PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS

PER A LA CONTRACTACIÓ DE

"Implantació i manteniment MDR"

Juliol 2025

INDEX

1. OBJECTE DEL PLEC

Aquest document constitueix el plec de prescripcions tècniques (PPT) que regeix el procediment de contractació i execució de la "**Implantació i manteniment MDR**", promogut per l'Ens d'Abastament d'Aigua Ter-Llobregat (ATL).

2. INTRODUCCIÓ

2.1. Antecedents ATL

L'Ens d'Abastament d'Aigua Ter-Llobregat (ATL d'ara en endavant) és una entitat de dret públic sotmesa a l'ordenament jurídic privat participada 100% per l'Administració de la Generalitat de Catalunya, d'acord DECRET LLEI 4/2018, de 17 de juliol, pel qual s'assumeix la gestió directa del servei d'abastament d'aigua a poblacions per mitjà de les instal·lacions de la xarxa d'abastament Ter-Llobregat de titularitat de la Generalitat i es crea l'Ens d'Abastament d'Aigua Ter-Llobregat.
El Decret llei estableix que ATL és una entitat de dret públic de la Generalitat de Catalunya amb personalitat jurídica pròpia, autonomia administrativa i financera, i plena capacitat d'obrar per al compliment de les seves funcions.

2.2. Objectiu i missió d'ATL

ATL té com a principal objectiu el subministrament d'aigua en alta a les comarques de l'Alt Penedès, l'Anoia, el Baix Llobregat, el Barcelonès, el Garraf, el Maresme, la Selva, el Vallès Oriental i el Vallès Occidental, el que representa uns 1.800 km2 i una població abastida del voltant de 5 milions d'habitants, així com també tota la indústria i els serveis que estan establerts en aquest territori.

Aquest objectiu s'ha d'assolir complint uns criteris de gestió estrictes que permetin:

- Optimitzar la disponibilitat d'aigua potable, així com la seva qualitat, en els punts de subministrament, gestionant equitativament les demandes en qualsevol circumstància.
- Minimitzar l'impacte negatiu de les operacions, incloent la utilització dels recursos, en el medi ambient, realitzant una gestió compromesa amb aquest.
- Aplicar correctament i optimitzar els recursos financers disponibles.
- Integrar en totes les operacions de l'empresa els recursos tecnològics que permetin aconseguir la més alta eficiència en el desenvolupament d'aquestes.

La xarxa de distribució que gestiona ATL té més de 1000 quilòmetres de canonades, més de 60 estacions de bombament. Per a produir l'aigua, ATL disposa de quatre infraestructures principals: quatre estacions de tractament d'aigua potable i dues plantes dessalinitzadores. Quant a capital humà, ATL compta amb una plantilla de més de 250 professionals.

Per complir amb la seva missió i objectius, ATL destaca la necessitat d'integrar a les seves operacions els mitjans tecnològics que permetin la més alta eficiència, donant un servei excel·lent, però alhora optimitzant els recursos financers disponibles.

Entre aquests mitjans, les tecnologies d'informació i comunicacions han esdevingut una eina clau a qualsevol empresa per complir els seus objectius amb excel·lència, contant amb la necessitat d'una evolució i adaptació continua d'aquestes aplicacions als nous canvis i evolucions de l'entitat. A més a més, aquestes tecnologies han experimentat recentment una evolució accelerada, amb la irrupció de solucions de digitalització.

En aquest sentit ATL necessita disposar d'un servei de manteniment per garantir el seu correcte funcionament. Conseqüentment, ATL publica aquest plec per a contractar la "**Implantació i manteniment MDR**".

3. ABAST DEL CONTRACTE

L'abast del contracte del servei contempla la implantació d'una solució XDR (Extended Detection & Response) gestionat a través d'un MDR (Managed Detection & Response) a ATL i el seu manteniment. Aquest contracte consisteix en el servei i subministrament, instal·lació, i suport a la configuració i manteniment de la solució MDR, complint amb els requeriments tècnics i condicions que garanteixin:

- L'adquisició del software, llicències i subscripcions necessàries i suport a la configuració dels mateixos per a la seva integració amb l'arquitectura d'ATL.
- Manteniment i suport associats a la solució adquirida, que asseguri els nivells de servei i seguretat en les millors condicions i la major qualitat.
- Un model de relació que permeti disposar d'unes eines de gestió i d'uns mecanismes de control i seguiment.

L'adjudicatari, a més, mitjançant el seu equip de professionals, serà responsable de les següents activitats:

- Resolució d'incidències i manteniment correctiu.
- Manteniment perfectiu i evolutiu.
- Garantia del manteniment realitzat.
- Gestió documental dels evolutius
- Administració de la plataforma i gestió de la configuració
- Suport al manteniment de la infraestructura i entorns tècnics dins de l'abast.

- Suport per resoldre dubtes i activitats de formació.
- Gestió i control de la qualitat.
- Disposar d'un servei integral de manteniment i suport 24x7x365.

L'aplicació informàtica en producció que està dins de l'**abast del contracte** és:

- XDR/MDR
- Servei MDR

A l'apartat "Requisits del servei", es descriu amb més detall les activitats i condicions del servei que haurà de prestar l'adjudicatari.

4. SITUACIÓ ACTUAL

ATL té implantada en producció la solució de seguretat de endpoint Kaspersky EDR Optimum. L'aplicació està allotjada a instal·lacions d'ATL, administrada i gestionada per personal propi i col·laboradors externs.

La plataforma actualment implantada a ATL, consta dels següents elements:

- 1000 llicències per a Endpoints i Servidors

ATL es troba en fase de renovació de la solució de seguretat indicada anteriorment.

En base als anàlisis realitzats per l'equip intern es determina que es requereixen els següents elements per assolir aquest propòsit:

- Adquirir la solució i serveis detallats en el **punt 5.1 d'aquest document**

L'entorn de treball de Desenvolupament serà responsabilitat de l'empresa adjudicatària, que haurà de posar a disposició aquest entorn pels desenvolupaments que faci per ATL.

Quant a la gestió de la demanda i necessitats del negoci, la Direcció de Sistemes d'Informació d'ATL es regeix en termes generals per la metodologia ITIL. Les peticions i seguiment de l'activitat es fa utilitzant una aplicació ITSM.

5. REQUISITS DEL SERVEI

En línies generals, el servei i subministrament que es vol contractar ha de complir amb l'objectiu del contracte que s'ha marcat a l'apartat Objecte del Plec.

El servei i subministrament que desitja contractar ATL inclou dos blocs de col·laboracions diferenciats, tot i que mantenen una interrelació molt estreta. Aquests són:

1. Adquisició, instal·lació i configuració de la nova solució MDR/MDR segons les directrius del equip intern d'ATL
2. Serveis de manteniment 24x7x365 i explotació d'aquests elements conjuntament amb l'equip intern d'ATL de la plataforma MDR

5.1. Adquisició, instal·lació i configuració de la nova solució MDR/MDR

Aquest contracte preveu el servei i subministrament de la solució de seguretat que permeti:

- Plataforma de seguretat de l'end-point (PCs, portàtils, servidors, dispositius mòbils…) amb funcionalitats avançades de detecció de amenaces i resposta.
- Servei de protecció completa d'equips (els llocs de treball d'usuaris, servidors i dispositius mòbils), controlant el comportament de cadascun dels processos executats al parc informàtic, a més de proveir els mitjans de detecció i desinfecció de codi maliciós (malware). Aquest servei permetrà la classificació de tot el programari que s'executa al lloc de treball, monitoritzarà el seu comportament, assegurarà la identificació del programari fiable i no fiable i bloquejarà l'execució del programari no fiable. S'ha d'incloure també un servei de gestió i manteniment d'equips que permeti el control de l'estat dels equips així com poder aplicar polítiques i instal·lar-hi remotament. Servei de monitoratge avançat de ciberseguretat per la detecció i resposta vers amenaces, amb possibilitats de comptar tant amb control local per part de l'ENS, com servei completament extern.
- S'ha d'incloure el desplegament complert de tota la plataforma amb la substitució de la tecnologia actual.

Funcionalitats requerides:

1. **Plataforma**

   Per tal de reduir els costos de manteniment i explotació de la solució es requereix una solució basada en cloud. És imprescindible que la plataforma on s'allotgi la infraestructura es trobi fora de les nostres instal·lacions i operada pel fabricant de la solució en un model cloud, en què no hi hagi un inconvenient en el creixement i escalabilitat de la

plataforma. Assegurant que independentment del nombre de nodes de la instal·lació la plataforma funcioni al mateix nivell d'eficiència. La ubicació de la plataforma ha d'estar allotjada a la Unió Europea. Hi ha nodes que estan distribuïts per diferents seus i fins i tot en mobilitat per la qual cosa aquests aprofitaran la disponibilitat de la infraestructura cloud perquè estiguin integrats de forma completa a la configuració i actualització de la solució. La plataforma de gestió ha de cobrir els principals nivells de certificació com ara: ISO 27001 i es valorarà positivament qualsevol altra certificació que disposi la infraestructura.

2. **Agents**

La solució ha de poder desplegar-se de manera silenciosa mitjançant els mecanismes següents: per adreça IP, rang d'adreces IP, nom de màquina i grups de Directori Actiu de Microsoft basat en polítiques de domini.

Es requereix suport de diferents sistemes operatius i versions:

- PCs des de Windows 7 fins a Windows 11

- Windows Server 2008 R2 fins a 2025

- Distribucions Linux com Debian 8 a 12, Ubuntu 14.04 LTS a 24.10, RedHat 6.0 a 9.5, CentOS 6.0 a 8.5, Rocky Linux 8.3 a 9.5, etc - MacOS 10.10 a 15

- Android 5.0 a 14

- iOS 13 a 17

3. **Protecció**

La solució sol·licitada ha de combinar protecció clàssica d'endpoint amb una solució de tipus EDR (Endpoint Detection and Response) en un sol agent, amb configuració unificada de totes les funcionalitats. No es permet l'ús de diferents components/fabricants. La solució haurà d'incloure les funcionalitats següents:

a) Protecció Antivirus Tradicional

• Antivirus per a arxius, correu i web. Permetre la detecció i la desinfecció de qualsevol tipus d'amenaça. Detectant malware per

comportament. El correu detectarà a POP3. Quant a la protecció web, es detectaran els intents d'accés a pàgines web que continguin elements maliciosos, i els bloquejaran.

• Firewall personal gestionat en local o de manera centralitzada des de la consola web. Ha de permetre:

O Bloquejar les connexions entrants i/o sortints de les aplicacions que desitgi

O Prevenció d'intrusions

O Crear regles de tallafocs per permetre/denegar el trànsit en sentit entrant/sortint de les màquines que vulgui per als protocols/ports que desitgi.

• Bloqueig de tots els dispositius o dispositius específics (unitats d'emmagatzematge extraïbles, dispositius de captura d'imatges, unitats de CD/DVD, mòdems USB, Bluetooth, etc.), impedint l'entrada de codi maliciós i fuites d'informació. Permet la definició de diferents accions per a cada tipus de dispositiu (bloqueig, accés, lectura/escriptura).

• Bloqueig d'accés a pàgines web no desitjades. Haurà de ser possible configurar aquesta protecció basada en categories, encara que també es podran afegir llistes blanques i negres de llocs i dominis permesos.

b) Endpoint Detection and Response Protecció vers les següents amenaces:

• Malware avançat

• PUP (Potential Unwanted Programs)

• Amenaces zeroday tipus ransomware

• Troians de nova generació indetectables pels antivirus

i suport de:

• Decoy files

• Shadow Copies

El sistema de protecció ha de ser capaç de classificar el 100% dels processos executats a les màquines, generant una classificació de malware o goodware. És un requisit que es bloquegi els processos desconeguts que intentin executar per evitar la possibilitat danyar les dades accessibles per la màquina (com pot ser el xifratge no desitjat) o el robatori o accés de dades. S'ha d'incloure un sistema Anti-Exploit que permet la detecció i bloqueig de l'ús d'exploits coneguts o desconeguts. S'han de poder establir diferents nivells de bloqueig (més o menys restrictius) així com diferents nivells en la capacitat dels usuaris de poder desbloquejar individualment els processos bloquejats pel sistema. La solució ha d'incloure la possibilitat de bloquejar aplicacions per nom i hash que l'administrador vulgui.

NOTA: degut a les limitacions i control que exerceixen Android i iOS no serà necessari que els agents per aquests dispositius suportin totes aquestes característiques.

c) Servei d'alerta d'amenaces (Threat Hunting)

Es requereix un servei que alerti i prengui les mesures correctives adequades quan es detecta una activitat anòmala als equips basada en el comportament normal auditat anteriorment al parc d'equips. Aquest servei haurà d'estar ofert per la tecnologia fent ús de les dades que s'hagin recollit a l'auditoria forense. Han de poder realitzar l'alerta i la inclusió a la intel·ligència del sistema EDR de les mesures correctives

4. Mòduls addicionals

Cal que la solució escollida disposi de mòduls addicionals per ampliar la seguretat de la infraestructura. Aquests mòduls han de complir com a mínim les funcionalitats següents:

• Gestió de nivell de xifratge dels dispositius (integració amb BitLocker per màquines Windows)

Requisits de la solució

La última versió de la solució ha d'estar certificada pel Centre Criptogràfic Nacional segons la guia "Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació" (CPSTIC), dins de la família de protecció del Lloc de

Treball com a QUALIFICAT, i té assolida com a minim la certificació de l'Esquema Nacional de Seguretat, categoria mitja.

Llicències de seguretat

- 1000 llicències que suportin els actius indicats anteriorment.

Tanmateix, es requereix per a tots els productes inclosos en aquest plec mencionats en el punt 5.1 d'aquest document, la garantia del suport per part del fabricant 24x7.

En línies generals, el servei que es vol contractar ha de complir amb l'objectiu del contracte que s'ha marcat a l'apartat Objecte del contracte. Els licitadors han de presentar la seva proposta, d'acord amb la seva experiència, capacitats i coneixements que d'una manera més òptima i amb menys riscos pugui donar compliment a aquest objectiu.

Els licitadors hauran de complir amb els següents requisits com a mínim:

- ✓ Partner en la solució proposada.

Justificació: S'ha d'acreditar el partnership de la solució proposada per garantir el correcte desplegament i manteniment de l'eina que s'instaurarà.

- ✓ Certificat oficial d'Esquema Nacional de Seguretat (ENS) nivell MIG o certificat equivalent emès per organismes establerts en qualsevol Estat membre de la Unió Europea i altres proves de mesures equivalents de garantia de la qualitat.

Es presentarà còpia del certificat vigent, en el cas que hagi caducat una vegada presentada la sol·licitud de participació s'ha d'acreditar mitjançant el certificat de l'empresa qualificadora haver sol·licitat la renovació de la certificació i assolit amb èxit l'auditoria corresponent amb anterioritat a la data de pèrdua de vigència.

L'Ens d'Abastament d'Aigua Ter-Llobregat disposa d'un Sistema Integrat de Gestió certificat basat en estàndards internacionals (ISO 9001, ISO 14001-EMAS, ISO 50001, ISO 45001, ISO 22000) el qual reconeix com una eina de gestió útil i eficaç per assolir els objectius de la seva organització en el marc de la millora contínua. ATL està compromesa a garantir l'aplicació dels corresponents sistemes de gestió en: la prestació del servei de subministrament d'aigua, la innocuïtat de l'aigua que distribueix, la seguretat, benestar, consulta i participació dels treballadors i treballadores, l'optimització dels recursos, la protecció del medi ambient, l'acció climàtica, l'eficiència energètica de les instal·lacions i la protecció de la informació i dels sistemes vinculats.

Justificació de l'exigència com a solvència de la certificació ENS nivell mig o certificat equivalent:
Que els licitadors disposin de certificat oficial del Esquema Nacional de Seguretat nivell mig o certificat equivalent, és garantia que el proveïdor compleix amb la normativa nacional de seguretat en la gestió dels seus processos i serveis. Certifica que tenen sistemes de gestió de seguretat establerts i documentats, per la qual cosa es redueix el risc d'incompliment de les especificacions documentades en la licitació en termes de seguretat del productes i dels serveis oferts. Tanmateix, la certificació en si implica un procés d'auditoria interna i externa que verifica el compliment dels requisits de la norma, la qual cosa al seu torn proporciona un nivell addicional de transparència en la gestió de qualitat dels proveïdors d'ATL.

5.2. Servei de manteniment i explotació post posada en marxa

L'adjudicatari mitjançant el seu equip de professionals, serà responsable del manteniment dels equips i donar suport atenent a les peticions que ATL els hi requereixi. En concret, serà responsable de les següents activitats:

Gestió de la solució

L'adjudicatari proporcionarà una interfície on es puguin consultar dades en temps real, descarregar informes/alertes, accedir a la configuració i polítiques i disposar de les actualitzacions dels agents. Els administradors del servei podran gestionar des d'una única consola i de manera centralitzada, mitjançant qualsevol navegador web, la seguretat i la productivitat de totes les estacions de treball i servidors, fins i tot ordinadors portàtils i oficines remotes. Es valorarà molt un entorn amigable i fàcil de seguir sense exigir grans coneixements d'amenaces avançades. A més, ha d'incloure informes d'estat de les proteccions, de les deteccions de malware, així com informes executius amb el resum de la informació global. Els informes s'han de poder obtenir de forma immediata amb les dades en temps real i també de forma periòdica per correu electrònic i en diferents formats per al tractament posterior. El sistema ha de generar informació forense relacionada amb cada equip de manera que pugui ser explotada posteriorment. El sistema haurà d'incloure informe per amenaça detectada en què es correlacioni les accions que ha fet el procés o en el context que ha estat embolicat, per exemple, si ha estat descarregat d'Internet o ha estat extret d'un fitxer comprimit.

Servei de Resposta i Remediació vers amenaces

S'han d'oferir 2 sistemes de resposta i remediació complementaris.

a) El primer ha de ser un nivell que permeti un control i gestió totalment local per part del Departament de Ciberseguretat d'ATL o de la empresa que ho gestioni; amb les següents funcionalitats bàsiques:

- El sistema ha de poder oferir resposta i remediació tant a nivell d'endpoint com a nivell de tallafocs.
- Visibilitat i detecció a nivells de xarxa tant nord/sur com est/oest per a tots els dispositius connectats.
- Motor de detecció de riscos per aplicacions SaaS, com Microsoft 365.
- Sistema d'informes personalitzable.

b) Es valorarà també la conveniència de comptar amb un servei extern de detecció i resposta vers amenaces (Managed Detection and Response, MDR). Ha de complir els següents requisits:

- SOC amb tecnologia S.O.A.R.
- Centre d'operacions de seguretat (SOC) operat per analistes 24x7x365.
- Servei de gestió d'amenaces.

- Capacitat per identificar amenaces de seguretat, tant conegudes com desconegudes, en:
  - Endpoints (PC's, portàtils, servidors, dispositius mòbils...)
  - Tallafocs Watchguard (Solució de seguretat perimetral implantada a ATL)
  - servei Microsoft 365
- Analistes del SOC amb capacitat per identificar processos maliciosos mitjançant consulta de hash o mapeig de TTPs.
- Més de 370 Indicadors d'Atac (IoA) per monitoritzar i investigar, amb nous IoA creats regularment.
- Monitoratge proactiu i anàlisi per identificar i prioritzar deteccions.

- Anàlisi manual de deteccions que presentin un alt nivell de severitat per confirmar-ne la naturalesa maliciosa i la necessitat de resposta.
- Notificacions sobre incidents de seguretat i informació relacionada.
- Recull, processament i ús de dades d'intel·ligència d'amenaces per millorar la solució i donar suport a la investigació i el desenvolupament.
- Cerca proactiva d'amenaces que puguin haver evadit els endpoints i servidors, utilitzant intel·ligència d'amenaces i IoCs.
- Capacitat de remediació en cas que la solució d'endpoint no hagi aturat l'amenaça.
- Capacitat per aïllar endpoints/servidors, quan calgui, per contenir o interrompre activitats malicioses.
- Opcions flexibles d'implementació que permeten configurar quins endpoints/servidors són crítics i quins no han de patir cap acció de mitigació.
- Provisió d'informes periòdics sobre l'estat de seguretat, els problemes identificats i les accions recomanades.
- Possibilitat de fer modificacions, actualitzacions o millores al servei amb el temps.

Suport tècnic 24x7x365

S'establirà el manteniment i l'assistència tècnica que permeti assegurar el funcionament correcte en tots els llocs i servidors de l'organització, mitjançant:

- Servei de suport ofert pel fabricant per telèfon en castellà
- Service Packs i hotfixes: Accés a les millores tècniques del producte durant el temps d'activació del servei
- Web de suport: Accés a fòrums, blogs, informació sobre darreres amenaces, enciclopèdia de virus, …
- Suport tècnic via email 24x7x365, per tècnics certificats a la solució implementada
- Accés a anàlisi en línia de virus ocults
- Accés il·limitat al Helpdesk: sense límit d'incidències

5.3. Productes a lliurar

En aquest apartat, s'enumeren els productes/serveis i documents que, com a mínim, ha de lliurar l'adjudicatari durant el projecte. Tot i així, l'adjudicatari pot proposar altres lliurables addicionals que puguin aportar valor al projecte.

Productes / serveis

- Solució instal·lada, servei configurat i monitoritzat.
- Integració totalment operativa amb els entorns d'ATL.
- Ampliació i llicenciament dels entorns actuals de monitorització i gestió completats

Documentació

- Pla de projecte
- Informes mensuals seguiment
- Actes: kick off, seguiment del servei i tancament.
- Manual administració, esquema d'arquitectura, configuració, instruccions operatives, etc.
- Manual del Model de gestió dels serveis (indicadors, processos, etc)
- Material de formació

5.4. Durada del servei, volum d'hores i planificació

La durada d'aquest contracte és de dotze (12) mesos a comptar des de l'acta d´inici. Tenint en compte que els primers 2 mesos corresponen a l'adquisició i desplegament de la solució i els 10 posteriors corresponen a l'explotació i manteniment del servei gestionat.

Quant a durada i terminis, diferenciarem 2 etapes principals de la col·laboració. El licitador haurà de proposar una assignació i dedicació de professionals que encaixi amb aquestes fases.

Les dues fases identificades són les següents:

1. Adquisició, configuració i instal·lació de la solució EDR amb una durada de 2 mesos màxim (inclou període d'aprovisionament).

2. Manteniment servei amb una durada de 10 mesos posteriors a la primera fase indicada anteriorment.

Per a major precisió indicar que la segona fase pot iniciar-se abans dels 2 mesos contemplats en la primera etapa, sempre i quan s'hagin donat per finalitzats els treballs de la primera etapa.

L'adjudicatari haurà de garantir un horari de cobertura d'atenció de 24X7x365 per les incidències crítiques segons especificacions de l'apartat 5.7 Acords de nivell de servei.

5.5. Calendari i lloc de treball

En relació als treballs a realitzar amb coordinació amb professionals d' ATL, aquest s'adaptarà al calendari laboral i horari d'oficina del serveis centrals (de 8:00 a 17:00 de dilluns a divendres), i al calendari laboral de la ciutat de Barcelona.

Atesa la particular naturalesa dels serveis, determinades activitats hauran de ser realitzades a les instal·lacions d'ATL (incidents que ho requereixin, assistència a reunions, configuracions, formació, etc.). El servei es durà a terme de forma presencial sempre que ATL ho requereixi. No obstant, en la mesura que sigui possible, es facilitarà que activitats es facin de forma remota.

ATL portarà a terme la supervisió dels treballs que realitzi l´adjudicatari i podrà en qualsevol moment exigir l'orientació en la prestació, que consideri més adient als seus interessos.

5.6. Equip de treball

L´adjudicatari haurà de destinar per l'execució del servei els professionals adequats amb coneixements i experiència en plataformes de seguretat EDR/MDR.

L'empresa licitadora per garantir el coneixement en la tecnologia objecte del contracte cal que disposi de l'habilitació empresarial mitjançant l'acreditació de la tecnologia proposada.

Igualment, el licitador designarà un responsable del contracte (gestor del servei) que es mantindrà durant el projecte. En cas de substitució de qualsevol membre de l'equip de treball, ATL haurà de donar la seva conformitat als candidats proposats amb els mateixos requisits.

Tanmateix, ATL es reserva el dret de sol·licitar canviar les persones assignades si al llarg del contracte es donen situacions justificades per al seu canvi.

L'equip de treball proposat pel licitador haurà d'identificar com a mínim 2 perfils (1 Gestor i 1 Tècnic), que són:

Gestor del servei:

Les responsabilitats del Gestor del servei seran:

- Organitzar l'execució del servei i posar en pràctica les indicacions del responsable del contracte que designarà la part contractant.
- Representar a l'equip de treball com a interlocutor en les seves relacions amb la part contractant.
- Sotmetre al responsable del contracte d'ATL el programa de treball i altres propostes que es determinen en el present plec per a la seva aprovació.
- Suport a la presa de decisions relatives als diferents àmbits dels serveis.
- Proposar al responsable del contracte d'ATL les modificacions que consideri convenients per a millorar els resultats dels treballs.
- El seguiment del projecte i de la planificació dels treballs inclosos en el servei.

Es requereix:

- Una experiència mínima de 10 anys en gestió d'entorns de seguretat, dels quals 5 anys d'experiència en serveis i/o projectes relacionats amb la solució proposada.
- Certificació del fabricant proposat

Tècnic XDR/MDR

Les responsabilitats del tècnic, inclouen, entre d'altres:

- Anàlisi dels requeriments i necessitats que es plantegin en el contracte.

- Definició de les solucions, d'acord als requisits tècnics del servei.
- Desenvolupament, test i desplegament dels treballs inclosos en el servei.
- Suport tècnic i funcional a les diferents tasques i lliurables durant el servei, seguint la metodologia de cicle de desenvolupament requerida.

Es requereix:

- Una experiència mínima de 5 anys d'experiència en serveis i/o projectes relacionats amb plataformes EDR.
- Certificació de la tecnologia proposada.

5.7. Organització i model de relació

ATL requerirà que s'estableixi un model d'Organització del Servei l´adjudicatari a diferents nivells per tal d'assegurar el correcte seguiment dels treballs objecte del contracte. L´adjudicatari a l'inici del servei haurà de descriure l'organització del seu equip de professionals involucrats al contracte, descrivint rols, funcions i la interrelació amb ATL, segons apartat 5.6 del plec.

El model de relació inclou reunions periòdiques mensuals entre els responsables del contracte per seguiment de la planificació i de l'avanç dels treballs.

En qualsevol cas, s'organitzaran tantes sessions de treball, o les reunions que siguin necessàries per assegurar la correcta coordinació i correcta consecució dels objectius del servei.

L'adjudicatari informarà al personal tècnic informàtic propi de ATL de les possibles incidències en el servei previstes i no previstes i dels canvis que potencialment afectin els sistemes de ATL. Així mateix s'haurà de coordinar sempre amb el mencionat personal tècnic per agendar qualsevol intervenció relacionada amb la prestació del servei.

5.8. Acords de Nivell de Servei (ANS)

El desenvolupament d'aquest servei estarà sotmès a l´acompliment d'acords de nivell de servei (ANS), que garanteixin un compromís de l'adjudicatari amb el projecte.

Els ANS hauran de considerat els conceptes habituals que es tenen en compte per valorar la qualitat del servei en el desenvolupament d'aquest servei, com són:

- Agilitat en el servei, quant a temps de resolució d'incidències per crítiques i prioritat alta.
- Fiabilitat i gestió d'expectatives, quant a acompliment de dates previstes per a evolutius i la implantació de solucions.
- Qualitat dels treballs, quant a que la solució no tingui incidències importants i no se'n generin de noves.

De forma orientativa (no limitativa) indicar que el volum d'incidents crítics els darrers 5 anys ha estat inferior a 3.

El ANS que seran d'aplicació són els següents:

	Acords de nivell de servei	Acords de nivell de servei (ANS): descripció	Compromís
ANS 1	Temps màxim de resposta a la comunicació d'incidències	Temps màxim de resposta conforme s'ha creat la incidència i s'ha donat el corresponent acús de rebuda.	< 1h
ANS 2	Temps d'inici de resolució incidències critiques	Temps des de la comunicació de la sol·licitud d'incidència, fins que l'equip de suport es trobi en disposició de resoldre-la.	< 4h
ANS 3	Temps d'inici de resolució incidències no critiques	Temps des de la comunicació de la sol·licitud d'incidència, fins que l'equip de suport es trobi en disposició de resoldre-la.	NBD
ANS 4	Temps màxim de resolució d'incidències critiques	Temps màxim de resolució, per a corregir i implementar una solució correctament. Serà el temps que trigui l'adjudicatari a donar i implementar una solució davant una incidència informada per ATL. Es contarà el temps des de que es dona l'avis i que la incidència està resolta o, cas que sigui complexa, es doni una solució pal·liativa provisional.	< 24h
ANS 5	Temps màxim solució d'incidències no critiques	Temps màxim de resolució, per a corregir i implementar una solució correctament. Serà el temps que trigui l'adjudicatari a donar i implementar una solució davant una incidència informada per ATL. Es contarà el temps des de que es dona l'avís i que la incidència està resolta o, cas que sigui complexa, es doni una solució pal·liativa provisional.	< 72h

Nivells de priorització

Els nivells de servei i acords de priorització, sempre vindran condicionada per la criticitat de les incidències i sol·licituds rebudes. En termes generals, s'estableixen dos conceptes per valorar la criticitat de les actuacions: Nivell d'impacte i Urgència de resolució.

Nivell d'impacte	Descripció
Alt	La falta de correcció de la incidència o de realització de la petició pot afectar negativament i de manera significativa a objectius de negoci
Mig	Es fa necessària la realització de la petició per garantitzar que objectius de negoci assoleixin els valors fitxats

Baix	La realització de la petició pot millorar d'alguna manera la gestió del negoci

Nivell d'urgència	**Descripció**
Molt Urgent	Sistema aturat. Afecta de manera generalitzada a molts usuaris i no existeix cap via alternativa de cobrir les necessitats.
Urgent	Incidències que impedeixen el funcionament correcte de l'aplicació a alguns usuaris i pot haver alguna via alternativa temporal.
Normal	Incidències que provoquen una degradació del funcionaments de la aplicació que impedeix a alguns usuaris treballar amb la productivitat habitual. Tenen una relativa afectació en el funcionament diari. o requisits/peticions que no es consideren crítiques per a l'organització
Baixa	Es tracta de millores de la aplicació, ja siguin tècniques o funcionals. Fins el dia de la petició es venia funcionant habitualment sense.

La combinació d'ambdós nivells estableix la matriu de prioritats a l'hora de resoldre les peticions i incidències registrades.

Matriu de prioritats		**Nivell d'urgència**			
		Molt urgent	**Urgent**	**Normal**	**Baixa**
Nivell d'impacte	**Alt**	Crítica	Alta	Alta	Necessària
	Mig	Crítica	Alta	Necessària	Necessària
	Baix	Alta	Necessària	Necessària	Recomanable

Acompliment dels ANS i aplicació de penalitzacions:

Mensualment es presentarà un informe d'activitats i nivell de servei on es recolliran totes les incidències i sol·licituds realitzades així com els indicadors de compliment en la seva resolució. S'estableix dues taules de valoració:

- CAS A - incidències/sol·licitud qualificades com a crítiques*
- CAS B - incidències/sol·licitud qualificades com no critiques*

* La matriu de prioritats es la que estableix la qualificació de cadascuna de les incidències/sol·licituds.

Es comptabilitzarà el nombre total d'incompliments dels ANS, sumant el total de tots quatre acords. Amb aquest nombre total d'incompliments, ATL podrà aplicar una penalització en % sobre la facturació d'aquell mes d'acord amb les següents taules:

CAS A:

Total incompliments CRÍTICS del mes	**Penalització aplicada sobre l'import de facturació del mes**
1 incompliment	3%
2 incompliments	6%
3 incompliments	10 %

En cas de superar el nombre de 3 incompliments serà motiu suficient per poder finalitzar el contracte de forma unilateral per part d'ATL

CAS B:

Total incompliments NO CRÍTICS del mes	**Penalització aplicada sobre l'import de facturació del mes**
2 o menys incompliments	Sense penalització
3 incompliments	3%
4 incompliments	4%
5 incompliments	5%

6 o més incompliments	6%

6. ALTRES REQUISITS I CONDICIONS

6.1. Especificacions de RGPD i seguretat

Els desenvolupaments realitzats i lliurats hauran de complir amb el Reglament (UE) 2016/679, General de Protecció de Dades ("RGPD"). L'adjudicatari haurà d'identificar tots aquells punts que puguin vulnerar el RGPD, resoldre'ls i presentar les evidències conforme compleixen amb el mateix.
D'altra banda, els sistemes a desenvolupar han d'estar exempts de vulnerabilitats, segons apliqui el Top 10 de OWASP Security Mobile i/o OWASP Top Security Web (https://www.owasp.org). A més haurà de complir la normativa de gestió d'usuaris i contrasenyes segons els criteris de seguretat reconeguts a les normatives més habituals.

En qualsevol cas, els desenvolupaments objecte d'aquest plec podran ser analitzats a través d'una auditoria tècnica de seguretat i anàlisi de codi. L'objectiu d'aquesta anàlisi és realitzar un diagnòstic de la seguretat amb la finalitat de detectar fallades de seguretat, possibles vectors d'atac, errors de programació, prevenir incidents de seguretat i millorar el nivell de seguretat dels sistemes d'informació. Aquesta auditoria es realitzarà sota els estàndards que marca OWASP.
Les evidències i vulnerabilitats que resultin de la realització d'aquesta auditoria, hauran de ser esmenades pel adjudicatari, assumint el mateix els costos dins de l'import de l'adjudicació del contracte que fa referència al present plec de prescripcions tècniques.

6.2. Propietat intel·lectual i propietat de les dades

En el cas que l'objecte del contracte comporti realitzar obres o creacions subjectes a la normativa de propietat intel·lectual, l'adjudicatari cedirà a ATL gratuïtament i amb caràcter d'exclusiva, sense límit de temps i per a tot l'àmbit territorial universal, els drets d'explotació de la propietat intel·lectual de les obres realitzades per a la prestació de l'objecte contractual, en qualsevol forma i, en especial, en totes les seves modalitats d'explotació, inclosa l'explotació en xarxa d'Internet, del dret de reproducció, distribució, comunicació pública i transformació (actualització, traducció i qualsevol altra modificació que pugui derivar en una altra obra).
La cessió en exclusiva en els termes que estableix el paràgraf precedent s'efectua també als efectes que l'ATL, com a cessionària en exclusiva dels drets d'explotació dels drets d'autor de les creacions realitzades per a la prestació de l'objecte contractual (dibuixos, logotips, textos, eslògans, gràfics, etc.), pugui enregistrar-los, si s'escau, com a titular dels drets de la propietat industrial derivats de totes aquestes creacions (marca o nom comercial).

La cessió de drets prevista en aquesta clàusula s'aplicarà també en el cas d'elements creats o produïts (fotografies digitals, etc.) per persones o empreses que hagin estat subcontractades pel adjudicatari, i a aquest efecte, l'adjudicatari haurà d'acreditar la cessió esmentada. Aquests drets es cediran a l'ATL també en exclusiva, sense límit de temps i per l'àmbit territorial universal en totes les seves modalitats d'explotació, inclosa la xarxa d'Internet: el dret de reproducció, distribució o comunicació pública.
A més, l'adjudicatari assumeix també l'obligació de respondre i indemnitzar contra tota responsabilitat de qualsevol naturalesa (incloses les quantitats reclamades per les societats de gestió col·lectiva de drets de propietat intel·lectual) originada o relacionada amb reclamacions que l'ATL pugui rebre sobre el fet que l'explotació dels treballs, peces, icones, materials i en general qualsevol creació produïda per a l'objecte d'aquesta contractació, infringeixin drets de propietat intel·lectual i/o industrial de tercers.
Així mateix, la propietat dels materials es cedirà pel adjudicatari a l'ATL i ningú podrà fer-ne ús sense l'autorització d'aquest.
La signatura del corresponent contracte suposarà la formalització de les cessions previstes en aquesta clàusula.
Tanmateix, les dades que es generin durant l'explotació de les aplicacions implicades a aquest servei seran propietat d'ATL i en qualsevol moment. Aquestes dades no podran ser cedides ni mostrades a tercers sense autorització expressa d'ATL.

6.3. Confidencialitat

Les dades a les quals s'hagi tingut accés durant la realització dels treballs, seran considerades, a tots els efectes, de caràcter confidencial, essent d'aplicació el que la llei ha establert per l'ús d'aquest tipus d'informació, i hauran de lliurar-se en la seva integritat a ATL, o bé certificar la seva total destrucció.
Les dues parts s'obliguen a tractar de manera confidencial i a no divulgar a tercers les dades, la documentació i la informació de l'altre part. Els deures de secret i no difusió subsistiran fins i tot quan hagin finalitzat les relacions contractuals mútues.
L'adjudicatari es compromet a guardar el més absolut secret sobre tota la informació a la qual tingui accés en compliment d'aquest contracte, especialment la de caràcter personal, i a subministrar-la només a personal autoritzat per ATL. Aquest compromís afecta tant a les dades que estan en documents en paper, com en qualsevol altre tipus de suport, així com aquelles que s'obtinguin per mitjans telemàtics. En cap cas es podrà copiar, utilitzar amb una finalitat diferent a la que figura en aquest plec o cedir a tercers, ni tan sols per a la seva conservació, les dades o els arxius.
De la mateixa manera, i en el que respecta a la informació que cadascuna de les parts rebi de l'altre com "informació confidencial", les dues parts es comprometen mútuament a retornar-la, esborrar-la o destruir-la, de la manera que indiqui l'altre part per escrit i sigui quin sigui el mitja en el que esta enregistrat.
L'adjudicatari es comprometrà a la no difusió de cap tipus de codi d'accés o qualsevol altre tipus d'informació que pugui facilitar l'entrada als sistemes d'ATL, així com a no fer un ús incorrecte dels permisos i privilegis que es concedeixin al seu personal per a l'execució d'aquest contracte.

L'adjudicatari es farà responsable dels perjudicis que se li puguin ocasionar a ATL degut a l'incompliment de qualsevol de les condicions esmentades.

6.4. Relació amb proveïdors

ATL té implantat un sistema integrat de gestió en el qual part dels serveis/compres són avaluats sobre la base de l'acompliment energètic, mediambiental i de la qualitat, seguretat i innocuïtat de l'aigua.

6.5. Seguretat i salut

L'adjudicatari haurà de complir amb els requeriments que es deriven de la Llei 31/1995, de 8 de novembre de prevenció de riscos laborals i del Reial Decret 171/2004 de 30 de gener pel que es desenvolupa l'article 24 de la Llei 31/1995 en matèria de coordinació d'activitats empresarials.

L'adjudicatari haurà d'aportar tota la documentació sol·licitada per ATL en matèria de PRL mitjançant la plataforma SmartOSH de gestió de la prevenció.

En el desenvolupament dels seus treballs compliran inexcusablement la normativa vigent sobre prevenció de riscos laborals, així com les instruccions, normes i/o procediments que siguin d'obligat compliment a l'empresa.

Si es disposa de personal que realitza treballs a les instal·lacions d'ATL i presenta símptomes que afectin al sistema respiratori com grip, refredat, bronquiolitis i/o Covid-19 caldrà posar-se una mascareta quirúrgica cobrint completament el nas i la boca durant tota la jornada laboral, evitar la interacció amb altres persones i consultar amb el servei públic de salut, si s'escau..

7. PRESSUPOST DE LICITACIÓ

Totes les mencions d'aquest Plec a quanties, imports, valors, pressupostos o equivalents s'entendran referides sense IVA, llevat que es disposi altrament.
L'adjudicatari mensualment certificarà els treballs realitzats, que serà el que s'utilitzarà per a la valoració i facturació dels treballs mensuals.

El pressupost de licitació del contracte serà de 174.808,7 € IVA inclòs (144.470 € IVA exclòs). Aquest import considera la durada de 12 mesos de contracte, contemplant tots els objectius i abast descrit a aquest plec.
Respecte el pressupost del contracte, que distribuït segons la següent distribució pressupostària:

Concepte	**2026 (sense IVA)**	**Iva (21%)**	**Total amb IVA**
Llicències, subscripcions i garanties	101.970€	21.413,7 €	123.383,7 €
Serveis gestionats (12 mesos incloent posta en marxa i servei 24x7)	42.500 €	8.925 €	51.425,00 €
TOTAL	**144.470,00 €**	**30.338,7 €**	**174.808,7 €**

Serveis gestionats (posta en marxa i servei 24x7) 42.500 € / 500 hores = 85 € / hora

Justificació del pressupost: Cost material estimat a partir de consultes a fabricants d'aquest tipus de solucions. Cost serveis estimat a partir del preu hora mig del sector segons perfil i la valoració d'esforços.

No s'admetran revisions de preu.

8. FACTURACIÓ

La facturació del servei es realitzarà de manera mensual a mes vençut, en base a la certificació dels treball realitzats reportats a l'informe mensual de seguiment. En qualsevol cas, la facturació de la fita final d'un treball NO es podrà fer abans de la seva posta en marxa i la seva aprovació per ATL.

Les factures hauran de ser emeses en format electrònic, de conformitat amb el que disposa la Llei 25/2013 i ha d'incloure, entre d'altres, el codi del contracte.

9. PROPOSTA TÈCNICA (Judicis de Valor)

La **proposta tècnica** ha de tenir els següents continguts mínims i ha d'estar obligatòriament estructurada de la forma que es detalla a continuació. El licitador pot adjuntar a la seva oferta tota la informació complementària que consideri d'interès.

1. PLA DE PROJECTE

Projecte de desplegament i posada en marxa (CJV1)

Justificació del criteri:

Aquest criteri permet valorar la capacitat organitzativa, tècnica i preventiva de les empreses licitadores en el desplegament de la solució. Atès que l'objecte del contracte implica una renovació d'elements crítics per a la seguretat de la xarxa corporativa (firewalls), és fonamental garantir una execució planificada, segura i amb el mínim impacte en l'operativa habitual.

Forma de valoració:

Les empreses hauran de presentar una **memòria tècnica** que inclogui com a mínim:

- **Planificació detallada del projecte**, amb calendari estimat de lliurament, fases, responsables, punts de control i recursos implicats.
- **Configuració inicial de la solució**, tenint en compte adaptació a l'entorn actual, polítiques de seguretat, integració amb altres sistemes.
- **Pla de proves i validació**, detallant les proves previstes abans de la posada en marxa i els criteris d'acceptació.
- **Anàlisi de riscos** i proposta de mesures correctores per minimitzar impactes.
- **Relació detallada dels lliurables** del projecte.

La valoració es farà en base a:

- Grau de concreció i claredat del pla.
- Viabilitat i coherència de les fases proposades.
- Anticipació de riscos i mesures preventives.
- Valor afegit aportat (millores logístiques, rapidesa d'execució, flexibilitat, etc.).

2. PLA DE MANTENIMENT (SERVEI GESTIONAT)

Servei de suport i manteniment (CJV2)

Justificació del criteri:

Donada la naturalesa crítica del servei contractat, la qualitat del manteniment i el suport continu són essencials per garantir la seguretat perimetral i la disponibilitat del sistema. Per això, s'estableix aquest criteri per valorar propostes que superin els mínims exigits, aportant un pla de treball sòlid, indicadors clars de seguiment i un equip tècnic altament qualificat.

Forma de valoració:

Les empreses presentaran un **pla de servei gestionat** que inclogui:

- **Detall de les operacions periòdiques de manteniment preventiu i correctiu**, especificant freqüències, mètodes i eines utilitzades.
- **Indicadors de qualitat del servei (KPI's)**, com temps de resposta, temps de resolució, disponibilitat del servei, etc.
- **Relació d'informes de seguiment**, amb continguts mínims, freqüència i responsables de lliurament.
- **Equip tècnic assignat**, indicant perfils professionals adicionals i dedicació estimada al servei.

Es valorarà positivament:

- La presència de **més d'un tècnic** assignat al servei. Només indicant el número de tècnics que s'assignaran a l'execució del contracte.
- La proposta d'eines de monitoratge proactiu o d'atenció via portal client/ticketing.

La valoració es farà sobre la base de:

- Adequació i qualitat del pla de manteniment.
- Grau de detall i realisme dels KPI's i informes.
- Capacitat tècnica i estructura de l'equip proposat.

3. PLA DE FORMACIÓ

Pla de formació (CJV3)

Justificació del criteri:

El correcte aprofitament de la nova infraestructura de seguretat depèn en gran mesura del coneixement i autonomia del personal tècnic intern. Per això, es valora la qualitat del pla de formació proposat, com a eina clau per garantir la transferència de coneixement i la gestió eficient de la nova plataforma.

Forma de valoració:

Les licitadores presentaran un **pla de formació** que haurà d'incloure:

- **Metodologia formativa**, amb descripció del format (presencial, online, pràctic, etc.) i enfocament didàctic.
    - Es valorarà especialment que la formació sigui **pràctica i aplicada** sobre la pròpia plataforma implementada.
- **Temari proposat**, estructurat en mòduls, amb claredat de continguts, nivell tècnic i adaptació als rols del personal destinatari.
- **Durada estimada en hores de formació.**
- **Documentació complementària**: manuals, guies ràpides, vídeos o altres recursos que facilitin l'aprenentatge posterior.

La valoració es farà tenint en compte:

- La claredat i adaptació del temari proposat.
- El valor pràctic i aplicabilitat immediata de la formació.
- L'adequació del nombre d'hores a la complexitat de la solució.
- L'existència de materials útils i reutilitzables.

Sant Joan Despí, a data signatura digital.

UNITAT SOL·LICITANT	RESPONSABLE JERÀRQUIC
Responsable de Seguretat de la Informació	Director de Sistemes d'informació

ANNEX I - MODEL DE PROPOSICIÓ ECONÒMICA

Concepte	Concepte desglosat	Element	Units	Preu unit.	Total (sense IVA)
Subscripcions i garanties	Subscripcions, suport i garantia	Llicència EDR	1000	46,17 €/unitat	46.170,00 €
		Llicència MDR	1000	55,8 €/unitat	55.800,00 €
	Total subscripcions i garanties				101.970,00 €
Serveis Gestionats	Servei	Servei de posta en marxa i 24/7	500 h	85 (€/h)	42.500,00 €
TOTAL OFERTA EXCLÒS					**144.470,00 €**
IVA 21%					**30.338,70 €**
TOTAL OFERTA IVA INCLÒS					**174.808,70 €**