PLEC DE PRESCRIPCIONS TÈCNIQUES PER AL SUBMINISTRAMENT D'UN NOU SISTEMA ANTIVIRUS I PROTECCIÓ PER A L'INSTITUT CATALÀ DE NANOCIÈNCIA I NANOTECNOLOGIA (ICN2).

Exp. 2025-28 ICN2

1. OBJECTE

L'objecte del present plec de prescripcions tècniques és establir les condicions i requisits tècnics que han de regir la contractació del subministrament, instal·lació, configuració i posada en funcionament d'un nou sistema antivirus per a la protecció dels equips informàtics i servidors de l'organització, en substitució de l'actual solució antivirus.

El nou sistema antivirus haurà de garantir una protecció integral davant de les amenaces informàtiques actuals i futures, incloent-hi virus, malware, ransomware, spyware, troians i altres tipus de codi maliciós, així com proporcionar eines de gestió centralitzada, actualitzacions automàtiques i informes detallats sobre l'estat de seguretat de la infraestructura.

Aquesta contractació inclou, a més, la migració des de l'antivirus existent, la formació necessària per al personal tècnic, el suport tècnic del fabricant i l'actualització de les llicències durant el període contractual establert.

2. PRESSUPOST LICITACIÓ

El pressupost total de licitació ascendirà com a màxim a **139.150 EUROS, IVA INCLÒS, amb el següent desglossament: base imposable: 115.000€ + 24.150€ (21% IVA).**

El pressupost es divideix de la següent forma:

- Pressupost màxim de licitació corresponent a les llicències: 100.000 euros + IVA.
- Pressupost màxim de licitació corresponent als serveis professionals i bossa d'hores: 15.000 euros + IVA

3. REQUERIMENTS MINIMS TÈCNICS

Per tal d' optimitzar les operacions de seguretat i beneficiar-se de les sinergies tecnològiques, l'ICN2 requereix una plataforma única, d' un fabricant de ciberseguretat de reconegut prestigi, que incorpori totes les funcionalitats de protecció, detecció, resposta, gestió de riscos i conscienciació d' usuaris definits en els següents punts.

Així mateix, la plataforma ha d' oferir la possibilitat a futur d' activar dins d' aquesta els mòduls addicionals següents:

- NDR
- Protecció de Correu Electrònic i eines col·laboratives.
- Gestió del risc.
- Conscienciació a usuaris i campanyes de phishing.

3.1 PLATAFORMA DE CIBERSEGURETAT

Requisits Generals

- La plataforma s'haurà de proporcionar en model Software as a Service (SaaS).

- La infraestructura de la plataforma, així com les dades contingudes en la mateixa, hauran d' estar allotjades dins de la Unió Europea.
- La plataforma haurà d' incorporar tots els mòduls descrits en els següents punts d' aquest apartat, no essent vàlides aquelles plataformes que requereixin solucions d' altres fabricants per proporcionar alguna de les funcionalitats demanades.
- La gestió de la plataforma i tots els seus mòduls, haurà de realitzar-se mitjançant una consola única i accessible mitjançant navegador web.
- La plataforma s'haurà d'integrar amb Microsoft Entra ID per a la gestió i el control d'accés dels usuaris que l'operin.
- La plataforma haurà de proporcionar control d' accés basat en rols per a la seva operació.
- La plataforma haurà d' emmagatzemar durant 180 dies com a mínim, tota la telemetria i esdeveniments de detecció generats pels diferents mòduls requerits.
- A continuació, es descriu, a alt nivell, la infraestructura tecnològica que la plataforma haurà de protegir:

Descripció	Volumetria
Estacions de treball	501
Servidors	80

3.1.1 Protecció d'estacions de treball

L' agent de protecció per a estació de treball haurà d' estar suportat en els següents sistemes operatius:

- Microsoft Windows XP i posteriors
- MacOS 12.0 i posteriors
- Ubuntu Linux

A més, la solució proposada haurà de complir amb els requisits següents:

- Antimalware avançat
  - Detecció basada en firmes i reputació de fitxers per a malware conegut.
  - Machine Learning predictiu per a la detecció d'amenaces desconegudes i Zero-Day.
  - Detecció de Spyware i Grayware.
  - Anàlisi de comportament per a la detecció i bloqueig d' activitats sospitoses i canvis no autoritzats, inclòs el ransomware.
  - Anti-ransomware avançat que permeti la detecció de variants de ransomware conegut i que incorpori un motor de recuperació de dades que creï còpies dels arxius xifrats, permetent la recuperació d' aquests en el cas que hagin estat xifrats per un procés de ransomware.
  - Protecció Anti-Exploit que permeti l' anàlisi de fitxers i processos a la recerca de codi d' explotació incrustat.
  - Detecció en temps real d' execució de codi maliciós en memòria.

- Anàlisi de reputació web
  - Haurà de proporcionar un filtratge de continguts mitjançant el bloqueig de l' accés a URLs, IPs i dominis maliciosos coneguts, així com el bloqueig de comunicacions C&C.
  - Aquesta protecció no s' haurà de limitar únicament a les comunicacions realitzades des del navegador, sinó que haurà de ser funcional a nivell de kernel, permetent l' anàlisi de les comunicacions de processos, serveis i altres aplicacions.

- Firewall de host
  - Haurà de permetre regles de firewall per al trànsit entrant i/o sortint a nivell de host.
  - Haurà de permetre definir IPs o xarxes d' IPs com a confiables per tal de no analitzar-ne el trànsit provinent.
  - Haurà de proporcionar un conjunt de regles predefinides per als casos d' ús més comuns, per tal de facilitar la configuració per part dels administradors.
  - Haurà de poder detectar i bloquejar, com a mínim, els següents atacs de reconeixement:
    - Escaneig de ports TCP i UDP
    - Escaneig TCP Null
    - Proves de detecció d'empremta del sistema operatiu (OS Fingerprint)

- Patching virtual
  - Haurà de detectar i bloquejar atacs basats en xarxa a vulnerabilitats conegudes, tant en aplicacions com en sistemes operatius, mitjançant l'ús de regles de prevenció d'intrusions (HIPS).
  - L' aplicació d' aquests patchings virtuals s' haurà de realitzar sense que es requereixi el reinici dels equips i sense que es produeixi pèrdua de servei.
  - Els patchings virtuals s'hauran de poder configurar indistintament en mode detecció i notificació o en mode bloqueig, tant a nivell de política com a nivell individual de cada patching virtual.
  - Haurà de proporcionar, com a mínim, un conjunt de patchings virtuals predefinits per:
    - Sistemes operatius Microsoft d'escriptori
    - Microsoft Office
    - Navegadors Chrome, Firefox i Edge
    - Adobe Acrobat

- Control d' aplicacions
  - Funcionalitat que permeti limitar l'execució d'aplicacions en el servidor basant-se en el checksum de l'arxiu (hash SHA-1).
  - Aquesta funcionalitat ha de permetre aplicar la protecció en 2 maneres:
    - Mode restrictiu: En aquesta manera no es permet l' execució de cap executable llevat d' aquells que hagin estat expressament autoritzats.
    - Mode permissiu: En aquesta manera es permet l' execució de qualsevol executable llevat d' aquells que hagin estat denegats expressament.

- La funcionalitat haurà de permetre l'activació d'una manera manteniment, durant el qual es permeti l'execució de programari (ex.: instal·lació de nou programari, actualitzacions, etc...).

- Control de dispositius

  Funcionalitat que permeti el control d' accés a dispositius d' emmagatzematge extern. Haurà de cobrir, com a mínim, els casos següents:

  - Accés a dispositius d' emmagatzematge extern USB amb els següents permisos: Accés complet, Només Lectura, Bloqueig.
  - Accés a dispositius mòbils com emmagatzematge extern amb els següents permisos: Accés complet, Només Lectura, Bloqueig.
  - Prevenir l'autoejecció (autorun) de dispositius USB.

  A més, es requereix poder excepcionar dispositius USB a nivell global o per política, indicant el fabricant, model i número de sèrie d'aquests.

3.1.2 Protecció de Servidors

L' agent de protecció per a servidors haurà d' estar suportat en els següents sistemes operatius:

- Microsoft Windows Server 2012 i 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 i Windows Server 2025.
- CentOS Linux versions 6, 7 i 8
- Debian Linux versions 10, 11 i 12
- Oracle Linux versions 7, 8 i 9
- Red Hat Enterprise Linux versions 6, 7, 8 i 9
- Suse Linux versions 12 i 15
- Ubuntu Linux versions 16.04, 18.04, 20.04, 22.04 i 24.04

A més, la solució proposada haurà de complir amb els requisits següents:

- Antimalware Avançat
  - Detecció basada en firmes i reputació de fitxers per a malware conegut.
  - Machine Learning predictiu per a la detecció d'amenaces desconegudes i Zero-Day.
  - Detecció de Spyware i Grayware.
  - Anàlisi de comportament per a la detecció i bloqueig d' activitats sospitoses i canvis no autoritzats, inclòs el ransomware.
  - Anti-ransomware avançat que permeti la detecció de variants de ransomware conegut i que incorpori un motor de recuperació de dades que creï còpies dels arxius xifrats, permetent la recuperació d' aquests en el cas que hagin estat xifrats per un procés de ransomware.
  - Protecció Anti-Exploit que permeti l' anàlisi de fitxers i processos a la recerca de codi d' explotació incrustat.
  - Detecció en temps real d' execució de codi maliciós en memòria.

- Anàlisi de Reputació Web
  - Aquesta funcionalitat haurà de proporcionar un filtratge de continguts mitjançant el bloqueig de l' accés a URLs, IPs i dominis maliciosos coneguts, així com el bloqueig de comunicacions C&C.
  - Aquesta protecció no s' haurà de limitar únicament a les comunicacions realitzades des del navegador, sinó que haurà de ser funcional a nivell de kernel, permetent l' anàlisi de les comunicacions de processos, serveis i altres aplicacions.

- Firewall de Host
  - Haurà de permetre regles de firewall per al trànsit entrant i/o sortint a nivell de host.
  - Haurà de permetre definir IPs o xarxes d' IPs com a confiables per tal de no analitzar-ne el trànsit provinent.
  - Haurà de proporcionar un conjunt de regles predefinides per als casos d' ús més comuns, per tal de facilitar la configuració per part dels administradors.
  - Haurà de poder detectar i bloquejar, com a mínim, els següents atacs de reconeixement:
    - Escaneig de ports TCP i UDP
    - Escaneig TCP Null
    - Proves de detecció d'empremta del sistema operatiu (OS Fingerprint)

- Patching virtual
  - Haurà de detectar i bloquejar atacs basats en xarxa a vulnerabilitats conegudes, tant en aplicacions com en sistemes operatius, mitjançant l'ús de regles de prevenció d'intrusions (HIPS).
  - L' aplicació d' aquests pegats virtuals s' haurà de realitzar sense que es requereixi el reinici dels equips i sense que es produeixi pèrdua de servei.
  - Els pegats virtuals s'hauran de poder configurar indistintament en mode detecció i notificació o en mode bloqueig, tant a nivell de política com a nivell individual de cada patching virtual.
  - L' agent de protecció haurà de realitzar una anàlisi de les vulnerabilitats de xarxa del sistema operatiu i les aplicacions que afecten l' equip per, seguidament, aplicar únicament aquells pegats virtuals als quals aquest és vulnerable. Tant l' anàlisi de vulnerabilitats com l' aplicació dels pegats virtuals, s' haurà de realitzar de manera automatitzada i periòdica sense que es requereixi intervenció per part dels administradors de la solució.
  - Haurà de proporcionar pegats virtuals per a tots els sistemes operatius requerits, inclosos aquells que són obsolets i per als quals els diferents fabricants ja no desenvolupen els seus físics.
  - Haurà de proporcionar, com a mínim, patchings virtuals per a les següents aplicacions crítiques:
    - Servidors de Base de Dades: Oracle, MySQL, Microsoft SQL Server
    - Servidors Web: Microsoft Internet Information Server, Apache i Nginx
    - Servidors d' Aplicació: Apache Tomcat, Oracle Weblogic, i servidors d' aplicació basats en PHP

- Control d' aplicacions
  - Funcionalitat que permeti limitar l'execució d'aplicacions en el servidor basant-se en el checksum de l'arxiu (hash SHA-1).
  - Aquesta funcionalitat ha de permetre aplicar la protecció en 2 maneres:
    - Mode restrictiu: En aquesta manera no es permet l' execució de cap executable llevat d' aquells que hagin estat expressament autoritzats.
    - Mode permissiu: En aquesta manera es permet l' execució de qualsevol executable llevat d' aquells que hagin estat denegats expressament.
  - La funcionalitat haurà de permetre l'activació d'una manera manteniment, durant el qual es permeti l'execució de programari (ex.: instal·lació de nou programari, actualitzacions, etc...).

- Correlació d' esdeveniments
  - Funcionalitat per a la correlació d' esdeveniments de seguretat detectats en els logs de sistema operatiu i aplicacions.
  - Aquesta correlació es basarà en regles assignades automàticament pel producte en base al sistema operatiu i aplicacions instal·lades.
  - Les regles definides permetran identificar comportaments sospitosos (ex.: Creació de comptes, intents d'autenticació per força bruta, etc) associant les deteccions a tàctiques i tècniques d'atac identificades pel framework de MITRE ATT&CK.

- Monitoratge d' integritat
  - Funcionalitat que permeti monitoritzar arxius, serveis i claus de registre comparant el contingut i permisos d' aquests en qualsevol moment, enfront d' una línia de base inicial.
  - Aquest monitoratge es basarà en regles predefinides i aplicades de manera automàtica pel producte en base al sistema operatiu i aplicacions instal·lades.
  - Aquestes regles facilitaran el compliment normatiu mapejant tècniques i tàctiques d' atac del marc ATT&CK de MITRE.
  - El sistema generarà una alerta en el cas de detectar qualsevol modificació sobre els mateixos.

3.1.3 XDR

Per millorar les capacitats de detecció i resposta enfront d' amenaces, es requereix un mòdul de XDR que permeti la detecció, correlació, investigació i resposta avançades.

El mòdul de XDR haurà d' estar suportat, com a mínim sobre els següents sistemes operatius:

- Microsoft Windows XP i posteriors
- MacOS 12.0 i posteriors
- Microsoft Windows Server 2012 i 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 i Windows Server 2025.
- CentOS Linux versions 6, 7 i 8
- Debian Linux versions 10, 11 i 12
- Oracle Linux versions 7, 8 i 9
- Red Hat Enterprise Linux versions 6, 7, 8 i 9

- Suse Linux versions 12 i 15
- Ubuntu Linux versions 16.04, 18.04, 20.04, 22.04 i 24.04

A més, el mòdul de XDR haurà de complir amb els requisits següents:

- Característiques generals
  - Haurà de recollir esdeveniments de seguretat i telemetria, sento això últim indispensable per a la detecció, ús, o accions de remediació de qualsevol activitat relacionada amb els actors implicats.
  - Tota la telemetria necessària serà recollida mitjançant agents o sensors del propi fabricant de la plataforma, no sent vàlides aquelles solucions que necessitin agents o sensors de tercers per a aquest propòsit.
  - El mòdul haurà de recollir telemetria i esdeveniments de seguretat dels següents vectors:
    - Servidors
    - Estacions de treball
    - Gestors d' identitats: Active Directory i Entra ID
    - Plataformes de correu electrònic: Exchange Online i Google Mail
    - Tallafocs: Fortinet, Palo Alto i Checkpoint

- Detecció i investigació d' amenaces
  - El mòdul haurà de ser capaç d' analitzar, correlacionar i contextualitzar la telemetria de tots els vectors requerits.
  - El fabricant de la solució haurà de proporcionar i mantenir un mínim de 1.000 models de detecció utilitzant tècniques de Machine Learning. Aquests models de detecció es basaran en les tècniques i tàctiques del Mitre ATT&CK Enterprise Framework (https://attack.mitre.org/tactics/enterprise/).
  - El mòdul haurà de permetre la creació de models de detecció personalitzats.
  - En base a les tecnologies d' anàlisi anteriorment esmentades, el mòdul de XDR haurà de ser capaç d' identificar aquells comportaments susceptibles de ser una amenaça i mostrar únicament alertes de valor, minimitzant els falsos positius i la informació supèrflua.
  - La solució d' XDR haurà de mostrar el contingut de les alertes de manera gràfica, amb tots els elements que conformen l' alerta i els fluxos de comunicació. Així mateix, haurà de permetre l' execució de les accions de resposta i recerques avançades directament des de l' objecte representat gràficament, mitjançant l' ús de menús contextuals.
  - L' alerta contindrà la informació bàsica per iniciar l' anàlisi:
    - Data i hora de la detecció.
    - Índex de risc de l' alerta.
    - Impacte (usuaris, equips i/o bústies involucrades en l'alerta).
    - Informació sobre el model de detecció que ha generat l'alerta i les tècniques del Mitre ATT&CK Enterprise Framework utilitzades.
    - Objectes clau involucrats en l'alerta (fitxers, claus de registre, execucions de comandaments, URLs, IPs etc...).

- El mòdul de XDR haurà de proporcionar l' arbre de processos dels esdeveniments i objectes involucrats en l' alerta, així com la cronologia de la seva execució.
- La solució d' XDR haurà de proporcionar una eina que permeti les recerques avançades pels principals camps de tota la telemetria recollida en els diferents vectors. Aquesta eina de recerca haurà de permetre el filtratge i l' execució d' accions de resposta directament en els resultats, així com guardar recerques per al seu posterior ús.
- Haurà de ser capaç d' agrupar automàticament aquelles alertes que estiguin relacionades en incidents de seguretat, assignant-li un índex de risc que permeti prioritzar les actuacions. Aquests incidents de seguretat hauran de proporcionar, com a mínim:
  - Informació sobre els esdeveniments que conformen l' incident de seguretat.
  - Informació sobre la línia de temps: cronologia en la qual s' han produït els esdeveniments que conformen l' incident.
  - Informació sobre l'impacte: quins equips, usuaris i/o bústies de correu estan involucrades en l'incident.
  - Informació sobre els objectes: que objectes estan involucrats en l'incident (fitxers, claus de registre, execucions de comandaments, URLs, IPs etc...).
- Haurà de permetre la creació de patrons de recerca personalitzats o "Watchlists", els quals alertaran si generen coincidència amb la telemetria rebuda.

- Intel·ligència d'amenaces

  - El fabricant de la plataforma haurà de proporcionar i mantenir un mínim de 2000 informes d'intel·ligència que incorporin indicadors de compromís (IoC) i indicadors d'atac (IoA) de les principals amenaces i campanyes existents. La solució també haurà de ser capaç d'analitzar automàticament la telemetria de tots els vectors a la recerca d'aquests indicadors i generar alertes en cas de coincidència.
  - A més dels informes d'intel·ligència a dalt esmentats, la solució XDR permetrà crear plantilles d'intel·ligència personalitzades basades en indicadors de compromís importats des de fitxers CVS, SITX o serveis com TAXII feeds o MISP, els quals també generaran una alerta en cas que aquests objectes maliciosos siguin trobats a la xarxa corporativa.
  - La solució XDR haurà de poder integrar-se amb serveis d'intel·ligència d'amenaces de tercers mitjançant els estàndards MISP i TAXII.
  - La solució XDR haurà de permetre la incorporació d' indicadors de compromís de manera manual o mitjançant la importació de fitxers CSV i STIX. Aquests indicadors de compromís han de ser, com a mínim:
    - URLs
    - IPs
    - Dominis
    - Hashes de ficheros SHA-1 o SHA-256

        - Remitents de correu electrònic
    - El mòdul XDR haurà de permetre compartir indicadors de compromís (IoC) a la resta de mòduls integrats a la plataforma, així com a solucions de tercers.

- Resposta davant d' amenaces

    - Des de la solució de XDR s' hauran de poder executar les següents accions de resposta a les estacions de treball i servidors:
        - Aïllar l' equip.
        - Executar una shell remota amb comandaments que permetin la recerca i que tingui la capacitat de realitzar un bolcat de memòria.
        - Executar un script remot prèviament carregat a la plataforma, ja sigui en powershell o en bash.
        - Acabar un procés.
        - Bloquejar fitxers mitjançant hash SHA-1 o SHA-256.
        - Bloquejar IPs, URLs i dominis.
        - Recol·lectar un fitxer de l'equip per a la seva posterior anàlisi.
        - Executar consultes en temps real mitjançant l' ús d' Osquery i regles YARA
    - El mòdul de XDR haurà de poder executar les següents accions de resposta en usuaris d' Active Directory i Entra ID:
        - Deshabilitar un usuari
        - Habilitar un usuari.
        - Forçar el reset de contrasenya d' un usuari.
        - Logout de les aplicacions d' Office 365.
        - El mòdul de XDR haurà de poder integrar-se amb firewalls de Fortinet, Palo Alto i Checkpoint per realitzar les següents accions de resposta:
        - Bloquejar IPs
        - Bloquejar URLs
        - Bloquejar Dominis
    - L' execució de les accions de resposta s' haurà de poder realitzar indistintament de manera manual o de manera automatitzada. L' automatització de les respostes es realitzarà mitjançant l' execució de playbooks ja preconfigurats o la creació de playbooks personalitzats.

4. SERVEIS PROFESSIONALS

Aquest és un projecte clau en mà.

En resum, els serveis professionals han d'incloure totes aquelles accions necessàries per garantir l'èxit del projecte:

- Anàlisi i disseny
- Validació de requeriments
- Desplegament de les plataformes
- Disseny i configuració de polítiques
- Realització integracions

- Desplegament equips maqueta i suport al desplegament
- Desinstal·lació de l'antivirus actual, mitjançant script per desinstal·lació massiva o, si no fos possible, mitjançant un procediment que inclogui la desinstal·lació en 10 equips a escollir per l'ICN2, formant als tècnics IT de l'institut per fer el mateix a la resta d'equips.
- Validació de funcionament
- Formació
- Documentació i gestió
- Bossa de 100 hores per a qualsevol requeriment per part de l'ICN2 relacionat amb la solució desplegada: noves polítiques, incidències, noves configuracions, etc.

En detall, es demana el següent:

- Anàlisi i disseny: Valoració dels sistemes operatius, requisits, comunicacions i la resta d'aspectes tècnics necessaris.
- Desplegament i configuració general: Instal·lació i ajust de la consola.
- Desenvolupament i configuració de polítiques de seguretat: Configuració de tots els mòduls de protecció, incloent la protecció en temps real, monitoratge comportamental, aprenentatge automàtic, etc.
- Disseny de perfils d'escombrat.
- Ajust de les regles de protecció IPS.
- Activació i parametrització de models de detecció i informes.
- Instal·lació d'agents: Desplegament automàtic d'agents en 10 estacions de treball i 10 servidors a escollir pel personal d'IT de l'ICN2. Sempre que sigui possible s'haurà d'utilitzar una eina de desplegament de software, i es cercarà automatitzar el procés en la mesura del possible.
- Validació i proves: Verificació del funcionament correcte i realització de proves.
- Documentació: Elaboració i lliurament de la documentació generada durant el projecte.
- Formació: Sessió de formació impartida per un enginyer certificat.
- Gestió integral del projecte: Coordinació i seguiment de totes les tasques des del principi fins a la finalització.

5. TERMINI D'EXECUCIÓ I DURACIÓ DEL CONTRACTE

El projecte haurà d'estar finalitzat en el termini de 2 mesos des de la data d'inici del contracte.

El contracte tindrà una durada de 5 anys.

6. FACTURACIÓ

La facturació serà de la següent manera:

- Els serveis professionals i la bossa d'hores es pagaran a l'inici del contracte i es farà en un sol pagament
- Les llicències es pagaran de forma anual durant els 5 anys de durada del contracte.

7. <u>INFORMACIÓ ADDICIONAL:</u>

Es podrà sol·licitar informació addicional mitjançant enviament d'email a la següent adreça.

- **contracts@icn2.cat**

Bellaterra, a 20 de novembre de 2025

Javier Dameá

L1-L2 Helpdesk support and Intranet Administrator