PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS

PER A LA CONTRACTACIÓ DE

"Subministrament de renovació de les llicències i manteniment de l'arquitectura Security Service Edge (SSE) a ATL i el seu manteniment associat"

Març 2026

INDEX

1. OBJECTE DEL PLEC

Aquest document constitueix el plec de prescripcions tècniques (PPT) que regeix el procediment de contractació i execució dels "**Subministrament de renovació de les llicències i manteniment de l'arquitectura Security Service Edge (SSE) de Netskope a ATL i el seu manteniment associat**", promogut per l'Ens d'Abastament d'Aigua Ter-Llobregat (ATL).

Els articles s'han descrit utilitzant el nom d'una marca per facilitar la identificació del software, sense que vinculi en cap cas les licitadores a l'hora de presentar les seves ofertes, que poden fer indicant una altra marca/gamma que sigui equivalent.

Dins d'un marc de SASE, l'objectiu d'aquesta licitació està orientada a adoptar un Security Service Edge (SSE) que actuï com a punt de control del trànsit dels usuaris d'ATL cap a internet, entenent per internet Web, SaaS i IaaS tant sancionat com no sancionat. Es pretén que la seguretat en el trànsit cap a Internet sigui transparent per a l'usuari, però no per això es deixi d'inspeccionar tot el trànsit, podent protegir l'usuari en la seva navegació i protegir la informació d'ATL en la seva sortida cap a serveis SaaS, IaaS o Web.

L'abast del contracte es centra principalment en garantir la disponibilitat de la plataforma SSE així com realitzar en manteniment, suport, i actualitzacions requerides.

Concretament l'objecte de la present licitació compren anualment:

- 400 – Llicències Netskope Secure Web Gateway Professional
- 400 – Llicències Netskope Private Acces Standard
- 400 – Llicències Netskope Standard Endpoint DLP
- 400 – Llicències Netskope Advanced Analytics 13-Month Extended Data Retention
- 208 hores de manteniment i suport anual (Destinada a serveis professionals d'assistència tècnica, suport, atenció a peticions en remot, o in situ, referent al producte ofert).

2. INTRODUCCIÓ

2.1. Antecedents ATL

Ens d'Abastament d'Aigua Ter-Llobregat (ATL) és una empresa pública de la Generalitat de Catalunya, adscrita al Departament de Territori i Sostenibilitat creada

segons el **Decret llei 4/2018, de 17 de juliol**, per el que la Generalitat assumeix la gestió directe del servei d'abastament d'aigua a les poblacions mitjançant les instal·lacions de la xarxa d'abastament 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 Solsonès, el Vallès Oriental i el Vallès Occidental, el que representa uns 3.112 km2 i una població abastida del voltant de 5,5 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 70 estacions de bombament. Per a produir l'aigua, ATL disposa de cinc infraestructures principals: tres 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. Consegüentment amb tot això, ATL publica aquest plec per a contractar els "**Subministrament de renovació de les llicències i manteniment de l'arquitectura Security Service Edge (SSE) de Netskope a ATL i el seu manteniment associat**".

3. ABAST DEL CONTRACTE

Els serveis que desitja contractar ATL inclouen totes les activitats de suport per a la solució de seguretat SSE d'ATL, contemplant manteniment, suport tècnic, assessorament, informes i actualitzacions dels equips.

El proveïdor, mitjançant el seu equip de professionals, serà responsable de les següents activitats:

- Resolució d'incidències i manteniment.
- Garantia del manteniment realitzat.
- Co-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.
- Gestió del servei.

Les **aplicacions** en producció que estan dins de l'**abast del contracte** son les següents:

- Netskope Secure Web Gateway Professional
- Netskope Private Acces Standard
- Netskope Standard Endpoint DLP
- Netskope Advanced Analytics (Advanced UEBA) retenció 13 mesos
- Premium support

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

A l'apartat "Situació actual", s'inclou informació rellevant per a que els licitadors puguin fer la seva millor proposta.

4. SITUACIÓ ACTUAL

ATL disposa en l'actualitat del programari SWG del fabricant Netskope per a la protecció dels seus equips informàtics i servidors. Per això, degut al bon funcionament de l'eina, es té la necessitat de contractar un servei SSE.

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 que es vol contractar ha de complir amb l'objectiu del contracte que s'ha marcat a l'apartat Objecte del contracte.

De manera més específica, i de cara a concretar en major detall els requisits d'ATL per aquest contracte, s'inclouen a aquest apartat les consideracions que el licitador haurà de tenir en compte.

5.1. Serveis a cobrir pel adjudicatari

L'abast del servei inclou els següents elements de la infraestructura SASE, que podran evolucionar o ser flexibles, previ acord:

- Servei gestionat mensual

Revisió de la plataforma SSE:

- Secure Web Gateway (SWG).
- Data Loss Prevention (DLP).
- Netskope Private Access (NPA) .
- Advanced UEBA Analytics 13 months

Assistència i suport en configuració:

- Gestió de URLs d'accés.
- Polítiques i objectes.
- Notificacions (Alert i Block) a usuaris.
- Perfils de seguretat.
- Suport en actualitzacions.
- Anàlisi de noves funcionalitats.

Suport davant incidències en horari 9x5.

Informe mensual dedicat a la revisió de la plataforma.

Gestió i manteniment de la plataforma:

- Manteniment i operació de la plataforma, amb horari d'atenció 9x5.
- Anàlisi mensual de l'estat de salut dels elements més crítics de la infraestructura.
- Manteniment i gestió de solucions acordada amb el client.
- Manteniment de la documentació i font d'informació de l'arquitectura.
- Resolució d'incidències i gestió de les mateixes amb els fabricants (si escau), amb el compromís d'atenció contractat.
- Assessorament i suport en la realització de canvis sobre la configuració
- actual.
- Informe mensual preventiu amb bones pràctiques i recomanacions sobre
- plataforma tecnològica.
- Reunions de seguiment trimestrals executives sobre l'estat de la

- plataforma i recomanacions.
- Mesurament de la qualitat del servei mitjançant KPIs i SLAs.
- Traspàs de coneixements de l'entorn i adopció de l'administració compartida, durant el primer mes de contracte.

5.2. Requisits tècnics i arquitectura

Les especificacions tècniques quant a infraestructura, arquitectura i aplicacions es mantindran d'acord amb a l'abast del contracte (apartat 3). En el cas de que en temps de contracte el proveïdor faci alguna recomanació o proposta de canvi i millores, aquestes hauran d'estar perfectament analitzades i justificades en termes econòmics. En tot cas, correspondrà a ATL la decisió final de realitzar aquests canvis.

Requisits tècnics de l'eina:

A nivell funcional la solució haurà de complir almenys amb els requisits llistats en els punts inferiors.

Plataforma del Servei.

- A fi de garantir la solvència de la plataforma, es requereix que la mateixa oferta sigui considerada líder en el seu segment tant per Gartner (en el seu últim informe Magic Quadrant for Security Service Edge) com per IDC (en el seu últim informe Cloud Security Gateways 2023).
- La solució haurà d'estar basada en el núvol, desplegada sobre la cloud pròpia del proveïdor, basada en micro-serveis i que no requereixi l'adquisició de maquinari addicional per part de ATL.
- La solució haurà d'estar certificada per, almenys, els següents estàndards:
  - ENS Alt (per als sistemes d'informació que donen suport a NextGen SecureWebGateway, Private Access, CASB i Public Cloud Security)
  - ISO27001
  - ISO27017
  - ISO27018
  - SOC2 Tipus II.
- El proveïdor haurà de comptar amb almenys dos nodes de processament de dades a Espanya. Aquests estaran situats en punts neutres d'Internet, localitzats a Madrid i Barcelona. Aquests nodes han de tenir les capacitats completes de SSE de cara a futures expansions, per la qual cosa es descartaran aquelles solucions basades en Virtual POPS, aquelles que presentin la majoria dels seus serveis sobre cloud pública (AWS, GCP o Azure), i aquelles que necessitin redirigir el trànsit entre nodes per a la inspecció profunda de la dada.
- El núvol del proveïdor ha de comptar amb peering directe amb els principals proveïdors de SaaS i IaaS, així com amb els ISPs. Es requereix peering directe en el node d'Ibèria amb Microsoft i Google, així com peering directe amb el ISP predominant d'Espanya (Telefonica).
- La infraestructura del proveïdor ha de garantir una disponibilitat del 99,999% de servei mitjançant SLAs.
- De cara a garantir l'experiència d'usuari, el proveïdor del SSE haurà d'assegurar baix SLA unes latències màximes sobre el trànsit http de

navegació xifrat de 50 mil·lisegons (round-trip), i sobre el trànsit http en clar inferior a 10 mil·lisegons, amb inspecció profunda en tots dos casos.
- Els controls que exerceixi la plataforma SSE hauran de poder-se dur a terme en els dispositius corporatius en tot moment, particularment en els dispositius en mobilitat, amb independència de si s'està usant la xarxa corporativa o qualsevol altra per a connectar a Internet.

Integracions.

- La solució oferta haurà de poder integrar-se amb els repositoris d'identitat del (Azure d'ATL AD i Active Directory), podent aplicar regles diferents de navegació i accés a SaaS sobre la base dels diferents grups d'usuaris i OUs.
- S'haurà de garantir la integració amb el SIEM d'ATL actualment basat en Splunk.

Mètodes de Desplegament de la solució.

- La solució haurà de suportar el desplegament mitjançant la instal·lació d'un client que redirigeixi el tràfic de navegació de manera selectiva al proveïdor.
- El client haurà de suportar almenys els següents sistemes operatius Windows, MAC, Linux, iOS i Android.
- El client haurà de detectar si l'usuari està dins de la xarxa d'ATL o fora d'aquesta, podent aplicar diferents configuracions de redirecció de trànsit en cada escenari.
  - Quan l'usuari estigui en les oficines d'ATL haurà d'enviar al SSE el trànsit de navegació, contra els serveis SaaS regulats i no regulats, evitant enviar el trànsit destinat a l'adreçament privat d'ATL. S'haurà de poder excepcionar per adreces IP, categories i dominis el trànsit que s'envia al SSE.
  - S'hauran de poder crear excepcions per a evitar que el trànsit d'un procés particular de l'equip vagi al SSE.
  - Quan l'usuari estigui en mobilitat s'haurà d'enviar al SSE tot el trànsit de navegació Web, el trànsit destinat a SaaS i la resta de trànsit amb destinació IaaS.

- El client haurà de ser compatible amb les solucions VPN existents en ATL, basades en tecnologia WatchGuard. D'aquesta manera, un usuari remot podrà manar el seu trànsit de navegació i SaaS al SSE, mentre que altres fluxos trànsit continua sent enviats per la VPN.
- S'haurà de poder desplegar el client fent ús de les eines de provisió de ATL (SCCM, MDM, PDQ, etc) i una vegada desplegat el client haurà de ser gestionat de forma centralitzada des de la pròpia plataforma.
- De cara a garantir la compatibilitat amb sistemes antics, la solució haurà de poder treballar mitjançant configuració de proxy explicit. El servei de proxy explicit haurà de permetre portar les direccions IPs dels proxies actuals d'ATL proveïdor del SSE, a fi d'evitar canvis massius de configuracions.

- El servei haurà de permetre l'establiment de túnels GRE i IPSEC des de les seus d'ATL cap al SSE, facilitant així la transformació de la xarxa cap a sortides locals a Internet. En relació amb aquest punt, no haurà d'haver-hi un cost addicional associat al nombre de seus connectades, de túnels llançats o d'amplada de banda processada pel SSE.
- A fi de poder controlar l'accés a serveis SaaS corporatius d'ATL des d'equips no gestionats, la solució haurà de suportar el seu desplegament com reveure's Proxy per a O365.
- Tots els mètodes de desplegament indicats hauran de poder ser configurats de manera concurrent en la plataforma, podent aplicar cadascun a diferents usuaris, dispositius i casuístiques.

Polítiques i controls en línia de SaaS i Web.

- La solució ha de permetre l'avaluació de la postura de seguretat del dispositiu abans de permetre el seu accés a uns certs serveis Web i SaaS. Per això, el client haurà de realitzar una avaluació configuració del PC abans de permetre la navegació, podent configurar diversos controls. D'aquesta manera, es podrà evitar l'accés l'O365 d'ATL el cas que l'equip no compleixi amb els criteris de seguretat, però permetre l'accés a O365 no corporatius, o limitar la navegació web des d'un equip no posat pegats.
- A fi d'evitar la navegació a llocs de risc, la solució haurà de comptar amb una base de dades de categories de navegació. S'hauran de poder crear diferents perfils de navegació i assignar els mateixos als diferents usuaris del directori, podent integrar amb els diferents forests existents en ATL.
- La solució haurà de permetre crear categories pròpies i llistats de urls permeses i denegades sota demanda. La solució ha de permetre la modificació d'aquestes llistes a través de API, a fi d'automatitzar la resposta davant incidents.
- A fi de reduir el risc, s'haurà de tenir un motor de classificació dinàmica de urls sobre la base del seu contingut, detecció de dominis generats aleatòriament, i detecció de llocs web de recent creació.
- S'haurà de poder configurar la solució per a realitzar el bloqueig silenciós de ads bàners, pop-ups, etc
- La solució haurà de permetre habilitar Safe-Search en la navegació, bloquejar serveis de traducció i controlar els canals de youtube que puguin ser necessari habilitar.
- S'hauran de poder definir regles granulars que limitin l'accés de l'usuari només a les aplicacions cloud i serveis web als quals hauria d'accedir. Per a això ha de disposar d'una base de dades de Serveis SaaS, en la qual es pugui veure el nivell de risc dels serveis consumits des de l'organització sobre la base de criteris marcats per la CSA (Cloud Security Alliance). S'hauran de tenir indexats més de 50.000 aplicacions cloud.
- La solució haurà de ser capaç d'identificar l'usuari logat en l'aplicació cloud, a més de l'usuari logat en l'equip, i d'aplicar controls sobre la base d'això.
- Ha de permetre aplicar polítiques i controls basats en el context (usuari, localització, aplicació, instàncies de l'aplicació, contingut/classificació del document, postura de seguretat del dispositiu, objecte/paràmetre), no és suficient amb permetre o bloquejar aplicacions SaaS i Web, ha de ser

capaç d'inspeccionar en profunditat i entendre les diferents activitats en tot moment (login, logout, convidar, compartir, afegir, editar, veure, reiniciar, upload, download, entre altres).

- La solució ha d'entendre les accions dels administradors sobre instàncies de IaaS (Azure, AWS i GCP almenys) identificant accions com crear, arrencar, rebotar, parar sistemes. Haurà d'identificar i controlar si s'estan fent sobre instàncies corporatives o no corporatives de IaaS.
- Quan es produeixi el compliment de les condicions d'activació de cadascuna de les polítiques definides en la plataforma, aquesta permetrà l'execució automàtica de les següents accions:
  - Permetre l'acció o bloquejar-la.
  - Redirigir l'acció a través d'un proxy.
  - Etiquetar la connexió.
  - Generar alerta en el sistema.
  - Notificar a través de correu electrònic, podent establir-se diferents plantilles per a això.
  - Notificar a l'usuari, podent establir-se diferents plantilles per a això.
  - Posar en quarantena el fitxer en qüestió, i en aquest cas es permetrà a l'administrador revisar els arxius que es trobin en quarantena i determinar si es permet la transacció, si s'elimina, etc.
  - Emmagatzemar una còpia de l'arxiu sospitós de violar les regles DLP o qualsevol política en una instància corporativa de OneDrive o SharePoint.
- Donar visibilitat i control del ShadowData. La solució haurà de ser capaç d'identificar i controlar (permetre, denegar o alertar) sobre la base de les dades que es cursen en les aplicacions cloud consumides pels empleats d'ATL, siguin aquestes regulades o no regulades, podent controlar sobre que documents s'acciona, fitxers que pugen, es comparteixen o editen, instància de l'aplicació SaaS en la qual acaben, usuari logados en el servei SaaS… controlant així el ShadowData.
- En línia amb el punt anterior, s'haurà de crear un hash de tots els fitxers que transcendeixin cap a o des d'internet, de manera que en cas d'incident es pugui localitzar ràpidament que usuari va moure aquest fitxer i sobre que servei SaaS.
- La solució haurà de ser capaç d'aplicar diferents polítiques sobre diferents instàncies d'una mateixa aplicació cloud, podent aplicar controls diferents entre instàncies d'una mateixa aplicació en dues organitzacions. Es requereix la creació de polítiques que permetin treballar sense límits en la instància corporativa d'ATL, però limitar el tipus d'informació (per exemple sobre la base del seu etiquetatge, contingut o xifratge) que pot acabar en el OneDrive d'un tercer sense bloquejar el mateix.
- Ha de permetre modificar els missatges de bloqueig, de manera que sigui possible implementar polítiques que inicialment bloquegin l'acció, però li donin opció a l'usuari a justificar el motiu del seu accés i procedir prèvia justificació. Aquestes polítiques s'utilitzaran per a educar als usuaris sense necessitat de bloquejar l'activitat.
- La solució haurà de ser capaç de bloquejar als usuaris quan es detecti algun comportament no autoritzat. Per exemple, si un usuari porta informació a un G-Drive personal, poder llançar un avís diferenciat a l'usuari sobre la base del contingut d'aquest fitxer. Si el document pujat té dades de PCI es podrà bloquejar la pujada, si són dades de GDPR es

podrà notificar a l'usuari -instruint-li perquè usi el SaaS corporatiu, i en un altre cas es permetrà la pujada.
- Totes aquestes activitats hauran de ser loguejades i emmagatzemades per, almenys, 90 dies en la plataforma, dins del territori europeu. A més, s'hauran de poder exportar aquests logs a la plataforma SIEM d'ATL.

Polítiques i controls fora de línia de SaaS i Web.

- La solució oferta ha d'incloure en la mateixa plataforma la possibilitat de connectar-se a instàncies corporatives via API Microsoft, i aplicar detecció de Malware amb Sandboxing i DLP sobre OneDrive, SharePoint i Teams.
- Atès que pogués existir més d'un Tenant d'un mateix servei cloud en ATL, la solució CASB haurà de permetre connectar simultàniament a tots ells i administrar-los de manera conjunta des d'una mateixa consola.
- S'ha de permetre la integració amb Directori Actiu, Azure ANEU o altres repositoris d'usuaris (OKTA, PING, etc) de cara a realitzar autenticació.
- Haurà de suportar la integració amb eines de MFA com Authpoint de Watchguard.
- La solució haurà de proporcionar accés remot en dos sabors: amb client i sense client (basada en navegador).
- El client a desplegar haurà de ser únic per a la resta de funcionalitats de SSE, en el cas que ATL vulgui continuar ampliant serveis no serà necessari desplegar nous clients ni comptar amb noves consoles de gestió.
- Es requereix suport per a almenys els següents sistemes operatius: OSX, Windows, Linux, iOS i Android. És necessari indicar les versions de SSOO suportades.
- La connexió al SSE haurà de ser transparent per a l'usuari, en un model similar a "Always On".
- El client haurà de poder detectar si l'usuari es troba "on-prem" o "en remot" podent aplicar diferents configuracions en cada cas.
- La solució basada en client haurà de proporcionar accés sobre qualsevol port de la pila TCP o UDP, no limitant-se a trànsit http.
- En el cas de treballar en model client-less s'haurà de donar accés a aplicacions http/https havent d'usar els mateixos connectors/publisher ja desplegats en la xarxa interna.
- De cara a proporcionar MFA, la solució haurà de poder integrar-se amb IDPs mitjançant SAML de manera que es validi la identitat de l'usuari amb un segon factor d'autenticació abans de donar-li el primer accés a un servei intern.
- S'hauran de generar logs de l'activitat de l'usuari i del seu accés als recursos interns.
- Les polítiques de ZTNA hauran de contemplar regles sobre la base d'usuari/grup/OU, Client/ClientLess, postura de seguretat del dispositiu, aplicació de destí.

Data Protection.

- La solució ha de comptar amb milers d'identificadors de dades precargats, i més de 40 perfils d'identificació d'informació associats a diferents

normatives (GDPR, PCI, SOX, codi font, etc). Els identificadors precargats han d'estar parametritzats per a l'idioma Castellà i localitzar dades d'Espanya (DNI, Telèfons, Noms, Municipis, etc).

- A més, la plataforma ha de permetre la creació de nous identificadors i nous perfils combinant-los amb els ja existents en el sistema, aplicant condicionants booleans com AND, OR o NEAR.
- Haurà de permetre la inspecció de dades ocultes i metadades en fitxers ofimàtics.
- Haurà d'integrar amb Azure Information Protection i Unified Labeling, podent llegir les etiquetes en els documents en trànsit, i aplicar polítiques sobre la base d'aquestes.
- Haurà de ser capaç d'inspeccionar no sols fitxers sinó també els posts en pàgines d'Intel·ligència Artificial, web, xarxes socials i aplicacions de missatgeria.
- Els perfils d'identificació de dades es podran aplicar directament sobre les regles de control de navegació i control del SaaS. D'aquesta manera es podran crear regles de navegació que limitin la pujada d'informació a unes certes webs i instàncies de serveis SaaS.
- En cas de contractar altres mòduls de la plataforma, els mateixos identificadors de dades es podran emprar per a escanejar dades en repòs en OneDrive, en buckets de IaaS o en el correu electrònic sortint.
- La solució haurà de ser capaç de mostrar totes les pujades de dades realitzades des del personal d'ATL qualsevol aplicació cloud o pàgines web, buscant sobretot aquelles pujades d'informació que han acabat fora de la UE, i aquelles pujades d'informació que han acabat en aplicacions malament prestigioses segons els criteris de la Cloud Security Alliance.
- En el moment de ser desitjat, els perfils d'identificació de dades creades, hauran de poder utilitzar-se en la protecció del correu electrònic mitjançant integració amb la MTA existent en ATL prèvia adquisició de la llicència apropiada.

Threat Protection.

- El motor de navegació haurà de comptar amb un filtre IPS que eviti l'execució de contingut maliciós des del servidor en el navegador de l'usuari que realitzi la connexió.
- La solució haurà de comptar amb un motor antimalware que permeti detectar amenaces en trànsit cap a i des d'ATL en temps real. S'hauran de poder inspeccionar tant uploads com downloads a SaaS, IaaS i Web.
- El motor de detecció de Malware haurà de combinar diversos mètodes com ara integració amb diferents fonts d'intel·ligència, tècniques anti-exploit, signatures antimalware.
- El motor antimalware haurà de suportar la integració amb IOCs generats pel SOC del , ATL de manera que es puguin importar els mateixos de manera dinàmica mitjançant API.
- El motor antimalware haurà de poder intercanviar IOCs amb la solució de endpoint d'ATL basada en Kaspersky EDR.
- La solució oferta ha d'incorporar un mòdul de UEBA que permeti l'anàlisi sobre el comportament de les accions de l'usuari, així com de les aplicacions a les quals es connecten.

Model de llicenciament.

- La solució haurà de llicenciar-se pel nombre d'usuaris totals, podent cada usuari tenir més d'un dispositiu.
- S'hauran de poder desplegar tants Publishers o Connectors a la xarxa interna com sigui necessari. Aquests connectors hauran de ser capaços de balancejar de manera autònoma les sessions dels usuaris cap a les aplicacions internes.
- La solució no portarà costos addicionals per consum d'amplada de banda, nombre d'aplicacions definides, localització d'aquestes aplicacions (IaaS o Datacenter), nombre de connectors, sent aquests punts transparents per a ATL.
- BYOD. Es desitja poder controlar l'accés a les aplicacions cloud regulades més comunes (almenys O365, G-Suite, Salesforce, ServiceNow, Workplace) encara quan el mateix es produeixi des de dispositius no corporatius, permetent l'accés a l'aplicació però registrant tota l'activitat de l'usuari en la mateixa i podent limitar la descàrrega d'una certa informació sensible a un dispositiu no gestionat.
- La solució oferta ha d'incorporar un mòdul de UEBA que permeti l'anàlisi sobre el comportament de les accions de l'usuari, així com de les aplicacions a les quals es connecten.
- La solució haurà de ser capaç de llançar alertes en el cas de detectar possibles exfiltracions (dades que passen d'una aplicació o instància corporativa a una aplicació o instància no corporativa).

Programari / Suport	**Unitats**	**Data inici**	**Durada**
Secure Web Gateway Professional	400	17/08/2026	2 anys
Network Private Acces Standard (ZTNA)	400	17/08/2026	2 anys
Standard Endpoint DLP	400	17/08/2026	2 anys
Netskope Upgrade to Advanced Analytics (UEBA) amb retenció de 13 messos.	400	17/08/2026	2 anys
Premium suport de fabricant (Netskope)	1	17/08/2026	2 anys
Servei de manteniment (bossa hores)	208 (hores mnt/any)	17/08/2026	2 anys

La renovació començarà a partir del 17/08/2026, no obstant, l'adjudicatari haurà de proporcionar les llicències amb una antelació superior a 1 setmana abans de la data de renovació. Sempre que sigui possible formalitzar contracte abans d'aquesta data.

Tasques a desenvolupar:

1. L'adjudicatari haurà de proporcionar a ATL les llicències indicades.
2. El contractista serà responsable d'oferir un suport especialitzat de manteniment reactiu i preventiu dels productes basats en la tecnologia proposada que han sigut contractats.

5.3. Garantia dels treballs

Tots els canvis que es posin en producció hauran de contemplar una garantia de correcte funcionament de mínim 3 mesos, des de que s'han posat en producció. Durant aquest període, l'adjudicatari es compromet a resoldre satisfactòriament totes aquelles incidències o defectes detectats en producció imputables a ell per acció o per omissió, sense cost per ATL.

Addicionalment, durant el període de manteniment, els treballs que es realitzin tindran també garantia de 3 mesos des de la resolució de les incidències que es detectin.

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

La durada d'aquest contracte de servei és de **vint-i-quatre (24) mesos** a comptar des de l'17/08/2026 o des de la data de formalització si aquesta és posterior.

Quant al dimensionament del volum d'hores requerides, s'estima un total de 416 hores de treball, que de forma anual son 208 hores de treball. Aquesta estimació d'hores inclou totes les activitats descrites al apartat de "Requisits del servei", contemplant els diferents perfils de professionals que siguin necessaris.

El volum d'hores indicat es el màxim contractat per any. ATL, d'acord amb les seves necessitats, farà les seves sol·licituds al adjudicatari consumint d'aquestes hores contractades. No obstant, ATL no estarà obligada a consumir el 100% de les hores contractades.

5.5. Calendari i lloc de treball

En relació als treballs a realitzar amb coordinació amb professionals d' ATL, aquests 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 i perfils professionals

L'adjudicatari haurà de destinar per l'execució del servei els professionals adequats amb coneixements i experiència en plataformes de securització i administració SASE, específicament hauran de tenir experiència en la solució SWG/NPA/DLP/Advanced Analytics (13 mesos de retenció) de Netskope.

Igualment, l'adjudicatari designarà almenys un responsable del contracte que es mantindrà durant el projecte.

L'equip de treball proposat haurà de identificar com a mínim 3 rols, que son:

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 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 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 3 anys en gestió de serveis i/o projectes relacionats amb plataformes/serveis de Netskope

2 Tècnics en plataformes SSE

Les responsabilitat dels tècnics/analistes, inclouen, entre d'altres:

- Anàlisi dels requeriments i necessitats que es plantegin en el contracte.
- Suport i manteniment de la solució SSE
- 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 3 anys en desplegament i suport en eines de securització i administració de plataformes de Netskope

El membres de l'equip es consideren obligació contractual essencial i, per tant, el seu incompliment comportaria la resolució del contracte, el compromís adscripció permanent a l'equip d'execució d'aquest contracte, durant la totalitat de la seva vigència, de l'equip tècnic que l'adjudicatari s'ha compromès a adscriure a l'execució

dels treballs, que necessàriament ha de complir amb els requisits establerts en el PPTP d'aquesta licitació.

Malgrat això, si per motius sobrevinguts i imprevistos al moment de formular la proposta el contractista sol·licita la seva substitució, ATL podrà autoritzar expressament aquest canvi , sempre que: el contractista justifiqui degudament la causa excepcional que l'impedeix mantenir l'adscripció al que es va comprometre i que la persona o persones proposades tinguin una qualificació i perfil professional equivalents als ofertats. En qualsevol cas, és ATL qui ha de valorar si concorren aquestes circumstàncies i resoldrà motivadament sobre l'acceptació de la substitució o bé la resolució del contracte per incompliment d'aquesta obligació essencial.

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 d'ATL de les possibles incidències en el servei previstes i no previstes i dels canvis que potencialment afectin els sistemes d'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 del 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:

- 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 son els següents:

	Acords de nivell de servei (ANS)	**Compromís**
ANS 1	ANS 1: Temps de màxim de resolució d'incidències crítiques: temps correcció incidència. 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.	< 24 hores
ANS 2	ANS 2: Temps màxim de resposta en dies, per a presentar la valoració i planificació de la solució. Serà el temps que trigui l'adjudicatari a presentar una proposta de solució, estimació en hores i planificació en resposta a noves peticions d'evolutius traslladades per ATL.	< 4 dies
ANS 3	ANS 3: Temps màxim per iniciar els treballs en dies, a contar des de que s'aprova la valoració. Serà el temps que trigui l'adjudicatari a iniciar els treballs d'implantació, des de que ATL doni la seva acceptació a la proposta presentada.	< 4 dies
ANS 4	ANS 4: Acompliment planificacions dels treballs planificats. Serà l'acompliment de les planificacions que hagi presentat i s'hagin acceptat. Es mesurarà en base a no tenir endarreriments de la data d'implantació i posta en marxa de les solucions dissenyades. Els endarreriments es mesuraran com un % relatiu a la durada total del treball planificat, segons la fórmula: % Endarreriment = dies de retard / total dies del treball planificat. El % de retràs es calcularà com el nombre de dies que s'endarrereix la posta en marxa del total de les funcionalitats en el abast del treball en qüestió planificat, dividit entre el nombre total de dies d'aquest treball segons la planificació inicial acordada. En cas de que al llarg del treball es pacti una re planificació, serà d'aplicació les noves dates i calendari pactat. En cas de que el retràs NO afecti a totes les funcionalitats posades en marxa, i les funcionalitats endarrerides no suposen un volum important de les solucions (inferior a un 10% del volum de treballs), NO es considerarà un endarreriment.	> 15%

Acompliment dels ANS i aplicació de penalitzacions:

Mensualment es comptabilitzarà el nombre total d'incompliments dels ANS, sumant el total de tots els acords. Amb aquest nombre total d'incompliments, ATL podrà aplicar una penalització en % sobre la facturació d'aquell mes d'acord amb la següent taula:

Total incompliments 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"). El proveïdor 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 esmentades pel proveïdor, 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, el proveïdor 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 proveïdor, i a aquest efecte, el proveïdor 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, el proveïdor 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 proveïdor 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 mitjà en el que està enregistrat.

L'adjudicatari es compromet 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 concedeix 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 son 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 ha 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.

Especialment, el licitador haurà d'indicar el **preu per hora de treball**, que serà el que s'utilitzarà per a la valoració i facturació dels treballs mensualment. El preu hora inclou els serveis de suport de l'equip assignat.

El licitador establirà un preu per hora de treball únic com a mitjana per tots els perfils involucrats en la prestació del servei, en base al dimensionament que consideri

adequat per a garantir els Acords de Nivell de Servei (definits en l'apartat 5.8) requerits per a la prestació del servei.

El pressupost de licitació del contracte serà de 280.053,99 € IVA inclòs (231.449,58 € IVA exclòs). Respecte el pressupost del contracte, que distribuït segons la següent distribució pressupostària:

Concepte	***2026***	***2027***	***2028***	***IMPORT SENSE IVA***	***IVA (21%)***	***IMPORT AMB IVA***
Servei (208 hores/any)	7.800,0 €	18.720,0 €	10.920,0 €	37.440,00 €	7.862,40 €	45.302,40 €
Eina (24 mesos - 400 usuaris)	97.004,79 €	97.004,79 €	0 €	194.009,58 €	40.742,01 €	234.751,59 €
TOTAL	***104.804,79 €***	***115.724,79 €***	***10.920,0 €***	***231.449,58 €***	***48.604,41 €***	***280.053,99 €***

41.250 €/ 416 hores totals (2 anys) = 90 €/hora

Justificació del pressupost: Els preus indicats s'han calculat d'acord a preus vigents de mercat i al cost del servei en anys anteriors i ja contemplen els costos directes dels mitjans personals i materials, també els costos d'altres mitjans, dietes i desplaçaments, treballs de reproducció i edició, etc. taxes, assegurances i impostos a excepció de l'IVA, necessaris per desenvolupar els treballs d'acord amb el que estableix el present plec.

No s'admetran revisions de preu.

8. FACTURACIÓ DEL SERVEI

La **facturació del servei** es realitzarà de manera mensual a mes vençut, en base a les hores reportades a l'informe mensual de seguiment. I al **preu de referència per hora de treball** que indiqui a l'oferta econòmica l'adjudicatari. La facturació dels treballs planificats NO podrà superar la planificació en hores que s'hagi acordat per cada un d'aquests. 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.

La **facturació de la llicència** s'efectuarà un únic cop de forma anual, en el moment del subministrament/renovació d'aquesta.

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 d'expedient.

Sant Joan Despí, a data signatura digital

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