PLEC DE CLÀUSULES TÈCNIQUES RELATIU AL SUBMINISTRAMENT PER SUBSCRIPCIÓ ANUAL DE LES LLICÈNCIES DE CYNET 360 AUTOXDR ALL IN ONE (per EndPoints i Servers) - CYNET 360 MOBILE (per iOS i Android) I SUPORT 24 X 7 PER AL LABORATORI DE REFERÈNCIA DE CATALUNYA S.A.

EXPEDIENT LRC 5/2025-PS

10 de febrer de 2025

ÍNDEX

Contingut

1. ANTECEDENTS

El laboratori de Referència de Catalunya, S.A. (en endavant LRC) ofereix als centres sanitaris i als seus professionals la informació en anàlisis clíniques que necessiten com a suport al diagnòstic i a les decisions clíniques, que els ajudaran a millorar l'atenció als seus usuaris. A més, disposa d'una xarxa de Laboratoris Hospitalaris i d'un Laboratori Core de Referència, posant a disposició dels seus Clients/Socis un ampli catàleg de proves de totes les àrees de coneixement.

El LRC té la necessitat de protegir la informació dels socis/clients perquè les dades són vitals per mantenir en funcionament el nostre negoci i per donar resposta a la necessitat de protegir les dades històriques per requeriments legals marcats pel Sector Salut.

Per això, es necessita una solució única i robusta per a la gestió integral de les dades, que sigui prou flexible i potent per protegir totes les fases del cicle de vida de les seves dades i tot el que sigui possible per enfrontar-se a les ciberamenaces ara i en el futur. D'acord a la nostre experiència la solució requerida està preparada per a aquesta tasca.

2. OBJECTE DE LA CONTRACTACIÓ

L'objecte del present contracte és la contractació per part del LRC del subministrament relatiu a les llicències de software, que es concreta en l'adquisició en modalitat subscripció de:

Concepte	Quantitat
CYNET 360 AUTOXDR ALL IN ONE (per EndPoints i Servers)	301
CYNET 360 MOBILE (per iOS i Android)	20

La data de venciment de l'actual subscripció és el **13 de maig de 2025**.

3. CYNET 360 AUTOXDR ALL IN ONE i CYNET 360 MOBILE

3.1. Característiques Tècniques Mínimes

Les característiques mínimes del subministrament de les llicències del programari de Ciberseguretat, en modalitat de subscripció anual, corresponents a l'objecte del present contracte, són les següents:

Compatibilitat amb Sistemes Operatius

La versió subministrada haurà de ser compatible amb els sistemes operatius següents:

- Windows:
    - Sistema operatiu d'estació de treball: Windows XP SP3 i superior, Windows Vista SP1 i superior, Windows 7 SP1 i superior, Windows 8, Windows 8.1, Windows 10, Windows 11.
    - Sistema operatiu del servidor: Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.
- Linux:
    - Ubuntu 16.04 i superior, RedHat 7 i superior, Centos 6.9 i superior, Fedora 23 i superior, Debian 9.X i superior, Suse 12 i superior, Oracle Enterprise Linux 7.6 i superior, Amazon Linux, Amazon Linux 2.

- Mac US:
    - 10.13 o superior.

Capacitats Essencials

Els productes han de ser capaços de suportar els sistemes operatius esmentats i oferir les capacitats següents:

- Protecció: Integrar tecnologies avançades per a la detecció i prevenció d'amenaces a tot l'entorn, amb capacitats EPP, EDR, anàlisi de comportament de l'usuari, regles de detecció de xarxa i intel·ligència d'amenaces.
- Correlació: analitzar dades rellevants d'agents, registres i sensors de tercers per generar incidents processables i gestionar-los de manera centralitzada.
- Investigació i Resposta: Facilitar la investigació d'amenaces i orquestrar accions automàtiques de resolució a tot l'entorn.

Funcionalitats Clau

La solució ha de proporcionar la monitorització, investigació, anàlisi sota demanda, resposta davant d'incidents i cerca proactiva d'amenaces amb un servei MDR del fabricant 24x7 que permeti:

- Vista 360 º d'alertes
- Protecció de punts de connexió

Antivirus NGAV

- Anàlisi estàtica de fitxers en repòs i no executables per protegir contra codi maliciós conegut.
- Prevenció d'explotació de vulnerabilitats basada en comportament.
- Protecció contra atacs sense fitxers mitjançant macros i scripts.
- Identificació i prevenció d'execució de codi maliciós (malware) amb firmes conegudes.

Control de Dispositius

- Detecció i bloqueig de dispositius d'emmagatzematge extern (ex. USB, targetes SD).

Protecció de Recursos Crítics

- Protecció d'usuaris, xarxes, endpoints, servidors, fitxers, processos i configuracions al núvol.

Detecció Estesa d'Amenaces EDR

- EDR avançat per prevenir, detectar i respondre a amenaces conegudes i desconegudes a tot l'entorn.
- Característiques com SSDEEP Scan, patrons de memòria, tecnologia de detecció avançada (ADT) i control en mode kernel.

Regles d'Anàlisi del Comportament de l'Usuari (UBA/UEBA):

- Analitzar el comportament d'usuaris i entitats per identificar activitats inusuals i generar alertes sobre comportaments sospitosos.

Detecció i Resposta a la Xarxa (NDR):

- Analitzar l'activitat de la xarxa per detectar atacs, incloent-hi:
    - Robatori de credencials basat a la xarxa: Suplantació d'ARP, resposta DNS.
    - Moviment lateral a la xarxa: Identificació d'activitats de propagació no autoritzades.
    - Comunicació sortint maliciosa: C2C, suplantació d'identitat, phishing.
    - Reconeixement basat a la xarxa: detectar atacs d'escaneig i exploració.

- Filtració de dades a la xarxa: Ex-filtració a través de túnels utilitzant diversos protocols.

Entorn de proves:

- Enviar fitxers per a la vostra inspecció mitjançant l'entorn de proves Smart Simulation Execution (SSE) en un Sandbox.

Operacions de TI, Seguretat i Higiene:

- Gestió de vulnerabilitats: Identificació i mitigació de debilitats a la infraestructura.
- Inventari d'actius: Registre i seguiment detallat de tots els actius de la infraestructura.

Threat Intelligence

- Protecció de memòria en temps real contra ransomware.
- Filtratge de fitxers i components crítics en temps real.

Deception

- Implementació de fitxers, hosts i comptes d'usuari fictícies per integrar-se a la infraestructura, sense necessitat d'instal·lar agents addicionals ni recórrer a maquinari On-Premise.

Centralized Log Management

- Recopilació centralitzada de logs de tercers, amb capacitat de manejar fins a 15 GB de dades diàries de mitjana i una retenció de logs de fins a 14 dies.

SSPM & CSPM

- Integració amb tres plataformes de Cloud de tercers per monitoritzar, comparar i corregir configuracions errònies de l'entorn. Aquesta integració es realitza comparant les configuracions amb els principals estàndards de seguretat de la indústria (com NIST, PCI, ISO27001, entre d'altres) i les millors pràctiques recomanades pels proveïdors de la plataforma.

Protecció de correu electrònic

- Antimalware de nova generació per a la protecció del correu electrònic integrat a M365.

Security Operations Center (SOC):

- Centre d'Operacions de Seguretat, per prevenir, monitoritzar i controlar la seguretat a la xarxa de l'organització 24x7. El SOC ha de tenir un servei de control d'alertes, resposta remota a incidents (IR) i informes sobre atacs.

3.2. Detecció i Prevenció de Malware

Capacitats

- La solució ha d'identificar fitxers maliciosos i prevenir-ne l'execució, incloent virus, troians, ransomware, spyware, cryptominers i qualsevol altre tipus de codi maliciós.
  - Protecció contra codi maliciós basada en signatures
  - Anàlisi estàtica mitjançant Machine Learning
  - Anàlisi dinàmic (Sandbox en temps real)
  - Intel·ligència d'amenaces (VT)
  - Intel·ligència d'amenaces (fonts externes no-VT)
- La solució ha d'identificar comportaments maliciosos de fitxers executats, processos en execució, modificacions al registre, accés a memòria i bloquejar en temps d'execució o generar una alerta.
  - Supervisió d'accés a memòria

  - Anàlisi del comportament del procés (heurística)
  - Alta similitud (fuzzy hashing)
  - Intel·ligència d'amenaces
- La solució ha de suportar la creació de regles per excloure rangs d'adreces/IP específiques.
  - Llistat negre d'IPs i dominis maliciosos
- La solució ha d'identificar i bloquejar atacs d'escalada de privilegis.
  - Supervisió de processos
- La solució ha d'identificar i bloquejar atacs de reconeixement (escaneig).
  - Supervisió del trànsit de xarxa
- La solució ha d'identificar i bloquejar intents de robatori de credencials, ja sigui des de la memòria (dump de credencials, força bruta) o tràfic de xarxa (spoofing ARP, Resposta DNS).
  - Supervisió de memòria
  - Supervisió de comptes d'usuari (intents d'accés)
  - Anàlisi del comportament del trànsit de xarxa

3.3. Moviment Lateral i Comportament Maliciós

- La solució ha d'identificar i bloquejar/alertar de moviments laterals (SMB relay, pass the hash, etc.).
  - Supervisió del trànsit de xarxa
  - Engany mitjançant nodes falsos
  - Engany mitjançant comptes d'usuari falsos
  - Engany mitjançant connexions de xarxa falses
- La solució ha d'identificar comportaments maliciosos a comptes d'usuari, indicatius d'un compromís previ.
  - Configuració de polítiques d'activitat d'usuari (violacions de polítiques)
  - Perfil de comptes d'usuari (detecció d'anomalies)
- La solució ha d'identificar interaccions malicioses amb fitxers de dades.
  - Engany mitjançant arxius esquer *"señuelo"*
- La solució ha d'identificar ex-filtració de dades mitjançant protocols legítims (túnels DNS, túnels ICMP).
  - Supervisió del trànsit de xarxa
  - Supervisió de l'accés a fitxers
- La solució ha d'identificar i bloquejar l'ús d'eines d'atac comunes (Metasploit, Empire, Cobalt, etc.).
  - Supervisió de processos
- La solució ha de tenir un mecanisme de protecció intern contra l'accés i la manipulació d'usuaris no autoritzats.
  - Generar alerta i bloquejar qualsevol intent de manipulació o desactivació

3.4. XDR - Monitorització i Control

Capacitats

- La solució ha de suportar File Integrity Monitoring (FIM).
    - Aplicar polítiques sobre entorns fixos per alertar sobre qualsevol canvi en fitxers
- La solució ha de tenir avaluació de vulnerabilitats incorporada.
    - Descobrir actualitzacions de seguretat mancants en sistemes i aplicacions
- La solució ha d'oferir la capacitat de gestionar inventaris.
    - Mapejar i correlacionar tots els actius dins de l'entorn, com ara punts finals, servidors, aplicacions instal·lades, comptes d'usuari i informes periòdics
- La solució ha de permetre la recopilació i retenció de logs.
    - Recopilar registres d'autenticació i activitat i retenir-los durant el període de temps exigit per diverses normatives
- La solució ha d'incloure Threat Hunting.
    - Buscar presència maliciosa mitjançant IOC coneguts
- La solució ha de suportar el descobriment de superfícies desateses d'atac.
    - Buscar fitxers, processos, connexions de xarxa i comptes d'usuari amb contrasenyes no modificades susceptibles al risc

3.5. Automatització de Resposta: Investigació i Remediació

Capacitats

- La solució ha de recopilar contínuament dades sobre totes les entitats i les activitats dins de l'entorn.
    - Interacció amb fitxers: crear, obrir, reanomenar, eliminar, executar
    - Execució de processos (inclòs l'arbre de processos)
    - Inici de sessió d'usuari
    - Trànsit de xarxa
    - Canvis al registre
    - Programari instal·lat
- La solució ha de permetre la visualització de dades d'entitat i activitat.
    - Cerca basada en patrons de comportament en tots els camps de cobertura (usuaris, fitxers, màquines i trànsit de xarxa)
    - Determinació de regles i/o creació d'alertes i/o determinació del nivell de risc, basada en una resposta al patró de cerca i en temps real
    - Habilitació perquè diversos usuaris realitzin activitats en paral·lel, segons permisos d'usuari, sense necessitat de desconnectar un altre usuari per executar l'activitat
- La solució ha de suportar anàlisi dinàmica.
    - Enviar arxius manualment per anàlisi a sandbox

- La solució ha de permetre consultes entre organitzacions.
    - Buscar ocurrències d'activitats de procés, fitxer, xarxa i usuari a través de tots els punts finals a l'entorn
- La solució ha de suportar l'execució d'investigacions forenses.
    - Procés en execució/arxiu
    - Nivell de màquina
    - Activitats de memòria
    - Obtenir bolcat de memòria
- La solució ha de suportar l'aïllament i la mitigació de presència i activitat maliciosa localment a l'endpoint.
    - Executar ordres coordinades (ex. interfície CMD)
    - Executar scripts o fitxers des d'una ubicació de xarxa o mapejar una unitat
    - Apagar un endpoint i/o servidor
    - Aïllar un endpoint/servidor de la xarxa
    - Eliminar un fitxer (inclosos fitxers en execució actius)
    - Posar un fitxer en quarantena
    - Matar un procés
    - Eliminar o deshabilitar un servei/tasca programada
    - Bloquejar un compte d'usuari local o de domini
    - Restablir la contrasenya d'un usuari
    - Desconnectar targetes de xarxa
    - Canviar adreça IP
    - Editar un fitxer HOST
    - Renovar l'operació d'un endpoint i servidor (Rollback)
- La solució ha de suportar aïllament i mitigació de presència i activitat maliciosa a nivell global a tot l'entorn.
    - Active Directory: deshabilitar usuari, restablir contrasenya
    - Firewall/proxy: bloquejar IP, bloquejar domini, bloquejar port
- La solució ha de suportar automatització de respostes.
    - Playbooks de resposta predefinits
    - Playbooks de resposta personalitzats creats per l'operador

3.6. Infraestructura

Capacitats

- La solució ha de tenir opcions flexibles de desplegament de servidors per adaptar-se a diferents tipus d'entorns.
    - On-prem
    - SaaS
    - Híbrid

- La solució ha de suportar instal·lació ràpida i sense problemes a tots els punts finals/servidors de l'entorn.
- La solució ha de tenir una petjada lleugera per minimitzar l'impacte en el rendiment dels endpoints/servidors.
    - ~25 MB de memòria del sistema (RAM) consumida per cada endpoint/servidor
    - ~2-5% de capacitat de CPU del sistema consumida per cada plataforma d'endpoint
- La solució ha de proporcionar comunicació xifrada entre el servidor de gestió i els agents als punts finals/servidors.
- La solució ha de suportar tots els sistemes operatius comunament usats:
    - Sistemes EOL: Windows XP SP3\Vista, Server 2003 SP2
    - Windows 7 i superiors
    - Windows Server 2008 R2 i superiors
    - Principals distribucions Linux: Fedora, Ubuntu, Debian, Centos, Red Hat, Suse
    - Mac OSX Catalina i superiors
- La solució ha de suportar la connexió a Active Directory.
    - Autenticació granular a la interfície d'usuari
    - Desplegament en diversos grups d'OU amb AD
- La solució ha de coexistir amb tot el programari comercial i propietari als punts finals/servidors:
    - Operació sense problemes de l'endpoint/servidor protegit sense pantalles blaves o caigudes de processos
- La solució ha de proporcionar protecció total per als endpoints i servidors fora de línia de la xarxa de l'organització.
    - Mecanisme de protecció contra amenaces que no depengui de la connectivitat amb el servidor de gestió

3.7. Operació

- La solució ha de poder especificar una llista de regles d'exclusió d'alertes per als objectes seleccionats.
- La solució ha de suportar desplegament a múltiples llocs que reportin a una sola consola de gestió.
- La solució ha de permetre habilitar/deshabilitar certs tipus de notificacions.
- La solució ha de permetre classificar la gravetat de les alertes de seguretat.
- La solució ha de proporcionar una col·lecció central i un processament d'alertes en temps real.
- La solució ha de permetre bloquejar l'accés a la configuració del programa pels usuaris finals.
- La solució ha de proporcionar distribució centralitzada d'actualitzacions sense necessitat d'intervenció de l'usuari i sense reiniciar l'endpoint/servidor.
- La solució ha de permetre especificar un horari per a la descàrrega d'actualitzacions, incloent-hi l'opció de deshabilitar l'actualització automàtica.
- La solució ha d'assignar una puntuació de risc a tots els objectes dins de l'entorn protegit.
- La solució ha de suportar el registre d'esdeveniments, alertes i actualitzacions.

- La solució ha de suportar integració amb la infraestructura de correu electrònic per notificar-ho al personal de seguretat en cas d'alertes.
- La solució ha de suportar integració amb productes SIEM comuns.
- La solució ha de suportar informes estandarditzats i personalitzables.

4. DURADA DEL CONTRACTE I ABAST DEL SERVEI

L'àmbit del contracte inclou l'entitat Laboratori de Referència de Catalunya S.A.

La durada del contracte serà de **tres (3) anys**. Aquest contracte **no** es podrà prorrogar.

La data prevista d'inici del llicenciament és a venciment de l'actual contracte **13 de maig del 2025**.

5. PRESSUPOST

L'import de licitació màxim per als **tres (3) anys** és de **106.365,00 €** sense IVA. Aquest s'ha calculat en base al número de llicències requerides per als anys 1, 2 i 3. Les empreses interessades han d'oferir proposta d'acord al parc de llicències indicades a continuació:

Tipus de llicència	Preu Licitació unitari/any	Nº llicències requerides	Import (sense IVA)
Cynet 360 AutoXDR **All in One** **(per EndPoints y Servers)**	**115,00 €**	301	34.615,00 €
Cynet 360 Mobile **Paquet Mobile** **(Per iOS y Android)**	**42,00 €**	20	840,00 €

	Any 1 - 2 - 3 Import (sense IVA)
Any 1	35.455,00 €
Any 2	35.455,00 €
Any 3	35.455,00 €
Totals Any 1 + Any 2 + Any 3	**106.365,00 €**

El codi CPV del present lot, és el 48920000-3 Paquets de software ofimàtic.

6. FACTURACIÓ DEL SERVEI

La facturació del servei serà anual en base a les llicències previstes.

El pagament al contractista s'efectuarà contra presentació de factura expedida, d'acord amb la normativa vigent sobre factura electrònica, en els terminis i les condicions establertes en l'article 198 de la LCSP.

D'acord amb el que estableix la Llei 25/2013, de 27 de desembre, d'impuls de la factura electrònica i creació del registre comptable de factures en el sector públic, les factures s'han de signar amb signatura avançada, basada en un certificat reconegut, i han d'incloure, necessàriament, el número d'expedient de contractació.

El format de la factura electrònica i signatura s'han d'ajustar al que disposa l'Ordre ECO/306/2015, de 23 de setembre, per la qual es regula el procediment de tramitació i anotació de les factures en el Registre comptable de factures en l'àmbit de l'administració de la Generalitat de Catalunya i el sector públic que en depèn.

Així, el contractista haurà de lliurar les seves factures al servei eFACT del Consorci d'Administració Oberta de Catalunya (AOC), en la seva condició de Punt General d'Entrada de Factures Electròniques la Generalitat de Catalunya i del seu Sector Públic. Per major informació podeu consultar aquest enllaç:

https://economia.gencat.cat/ca/ambits-actuacio/factura-electronica/

Les factures han de ser electròniques i s'han de penjar en format XML mitjançant el següent enllaç a la "bústia d'entrega" del sector públic que ens correspon: https://efact.eacat.cat/bustia/?emisorId=7

Les factures hauran de vincular-se únicament amb una comanda, i per tant, una factura no podrà agrupar més d'una comanda.

A la descripció del producte que consti a la factura, serà necessari que primer s'introdueixi el codi de producte seguidament del nom.

El codi DIR del Laboratori de Referència de Catalunya, SA (en endavant LRC) pels tres centres gestors (Oficina Comptable, Unitat Tramitadora i Òrgan Gestor) és el A09039354.

El/s pagament/s efectiu del subministrament i/o prestacions executades es realitzarà d'acord amb el contingut de la LCSP i únicament mitjançant transferència bancària, amb venciment 30 dies / data factura, el proper dia 15 del mes següent, i prèvia recepció de la factura al departament d'Economia i Finances de LRC, a través dels canals descrits anteriorment. LRC únicament abonarà a l'empresa adjudicatària els serveis efectivament prestats, sense que en cap cas LRC estigui obligat a esgotar el valor estimat del contracte/pressupost de licitació.

Durant la vigència del contracte no tindrà lloc cap increment de preu. Qualsevol modificació sobre l'IVA serà motiu de revisió, no podent-ne repercutir cap altre increment.

La facturació haurà d'emetre's amb arrodoniment a dos dígits, conforme a allò establert a l'article 11 de la Llei 46/1998, de 17 de desembre, sobre introducció de l'euro.

El seguiment de l'estat de les factures es podrà consultar al web del Departament de la Vicepresidència i d'Economia i Hisenda a l'apartat de Tresoreria i Pagaments (consulta de l'estat de factures i pagaments de documents), a partir de l'endemà del registre de la factura.

En cas de retard en el pagament, el contractista té dret a percebre, en els termes i les condicions legalment establerts, els interessos de demora i la indemnització corresponent pels costos de cobrament en els termes establerts en la Llei 3/2004, de 29 de desembre, per la qual s'estableixen mesures de lluita contra la morositat en les operacions comercials.

El contractista podrà transmetre els drets de cobrament en els termes i condicions establerts en l'article 200 de la LCSP. Per a l'eficàcia d'aquesta transmissió de drets front a l'LRC, caldrà que li hagi estat notificada fefaentment, això és, mitjançant documentació que permeti acreditar la celebració del contracte i la capacitat dels intervinents.

7. ALTRES CONDICIONS D'EXECUCIÓ

7.1. Prestacions del Contracte

L'adjudicatari subministrarà les llicències en modalitat de subscripció, assegurant la configuració òptima i l'actualització contínua de les aplicacions.

L'adjudicatari serà l'encarregat d'enregistrar aquestes subscripcions i fer arribar a LRC el codi de la subscripció de llicències.

L'empresa adjudicatària ha d'estar autoritzada per al subministrament a l'estat espanyol dels productes inclosos a l'oferta. Caldrà que el licitador així ho demostri mitjançant la corresponent acreditació/certificació pròpia del fabricant o bé el compromís d'obtenir-la en un termini màxim de 10 dies naturals a comptar des de la formalització del contracte.

Un cop adjudicat, l'adjudicatari no podrà canviar les característiques tècniques dels articles que li han estat adjudicats, a no ser que suposin una millora tècnica; en cap cas es podran modificar els seus preus unitaris. Qualsevol modificació de les característiques dels productes, a petició del contractista, haurà de ser prèviament autoritzada per LRC, però sense alterar-ne el preu unitari adjudicat i sense perjudici del règim de modificacions contractuals.

En cas què fos necessari contractar més llicències que les marcades en el present PLEC, per necessitat obligada per part del LRC, l'empresa adjudicatària mantindrà el preu ofert en el contracte.

7.2. Prova de Concepte

L'empresa adjudicatària realitzarà una prova de concepte de 14 dies, sense cost addicional, per validar que la solució s'ajusta a les especificacions del contracte. Es proporcionaran fins a 20 equips amb sistemes operatius diversos per avaluar-los. **Aquesta tasca s'ha de realitzar prèvia a la finalització de l'actual contracte.**

7.3. Instal·lació i Formació

La instal·lació estarà a càrrec de l'adjudicatari amb el suport del departament d'informàtica. La formació es durà a terme a mesura que avanci el desplegament de la solució per tal que el departament TIC sigui el més autosuficient possible.

7.4. Manteniment i Suport Tècnic

El manteniment inclourà actualitzacions, suport tècnic remot i accés a informació sobre noves versions. S'oferirà suport tècnic per resoldre qualsevol incidència durant el contracte.