livrate;
		2. înștiințarea achizitorului de apariția unor îmbunătățiri sau modificări aplicabile echipamentelor livrate și software-ului aferent, și aplicarea acestora;
		3. accesul la resursele de update și upgrade firmware/software oferite de producător;
		4. înștiințarea achizitorului privind încetarea producției oricăruia din tipurile de echipamente livrate în baza Contractului, modificări în politica de licențiere a producătorului sau alte modificări privind produsele software livrate care pot afecta drepturile și/sau modul de utilizare a produselor de către achizitor sau privind încetarea suportului oferit de producător;
		5. actualizări de programe (incluzând noi versiuni, ediții, patch-uri), pe măsură ce ele devin disponibile comercial și dacă ofertantul le recomandă sau achizitorul le solicită;
		6. accesul la site-ul de suport al producătorului pentru descărcarea tuturor noilor versiuni, ediții și patch-uri, precum și a documentației aferente serviciilor care fac obiectul contractului;
		7. asistență tehnică și suport, ca răspuns la solicitările achizitorului, care se referă la diagnosticarea și izolarea cauzei problemelor apărute în funcționare;
		8. mentenanță corectivă și patch-uri de programe, pentru orice probleme identificate de către achizitor sau contractant;
		9. accesul la baza de cunoștințe și suport telefonic pentru toate produsele software ofertate.

Pentru achizitor este esenţial ca suportul tehnic să fie conform parametrilor de funcţionare proiectaţi/stabiliţi de producător, pentru a se evita eventualele pagube produse de intervenţii neautorizate.

Furnizorul va avea în vedere că serviciile de suport tehnic se vor desfășura cu precădere în timpul programului normal de lucru al achizitorului, existând însă cazuri de excepție, pentru care reviziile și intervențiile în caz de incident, la cererea personalului achizitorului, se pot planifica de comun acord și în afara programului normal de lucru.

Furnizorul va asigura un punct de contact dedicat personalului autorizat al achizitorului unde se poate semnala orice problemă/defecțiune care solicită suport tehnic al furnizorului, în gestionarea unui incident, pentru a se asigura că orice situație semnalată este tratată cu promptitudine. Pentru rezolvarea incidentelor, serviciile de suport tehnic vor fi prestate de către personalul tehnic al ofertantului, în limba română, remote și on-site la sediile achizitorului, telefonic și prin e-mail. Furnizorul va prezenta o listă a persoanelor abilitate să asigure serviciile de suport tehnic, listă ce va cuprinde minim informații privind nume și prenume, număr de telefon, adresă e-mail. Furnizorul va notifica achizitorul despre eventuale schimbări în structura persoanelor desemnate să asigure suportul tehnic. Furnizorul trebuie să asigure disponibilitatea serviciilor de suport tehnic 24x7 (48 ore timp de remediere), pe toată durata garanției, care să garanteze diagnosticarea incidentelor de funcționare a soluției și remedierea acestora.

Vor trebui onorate, la timp și la nivelul cerut de parametrii de calitate, toate acele solicitări venite din partea personalului specializat în tehnologia informației desemnat de achizitor, către oricare din specialiștii tehnici desemnați din partea furnizorului, cu respectarea următorilor timpi de intervenție:

|  |  |  |
| --- | --- | --- |
| **Timp de răspuns** | **Timp de implementare soluție provizorie** | **Timp de remediere** |
| 1 oră | *4 ore* | *48 ore* |

Nerespectarea timpilor de mai sus dă dreptul achizitorului de a solicita penalități/ daune/ interese în conformitate cu clauzele Contractului, astfel:

* în cazul în care furnizorul depășește timpul de implementare a unei soluții provizorii, calculat de la momentul sesizării problemei la punctul de contact dedicat personalului autorizat al achizitorului unde se poate semnala orice incident/defecțiune care necesită sau solicită suport tehnic în gestionarea unui incident, achizitorul va aplica penalități de 300,00 lei/oră de întârziere;
* în cazul în care furnizorul depășește timpul de remediere, calculat de la momentul sesizării problemei la punctul de contact dedicat personalului autorizat al achizitorului unde se poate semnala orice incident/defecțiune care necesită sau solicită suport tehnic în gestionarea unui incident, achizitorul va aplica penalități de 250,00 lei/oră de întârziere.

Furnizorul va ține cont că pentru serviciile de suport tehnic caracteristicile cheie așteptate de către achizitor vor trebui să includă continuu:

1. Diagnosticarea și rezolvarea problemelor, prin acces la informațiile tehnice și asistență așa cum sunt ele organizate/furnizate de către producător, ținând seama de timpii de răspuns așa cum sunt aceștia definiți în această secțiune;
2. Soluții în timp real prin acces permanent la expertiza tehnică, directă sau indirectă, a producătorului;
3. Soluții alternative în cazul în care nu sunt posibile cele cerute la punctul b), cu condiția ca acestea să fie organizate/furnizate pe baza expertizei tehnice, directă sau indirectă, a producătorului. Prin soluție alternativă se înțelege soluție temporară oferită de furnizor care asigură funcționalitățile sistemului informatic/aplicației informatice până la remedierea produsului software;
4. Accesul la o gamă de resurse tehnice, resurse umane – inclusiv biblioteci de soluții tehnice și abilitatea/facilitatea de a se conecta la acestea, inclusiv la cele în limba română dacă există;
5. Să asigure înregistrarea și evidența solicitărilor de suport tehnic – prin serviciul dedicat al producătorului sau serviciul indicat de acesta, opțiunea să fie disponibilă 24x7x365.

## Piese de schimb și materiale consumabile pentru activitățile din programul de mentenanță corectivă după expirarea garanției

Nu este cazul

## Mediul în care este operat produsul

Mediul în care se utilizează produsele este descris la cap.3.1: *centru de date.*

* + 1. **Constrângeri privind locația unde se va efectua livrarea/instalarea**

Locația de livrare/instalare este în București. Adresa exactă va fi precizată ofertantului devenit furnizor, în cadrul Contractului.

Pe perioada executării activităților de instalare, configurare, punere în funcțiune și testare a produselor, furnizorul are următoarele obligații:

1. să nu afecteze serviciile existente în rețeaua de comunicații a MF;
2. să respecte toate regulile privind confidențialitatea informațiilor, accesul în locații și protecția muncii;
3. să nu afecteze prin activitățile desfășurate buna funcționare a echipamentelor existente în locații, precum și mediul de comunicații pus la dispoziție.

Soluționarea eventualelor probleme de natură tehnică apărute pe parcursul derulării Contractului referitoare la soluția livrată cade în sarcina exclusivă a furnizorului.

1. **Atribuțiile și responsabilitățile Părților**
2. Furnizorul va utiliza în proiectare/configurare/dezvoltare etc. produse software sau tehnologii hardware care înglobează tehnologii software, doar a acelor produse ce beneficiază de suport pe termen lung (de tip Long-term support – LTS), ca intenție a Autorității contractante de asigurare a unei politici de management a ciclului de viața al produsului prin adoptarea de versiuni stabile care sunt menținute pe perioade mai lungi de timp decât versiunile standard. Justificarea se poate face prin prezentarea de Roadmap (foaie de parcurs privind ciclul de viață al produsului), alte documente echivalente disponibile publicului larg elaborate de către producători sau declarații semnate ale acestora.
3. Furnizorul va avea obligația ca, pentru componentele livrate, ori va obține din timp în numele Autorității contractante, ori va transfera acesteia, prin documente cu caracter juridic, licențele necesare pentru utilizarea lor conform cu scopul prezentului contract. Aceasta prevedere se aplică tuturor componentelor/resurselor licențiate și/sau sub licențiate, componentelor software comercializate de contractant, componentelor software ale unor terți, componentelor pre-existente, uneltelor software necesare livrării, monitorizării și mentenanței ș.a.m.d.
4. Furnizorul va oferi licențele pentru cumulul total al tehnologiilor HW și SW (atât cele proprii cât și ale terților, indiferent că sunt OEM, distincte, orice altă metodă) înglobate în echipamentele livrate funcționale. Aceeași cerință este valabilă inclusiv pentru utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată.
5. Furnizorul va prezenta documente care dovedesc faptul că software-ul în ansamblul său este supus sau nu unor politici de licențiere (inclusiv se vor avea în vedere utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată). Documentele justificative trebuie să fie clare, să permită identificarea tipului de licențiere, metodele de calcul (fie virtual, fizic, grad de încărcare, număr de utilizatori etc.), condițiile de utilizare, perioada de timp precum și orice altă informație valabilă la momentul contractării). Orice diferend juridic ulterior cu un terț pe subiectul drepturilor de proprietate intelectuală va cădea în sarcina și responsabilitatea furnizorului .
6. Furnizorul va avea obligația ca transferul drepturilor de proprietate și/sau folosință, și al oricăror drepturi conexe către achizitor va avea loc de la data recepției finale.
7. Furnizorul va avea obligația să despăgubească achizitorul împotriva oricăror: a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.) și b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea caietului de sarcini întocmit de către Achizitor.
8. Furnizorul trebuie să aibă în vedere că după livrare și instalare se va întocmi un Raport de livrare și instalare, pentru numărul total al licențelor care acoperă integral, distinct, licențele furnizate. Este obligatoriu ca la întocmirea acestui Raport de livrare și instalare a licențelor aferente softului să se țină seama de împerecherea datelor din lista generată de către sistemul funcțional propus pentru livrare finală (lista prin care este indicată de sistemul conceput toate software-urile utilizate și livrate), cu documentele în original (documente care să indice clar numărul licențelor, felul acestora, durata (nelimitată/ perpetuă sau limitată) etc. într-o formă care să permită înregistrarea în patrimoniul/contabilitatea Autorității contractante) prin care se atestă și se transmit drepturile de proprietate/folosință, după caz, condițiile de utilizare etc. astfel încât la finalizarea recepției calitative achizitorul să dețină toate documentele privind licențele proprii sau cele din partea terților.
9. Furnizorul va avea în vedere, ca obligație, la recepție, că achizitorul va proceda la preluarea tuturor licențelor livrate și instalate, doar prin întocmirea Proceselor verbale de recepție cantitativă și calitativă a licențelor, ca documente necesare în implementarea Contractului, care se vor întocmi pe baza constatării existenței tuturor documentelor în original privind drepturile de proprietate acordate și condițiile utilizării acestora, drepturile de folosință și condițiile acestora, identificarea clară (distinctă) a fiecărei tehnologii supuse licențierii/sub licențierii, a existenței listei de software/hardware generate de către sistemul propus pentru livrare.
10. Furnizorul va garanta faptul că toate suporturile ce conțin software vor fi livrate fără viruși informatici, viermi informatici sau cod periculos, care pot distruge sau altera software, firmware sau hardware și care, prin orice metodă, pot colecta, distruge sau altera orice dată sau informație accesată sau procesată de software. Furnizorul va anunța imediat achizitorul în scris, dacă există suspiciunea sau are cunoștință că software-ul livrat poate provoca neajunsuri de tipul celor enunțate mai sus.
11. Furnizorul va avea obligația ca, la transferul documentelor privind licențele, ca drepturi de proprietate intelectuală/folosință, să facă transferul către achizitor a unor documente în original, atât pentru propriile produse cât și pentru toate cele ale unor terți pe care le-a înglobat, adaptat, modificat, îmbunătățit, ș.a.m.d. și simultan să aibă în vedere că orice reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), în legătură cu produsele achiziționate, montate și puse în funcțiune, vor fi în sarcina și responsabilitatea sa.
12. Furnizorul are obligația de a garanta că produsele software furnizate prin Contract sunt noi, de ultimă generație, nu vor fi „end of suport” în următorii 5 ani, încorporează toate îmbunătăţirile recente în proiectare, sunt din ultima generaţie / versiune (ultimul ”release” disponibil pe site-ul producătorului), inclusiv din punct de vedere al securităţii (sunt aplicate ultimele upgrade-uri/updare-uri/patch-uri).
13. Furnizorul are obligația de a garanta că toate produsele furnizate prin Contract sunt livrate pe canalul oficial al producătorului, acoperind zona Uniunii Europene. În acest sens, furnizorul, la momentul livrării produselor, va face dovada că este distribuitor/furnizor autorizat / acreditat să comercializeze produsele ofertate, prin indicarea unei referinţe publice, cum ar fi un link către site-ul oficial al producătorului sau prezentând documente justificative.
14. Furnizorul va avea în vedere obligația de a deschide sau, după caz, de a actualiza un cont de identificare deschis pe numele/seama Autorității contractante la producător. Această cerință poate să nu fie aplicabilă în situația în care producătorul nu are o astfel de politică.
15. Toate documentele şi informaţiile primite de la ofertant precum şi rezultatele tuturor activităţilor din cadrul acestui contract (cum ar fi: documente de analiză, arhitecturi de sisteme, adrese, etc., fără a se limita la acestea) reprezintă informaţii confidenţiale, iar furnizorul câştigător va asigura respectarea confidenţialităţii lor, urmând să semneze o declaraţie în acest sens.
16. Furnizorul şi personalul său au obligaţia de a respecta confidenţialitatea documentelor şi informaţiilor menţionate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia şi după încetarea contractului. În acest sens, furnizorul precum şi personalul acestuia implicat în activităţile contractului sunt obligaţi să semneze Acorduri de Confidențialitate cu achizitorul.
17. Toate documentele, rapoartele şi datele, inclusiv diagrame, scheme tehnice, specificaţii tehnice, planuri şi orice alte materiale realizate de către furnizorîn cadrul contractului, sunt în proprietatea /proprietatea intelectuală a Autorităţii contractante, aceasta având dreptul să le utilizeze, modifice, transfere fără acceptulfFurnizorului sau al unei terţe părţi. Furnizorul le va furniza Autorităţii contractante, la finalizarea contractului, fără a păstra copii şi fără a le utiliza în alte scopuri care nu au legătura cu contractul.
18. Furnizorul nu va publica articole sau informaţii legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terţi şi nu va divulga informaţiile obţinute de la Achizitor, fără acordul scris al acesteia.
19. Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de proprietate intelectuală sau industrială, obţinute în cadrul contractului, sunt proprietatea Autorităţii contractante, care poate dispune de ele după cum consideră.
20. Achizitorul va asigura accesul reprezentanților furnizoruuilîn locațiile în care se vor efectua activitățile de livrare, instalare, punere în funcțiune și testare a soluției, precum și condițiile necesare efectuării acestora, astfel cum vor fi stabilite prin Contract.
21. **Documentații ce trebuie furnizate achizitorului în legătură cu produsul**

Furnizorul va prezenta următoarele documente din care să reiasă perioada de valabilitate a produselor software și sistemul pe care au fost activate, precum și următoarele documente în legătură cu produsul:

* Documentele de însoțire a mărfii;
* Documentație tehnică***(\*)***, respectiv:
	+ - descrierea tehnică;
		- documentația de instalare, configurare și utilizare;
		- documentația de întreținere și remediere a defecțiunilor;
* Certificate de garanție producător/furnizor/distribuitor;
* Documentele de licențiere pentru produsele software ofertate;
* Politica de licențiere stabilită de producător pentru produsele software ofertate;
* Orice alt document solicitat în celelalte capitole din Caietul de sarcini și nespecificat explicit în acest capitol.

**(\*)** Documentația tehnică va fi pusă la dispoziție în format electronic digital agreat de achizitor.

1. **Recepția soluției**

Recepția soluției se va realiza conform „Planului de execuție” propus de către furnizor și agreat cu achizitorul, conform cap.9 din Caietul de sarcini.

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

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

Recepția soluției se va efectua pe bază de procese verbale semnate de către reprezentanții achizitorului. Reprezentantul furnizorului va semna procesele verbale pentru luare la cunoștință și posibilitatea de a prezenta eventuale explicații și/sau observații. Recepția soluției se va realiza în mai multe etape, în funcție de progresul Contractului, respectiv:

* 1. **Recepția cantitativă**

Se va realiza după livrarea produselor ce compun soluția, în cantitatea stabilită conform contractului, la locația indicată de achizitor și va consta în efectuarea următoarelor operațiuni:

1. numărare bucată cu bucată a echipamentelor, componentelor și a accesoriilor acestora care compun soluția;
2. verificarea aspectului exterior, a integrității fizice și a caracteristicilor constructive;
3. verificarea existenței tuturor componentelor și accesoriilor;
4. verificarea existenței documentelor de însoțire a mărfii (aviz de însoțire a mărfii/aviz de expediție etc.);
5. verificarea existenței documentației tehnice aferente fiecărui tip de echipament;
6. verificarea existenței certificatelor de garanție;
7. verificarea existenței documentelor de licențiere pentru software-ul livrat;
8. verificarea existenței documentațiilor privind produsele software pe care furnizorul trebuie să le furnizeze achizitorului conform Caietului de sarcini;
9. întocmirea unui **Proces verbal de recepție cantitativă *(PVRcant.)***, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus.

Achizitorul își rezervă un termen de 3 zile lucrătoare pentru realizarea recepției cantitative.

* 1. **Recepția calitativă**

Se va realiza după instalarea și configurarea întregii soluții și a instruirii personalului pentru utilizarea acesteia, și va consta în în efectuarea următoarelor operațiuni:

1. verificarea instalării și electroalimentării echipamentelor livrate;
2. verificarea configurării hardware-software a echipamentelor livrate;
3. verificarea punerii în funcțiune a echipamentelor livrate;
4. verificarea conformității componentelor livrate cu specificațiile tehnice din Caietul de sarcini și din Propunerea tehnică, prin efectuarea de inspecții și teste funcționale. Inspecțiile și testele funcționale din cadrul recepției, vizează respectarea cerințelor Caietului de sarcini și a specificațiilor producătorului (caracteristici tehnice, constructive, electrice, cerințele funcționale etc.);
5. verificarea integrării funcționale a componentelor livrate conform specificațiilor din Caietul de sarcini/Propunerea tehnică prin efectuarea de inspecții și teste funcționale. Inspecțiile și testele funcționale din cadrul recepției vizează respectarea cerințelor funcționale și de management pentru întregul ansamblu funcțional rezultat în urma instalării și punerii în funcțiune a soluției livrate;
6. testările funcționale din cadrul recepției se vor efectua pe baza unui set de teste, care vor fi propuse de către furnizor în „*Planul de execuție”* și agreate de achizitor;
7. generarea unei liste de către sistem acolo unde este tehnic posibil prin care să fie indicată totalitatea software-ului livrat și împerecherea acestei liste cu documentele juridice în original, prin care se transmit drepturile de proprietate/folosință, după caz, verificarea versiunii codurilor software instalate, a licențelor corespunzătoare acestora, astfel încât la finalizarea recepției calitative achizitorul să se asigure că va deține toate documentele juridice privind licențele proprii sau cele din partea terților;
8. verificarea Raportului de instruire;
9. întocmirea unui Proces Verbal de Recepție Calitativă (PVRcal.) în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus.

Achizitorul își rezervă un termen de 5 zile lucrătoare pentru realizarea recepției calitative.

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

* acceptat;
* refuzat.

În cazul procesului verbal de recepție refuzat, furnizorul va analiza observațiile primite și va efectua modificările solicitate în termen maxim de 5 zile lucrătoare, după care se va relua procedura de recepție a acestora.

1. **Modalități și condiții de plată**

Furnizorul va emite factura pentru produsele livrate în sistemul Ro-eFactura, potrivit prevederilor OUG nr. 120/2021, aprobată cu modificări prin Legea nr. 139/2022. Factura va avea menționat numărul Contractului, datele de emitere și de scadență ale facturii respective. Factura va detalia cantitativ/valoric produsele furnizate și va prezenta prețul unitar al acestora.

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

1. certificatul de garanție;
2. documentele de livrare;
3. procesul verbal de recepție cantitativă.

Plata se va efectua în termen de 30 de zile, în conformitate cu prevederile art. 6 alin. (1) lit. a) din Legea nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și autorități contractante.

Plata se va efectua în lei, în contul furnizorului, în baza facturii fiscale însoțite de Procesul-verbal de recepție calitativă, semnat de reprezentanții ambelor părți.

1. **Cadrul legal care guvernează relația dintre Achizitor și Furnizor**

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

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

* Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;
* Normele metodologice de aplicare a prevederilor referitoare la atribuirea Contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, aprobate prin HG nr. 395/2016, cu modificările și completările ulterioare;
* Legea nr. 8/1996 privind dreptul de autor și drepturile conexe, cu completările și modificările ulterioare;
1. **Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului**
	1. **Activitățile în cadrul Contractului**

Se vor desfășura conform unui ***”Plan de execuție”*** propus de către furnizor și agreat împreună cu achizitorul în termen de 10 zile de la încheierea Contractului.

* 1. **Evaluarea performanței furnizorului**

Performanța furnizorului va fi evaluată, luându-se în considerare:

* Respectarea termenelor de livrare/instalare/ punere în funcțiune/testare/instruire în raport cu prevederile contractuale și **Planul de execuție** propus de Furnizor și agreat împreună cu achizitorul;
* abateri de la calitatea produselor și a serviciilor contractate.

| **Indicator de performanță** | **Referință în Caiet de Sarcini** | **Nivelul de performanță așteptat (conform Caiet de Sarcini)** | **Ce se măsoară** | **Modalitatea de evaluare** | **Scop** |
| --- | --- | --- | --- | --- | --- |
| Produse livrate și servicii associate prestate în termenele agreate | Cap. 9.1 | Produsele sunt livrate și serviciile asociate sunt prestate conform termenelor stabilite în Planul de execuție | Livrarea la timp  | **Foarte bine (5 pct.)** – Produsele sunt livrate și serviciile asociate sunt prestate conform termenelor stabilite în Planul de execuție,**Bine (3 pct.)** – Produsele sunt livrate și serviciile asociate sunt prestate după termenele stabilite în Planul de execuție însă fără depășirea termenului de livrare prevăzut în Caietul de sarcini (cap.3.4.1) și în contract.**Acceptabil (2 pct.)** – Produsele sunt livrate și serviciile asociate sunt prestate cu depășirea termenelor stabilite în Planul de execuție și cu depășirea termenului de livrare prevăzut în Caietul de sarcini (cap.3.4.1) și în contract cu mai puțin de 30 de zile.**Nesatisfăcător (1 pct.)–** Produsele sunt livrate și serviciile asociate sunt prestate cu depășirea termenelor stabilite în Planul de execuție și cu depășirea termenului de livrare prevăzut în Caietul de sarcini (cap.3.4.1) și în contract cu 30 de zile sau mai mult. | Evaluarea livrării produselor și prestării serviciilor asociate la timp |

Calificativele din coloana „modalitatea de evaluare” de mai sus vor fi menționate în procesul verbal de recepție calitativă.

1. **Cerințe privind personalul de specialitate**

Ofertantul va nominaliza specialiștii proprii (cel puțin doi specialiști) care vor asigura pe parcursul contractului serviciile de instalare, configurare, punere în funcțiune și testare, respectiv cele de înlocuire a componentelor, în perioada derulării asistenței tehnice software și hardware pentru platformele solicitate prin intermediul Caietului de sarcini.

Specialiștii propuși trebuie să dețină calificarea și experiența necesare pentru prestarea serviciilor solicitate prin Caietul de sarcini și trebuie să îndeplinească următoarele cerințe minime privind experiența specifică:

1. Studii superioare de lungă durată absolvite cu diplomă de licență, diplomă de absolvire sau echivalent;
2. Minim 3 ani experiență în configurarea platformelor solicitate prin Caietul de sarcini.

De asemenea, specialiștii propuși trebuie să îndeplinească cumulat următoarele cerințe minime privind competențele specifice:

1. Certificare de tip specialist pentru platforma F5 Networks Security și F5 CTS ASM + Certificare de tip profesional în soluții de testare de securitate informatică;
2. Certificare de tip profesional pentru soluții de comunicații datacenter;
3. Certificare de tip profesional pentru platforma de virtualizare ofertată.

Pentru aceștia se vor prezenta următoarele documente:

1. CV actualizat, semnat de către titular;
2. Documente suport (diplome, atestate, acreditări, certificări) din care să rezulte studiile și competențele/calificările profesionale pentru îndeplinirea serviciilor solicitate prin prezentul Caiet de sarcini;
3. Documente suport din care să rezulte experiența specifică în domeniu: contracte de muncă, contracte de colaborare, contracte de prestări servicii, fișe de post, adeverințe, recomandări sau alte documente similare emise de beneficiarul serviciilorsau de angajator. Din document(e) trebuie să rezulte în mod clar numele și prenumele specialistului, rolul/postul/funcția acestuia, activitățile desfășurate și perioada de desfășurare. Pentru demonstrarea îndeplinirii cerințelor privind experiența specifică în cele două domenii solicitate, se vor lua în considerare următoarele: durata în care specialiștii au fost implicați în proiecte ca experți în domeniile solicitate sau ca angajați ca experti în specializările solicitate, perioada minimă solicitată fiind de 3 ani; Pentru demonstrarea îndeplinirii cerințelor privind experiența specifică în cele două domenii solicitate, se vor lua în considerare următoarele: durata în care specialiștii au fost implicați în proiecte ca experți în domeniile solicitate sau ca angajați ca experti în specializările solicitate, perioada minimă solicitată fiind de 3 ani.

În cazul în care se prezintă declarație pe proprie răspundere emisă de ofertant/angajator, aceasta va cuprinde în mod obligatoriu, pe lângă celelalte informații necesare, următoare mențiune: „C*unosc prevederile art. 57 din Regulamentul financiar UE nr. 966/2012 și legislația națională în vigoare cu privire la conflictul de interese, precum și prevederile art.292 „Falsul în declaraţii” din Codul penal potrivit căruia „Declararea necorespunzătoare a adevărului, făcută unui organ sau instituţii de stat ori unei alte unităţi în vederea producerii unei consecinţe juridice, pentru sine sau pentru altul, atunci când, potrivit legii ori împrejurărilor, declaraţia făcută serveşte pentru producerea acelei consecinţe, se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă*.”

1. Declarație de disponibilitate pentru perioada implicării efective în derularea Contractului.

Prin aceste cerințe se urmărește protejarea integrității echipamentelor complexe și de mare valoare ale achizitorului și implicit disponibilitatea Sistemului informatic al MF. În acest sens, cunoștințele dobândite de către specialiști în instituțiile de învățământ trebuie completate cu instruiri/certificări specifice și cu experiență practică.

Ca urmare, furnizorul trebuie să dovedească faptul că dispune de personal calificat corespunzător și cu experiență în asigurarea serviciilor de instalare, configurare, punere în funcțiune și testare a infrastructurii ofertate..

Un specialist poate fi înlocuit pe parcursul derulării contractului doar cu notificarea prealabilă a achizitorului, cu minim 10 zile calendaristice înainte de data propusă pentru înlocuire.

Situațiile în care un specialist poate fi înlocuit sunt următoarele:

* 1. în cazul decesului, al îmbolnavirii sau accidentării specialistului;
	2. în cazul în care se impune înlocuirea specialistului pentru orice alt motiv care nu este sub controlul furnizorului (ex. demisia etc.);
	3. ori de câte ori se consideră necesar și justificat, pentru buna implementare a contractului.

Notificarea va fi în mod obligatoriu însoțită de justificarea necesității înlocuirii și de documentele justificative asociate noului specialist, așa cum au fost acestea solicitate prin documentația de atribuire a contractului.

Furnizorul are obligația de a se asigura că specialistul nou propus îndeplinește toate cerințele minime solicitate de achizitor prin prezentul Caiet de sarcini, inclusiv condițiile și cerințele cu privire la inexistența unui conflict de interese.

Achizitorul are dreptul de a respinge motivat noul specialist propus, în situația în care constată că acesta nu îndeplinește cerințele minime prevăzute în prezentul Caiet de sarcini sau constată existența unui conflict de interese.

**11 Modul de întocmire a Propunerii tehnice**

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

Documentul principal al propunerii tehnice este formularul de propunere tehnică pus la dispoziție de Autoritatea contractantă în Secțiunea Formulare a Documentației de atribuire), în care se va răspunde punct cu punct la fiecare dintre cerințele/specificațiile tehnice(\*) prevăzute în prezentul Caiet de sarcini și în care se face trimitere la documentația tehnică/documentele suport, anexate formularului.

***(\*)*** *Pentru specificațiile tehnice ale fiecărui produs în parte se va indica pagina din datasheet-ul oficial și link-ul valid al site-ului oficial al producătorului; se atașează extrasele la data ultimei accesări de pe site-urile indicate, relevante pentru demonstrarea conformității cu cerințele din Caietul de sarcini.*

La completarea Formularului de propunere tehnică, în situațiile în care informațiile ce trebuie introduse de ofertant pe coloana *„Mod de îndeplinire”* ocupă mult spațiu, acestea vor fi cuprinse în anexe, numerotate, respectând ordinea de prezentare înscrisă în formular. Pentru fiecare cerință din Formularul de propunere tehnică pentru care se întocmește o anexa privind modul de îndeplinire, ofertantul va indica în mod clar numărul anexei.

În sensul celor mai sus menționate, în anexele la Formularul de propunere tehnică vor fi înscrise informații privind:

* + - 1. **Îndeplinirea cerințelor Caietului de sarcini referitoare la:**
1. Documentația tehnică și documentele suport necesare pentru identificarea produselor și a serviciilor de suport tehnic ofertate, a specificațiilor tehnice și funcționale ale acestora, precum și a modului de integrare funcțională a acestora în cadrul soluției ce se achiziționează, conform cerințelor Caietului de sarcini, cu referire clară la specificațiile tehnice ale producătorului, la standardele aplicabile și la Politica de licențiere a producătorului pentru produsele software ofertate.
2. Identificarea fiecărui produs ofertat, pentru care se vor prezenta:

a) producătorul;

b) denumirea comercială, tipul/versiunea;

c)configurația hardware detaliată pe subansamble/componente/module;

d) versiunea de firmware;

e) pachetele software;

f) licențele ofertate (proprii și ale terților) și condițiile acestora; furnizorul va prezenta în formă scrisă, printr-o adresă oficială semnată, datată și ștampilată, un exemplar tipărit după politica de licențiere a producătorului, valabil la momentul semnării contactului;

g) servicii asociate;

h) specificațiile tehnice emise de Producător;

i) standardele / protocoalele respectate;

j) modul de integrare funcțională a fiecărui produs ofertat, conform cerințelor Caietului de sarcini:

1. Informații privind livrarea, instalarea, configurarea, testarea și punerea în funcțiune a produselor, modul de asigurare a activităților de instruire, garanției și suportului tehnic, incluzând: detalierea resurselor și mijloacelor pe care furnizorul le va angaja pentru îndeplinirea contractului, obligațiile asumate referitoare la modul de asigurare a garanției și suportului tehnic, responsabilități ale personalului furnizorului implicat pentru îndeplinirea contractului de furnizare;
2. Documentele doveditoare ale calificării și experienței specialiștilor desemnați de ofertant conform cap.10 din Caietul de sarcini;
3. Alte informații considerate relevante de ofertant pentru demonstrarea îndeplinirii cerințelor minime din caietul de sarcini.

***Notă:***

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

*Pentru acele componente (hardware, software etc.) ofertate și definite de furnizor ca fiind echivalent sau cel puțin similare ca performanțe, furnizorul va prezenta documente care să justifice în detaliu din punct de vedere tehnic acest lucru.*

* + - 1. **Factori de evaluare pentru componenta tehnică:**
1. Formularul pus la dispoziţie de autoritatea contractantă în Secţiunea Formulare a Documentaţiei de atribuire);
2. Documente justificative privind susţinerea celor declarate în Formular.
	* + 1. **Respectarea obligațiile relevante în domeniile mediului, social și al relațiilor de muncă:**
3. Declarație privind respectarea condițiilor specifice de muncă și protecție a muncii potrivit art. 51 din Legea nr. 98/2016\*

Informații detaliate se pot obține de la instituțiile competente în domeniu, respectiv Ministerul Mediului, Apelor și Pădurilor, Ministerul Muncii și Solidarității Sociale și de pe site-ul [www.inspectiamuncii.ro](http://www.inspectiamuncii.ro).

***Notă:*** *Autoritatea contractantă nu permite modificarea clauzelor contractuale care ar putea afecta obiectului contractului/obiectivelor stabilite prin prezentul Caietul de sarcini și/sau condițiilor cadru privind îndeplinirea acestora. Autoritatea contractantă va analiza propunerile de modificare a clauzelor contractuale din perspectiva respectării legislației speciale, cât și a celor prevăzute în Caietul de sarcini.*

* + - 1. **Confidențialitatea propunerii tehnice:**

În conformitate cu prevederile art.57 alin.(4) din Legea nr.98/2016, operatorii economici indică și dovedesc în cuprinsul ofertei care informații din propunerea tehnică sunt confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Informațiile indicate de operatorul economic ca fiind confidențiale, inclusiv secrete tehnice sau comerciale și elementele confidențiale ale ofertelor, trebuie să fie însoțite de DOVADA care le conferă caracterul de confidențialitate, în caz contrar nefiind aplicabile prevederile art.57 alin.(1) din Legea nr.98/2016.

Astfel, Propunerea tehnică nu poate fi declarată confidențială, clasificată sau protejată de un drept de proprietate intelectuală în integralitatea sa, ci doar anumite informații din cuprinsul acesteia. Cu titlu de exemplu, precizăm următoarele:

a) toți termenii din Caietul de sarcini care sunt preluați în Propunerea tehnică nu pot fi declarați confidențiali, întrucât Caietul de sarcini este o secțiune a Documentației de atribuire, care este un document public, atașat la Anunțul de participare aferent procedurii de atribuire,

b) CV-urile specialiștilor pot fi declarate confidențiale, pentru acele informații care intră sub incidența prevederilor legale privind datele cu caracter personal sau dacă conțin informații a căror divulgare ar aduce atingere persoanelor respective.

Ofertantul consimte ca, dacă nu marchează informațiile conținute de propunerea tehnica care sunt confidențiale, clasificate sau protejate de un drept de proprietate intelectuală și nu sunt însoțite de dovezi care sa le confere acest drept, autoritatea contractantă are libertatea de a utiliza sau de a dezvălui oricare sau toate aceste informații fără înștiințarea ofertantului.

*NOTA: Documentele propunerii tehnice vor fi numerotate și însoțite de un OPIS.*

Toate produsele componente ale soluției ofertate vor fi prezentate cantitativ în Propunerea tehnică și cantitativ-valoric în Propunerea financiară, specificându-se prețul unitar al fiecărui produs ofertat, cu maxim două zecimale. Prețul produselor componente ale soluției va include toate serviciile asociate, inclusiv suportul tehnic oferit. În cadrul Propunerii financiare, ofertanții vor detalia prețul produselor ofertate, pentru fiecare număr de producător („part number”).

# 12 Alocarea riscurilor în cadrul contractului, măsuri de gestionare a acestora

| **Nr. crt.** | **Risc identificat** | **Măsuri de gestionare a riscurilor****(prevenire, reducere sau eliminare)** |
| --- | --- | --- |
| **1** | Din cauza capacității tehnice/financiare/profesionale reduse a contractantului, execuția contractului se realizează cu dificultăți. | Autoritatea contractantă a solicitat ca cerință minimă de calificare privind capacitatea tehnică și profesională, demonstrarea unui nivel al experienței similare, pentru a se asigura că ofertanții participanți la procedură dețin capacitatea de a asigura cu profesionalism implementarea contractului, dată fiind specificitatea produsului solicitat și a serviciilor asociate. |
| **2** | Din cauza capacității tehnice/financiare/profesionale reduse a contractantului, este posibil ca obligațiile contractuale să fie neîndeplinite/îndeplinite necorespunzător, ori cu întârziere. | Pentru compensarea prejudiciului suferit ca urmare a îndeplinirii necorespunzătoare, ori cu întârziere sau a neîndeplinirii obligațiilor asumate de către contractant, autoritatea contractantă include în contract:1. dreptul de a aplica valoarea dobânzii legale penalizatoare, conform prevederilor art. 3 alin. (21) din OG nr. 13/2011 privind dobânda legală remuneratorie și penalizatoare pentru obligații bănești, precum și pentru reglementarea unor măsuri financiar-fiscale în domeniul bancar, cu modificările și completările ulterioare, aprobată prin Legea nr. 43/2012, cu modificările şi completările ulterioare, calculată la valoarea cu TVA a obligației neîndeplinite pentru fiecare zi de întârziere, dar nu mai mult decât valoarea contractului;
2. dreptul de a aplica penalități în caz de abateri de la nivelul minim de disponibilitate a serviciilor de suport tehnic, respectiv timpii de intervenție prevăzuți în Caietul de sarcini;
3. dreptul de a rezilia contractul din vina contractantului și de a pretinde plata de daune-interese;
4. posibilitatea executării garanției de bună execuție, în limita prejudiciului creat.
 |
| **3** | Din cauza analizării neaprofundate a documentelor, există riscul apariției unor erori nedetectate la momentul semnării contractului, incluse în oferta contractantului. | În contract se prevede faptul că, în cazul apariției de neconcordanțe între Propunerea tehnică și Caietul de sarcini, primează prevederile din Caietul de sarcini. |
| **4** | Din cauza unei slabe organizări a contractantului, există riscul nerespectării termenelor de livrare, instalare, punere în funcțiune. | Prin Caietul de sarcini, autoritatea contractantă a solicitat „Planul de execuție”, ce va fi propus de către furnizor și agreat cu achizitorul. |
| **5** | Din cauza unei slabe comunicări între furnizor și producător/distribuitor, există riscul de a furniza produse care nu îndeplinesc specificațiile tehnice. | Prin Caietul de sarcini s-a prevăzut obligația contractantului de a garanta că produsele software și hardware furnizate prin contract sunt noi, de ultimă generație, și încorporează toate îmbunătățirile recente în proiectare și din ultima versiune, inclusiv din punct de vedere al securității. Furnizorul are obligația de a garanta că toate produsele furnizate prin contract sunt livrate pe canalul oficial al producătorului, acoperind zona UE. |
| **6** | Din diverse cauze de natură tehnică, produsele livrate pot funcționa necorespunzător sau se pot defecta. | Autoritatea contractantă a inclus în Caietul de sarcini cerința de asigurare a serviciilor de garanție și suport tehnic pentru o perioadă de minim 36 de luni.De asemenea, prin Caietul de sarcini, autoritatea contractantă a prevăzut obligația contractantului de a asigura funcționarea produsului, reparând sau înlocuind prin grija și pe cheltuiala lui orice componentă hardware sau accesoriu. Dacă durata de efectuare a reparației depășește 5 zile lucrătoare de la notificarea transmisă de achizitor, produsul defect se va înlocui cu un alt produs nou, identic sau superior calitativ, compatibil din punct de vedere hardware și software. |
| **7** | Din cauza unei slabe organizări a contractantului, există riscul de a nu respecta nivelul de disponibilitate a serviciilor de suport tehnic, respectiv timpii de intervenție prevăzuți în Caietul de sarcini. | La nivel contractual s-au introdus penalități în caz de abateri de la nivelul minim de disponibilitate a serviciilor de suport tehnic, respectiv timpii de intervenție prevăzuți în Caietul de sarcini. |
| **8** | Riscul utilizării necorespunzătoare a soluției de către personalul achizitorului. | Prin Caietul de sarcini, autoritatea contractantă a prevăzut obligația contractantului de a asigura cursuri de instruire pentru minim 5 persoane. Cursurile vor cuprinde atât partea teoretică cât și practică. |