PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS

PER A LA CONTRACTACIÓ DE

"Servei d'adquisició i implantació d'una aplicació on premise de Gestió de Vulnerabilitats IT"

(2026-0078-OSE)

Febrer 2026

INDEX

1. OBJECTE DEL PLEC

Aquest document constitueix el plec de prescripcions tècniques (PPT) que regeix el procediment de contractació i execució dels "**Servei de Gestió de Vulnerabilitats IT**", promogut per l'Ens d'Abastament d'Aigua Ter-Llobregat (ATL).

L'abast del contracte es centra principalment en el **subministrament i posta en marxa d'una aplicació on premise de gestió de Vulnerabilitats IT amb el llicenciat corresponent i el servei de suport i gestió continua de les vulnerabilitats dels sistemes**.

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 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 "**Servei de Gestió de Vulnerabilitats IT**".

3. ABAST DEL CONTRACTE

L'abast del contracte del servei és el de consolidar un model de gestió de Vulnerabilitats IT.

Per assolir aquest objectiu es planteja abordar fent ús d'eines, procediments i protocols d'actuació per a gestionar de manera eficient els riscos derivats de les vulnerabilitats que potencialment puguin afectar els Sistemes d'Informació i facilitar la detecció, protecció, resposta i manteniment proactiu de la infraestructura tecnològica d'ATL.

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

La missió de la direcció de Sistemes d'Informació d'ATL és la d'aportar el conjunt d'activitats, maquinari i programari de manera organitzada i eficient per a donar

solució a les necessitats funcionals de les àrees de negoci d'ATL. Tot això complint els requisits d'òptim rendiment, màxima seguretat i costos adequats.

Sota aquests propòsits, la Direcció de Sistemes d'informació ha marcat als últims anys les directrius, procediments i catàlegs de serveis que permeten un correcte govern del servei i securització dels seus actius. Front això, ATL **vol implantar el servei de gestió de vulnerabilitats de la infraestructura IT amb una solució on premise**. Aquesta infraestructura haurà d'estar allotjada a les instal·lacions d'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 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 per l'adjudicatari

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:

- Desplegament de la solució
    - Inici del projecte (Kickoff, llançament del projecte)
    - Anàlisis i disseny de l'arquitectura
    - Desplegament de la infraestructura Base
    - Desplegament i configuració de la resta del parc
    - Documentació i traspàs de coneixement

- Servei de gestió continua de les vulnerabilitats
    - Configuració inicial
    - Gestió d'inventari
    - Classificació i normalització
    - Detecció de vulnerabilitats (aquí comença la part recurrent)
    - Anàlisis de resultats. Priorització
    - Seguiment correccions
    - Validació de correccions
    - Reporting & Control
    - Millora continua

5.1.1. Desplegament de la solució

Kick-off (Acta d'inici), Anàlisi i disseny d'arquitectura

Aquesta fase possibilita la coordinació entre tots els interlocutors que prendran part en el desenvolupament de cadascun d'ells mitjançant una reunió de llançament amb els següents objectius:

- Presentació d'interlocutors
- Recepció d'equipament i llicencies
- Coordinació de dates

A posteriori, en aquesta fase s'executarà la coordinació entre tots els agents que prendran part en el desenvolupament de cadascun d'ells mitjançant una reunió de llançament amb els següents objectius:

- Definició d'Arquitectura i Pla d'Implantació.
- Recopilació d'informació d'abast.
- Identificació d'aspectes específics de les comunicacions.
- Identificació de mecanismes i eines de desplegament
- Proposada de la planificació
- Disseny i validació del Pla de Proves

Al final d'aquesta fase es posaran a disposició dos lliurables:

- Disseny i arquitectura final
- Pla de proves

Desplegament de la infraestructura base

Realització de les activitats necessàries per al desplegament de la infraestructura base de la solució segons l'arquitectura definida en la fase de disseny preparant-la per a la construcció de les polítiques d'accés establertes en l'abast del servei.

Al llarg d'aquesta fase es duran a terme les següents tasques:

- Instal·lació remota i configuració inicial de les màquines, interfícies i components requerits per la solució.
- Suport al desplegaments inicial de scanner, agents, sensors requerits en la infraestructura.
- Configuració de l'entorn i la línia base d'escanejos
    - Identificar els requisits (legals o reglamentaris, polítiques, etc.)
    - Configuració d'escanejos, Reports personalitzats i Dashboard.

- Validació inicial de l'entorn, prova inicial de funcionament.

Desplegament i configuració de la resta del parc

Una vegada desplegada la infraestructura base, l'adjudicatari haurà de col·laborar amb el desplegament i configuració de la resta de components:

L'adjudicatari haurà de proposar diferents mètodes de desplegament que ATL usarà segons les seves necessitats o preferències i que hauran estat validats i provats en la fase anterior.

Al llarg d'aquesta fase es duran a terme les següents tasques:

- Desplegament dels agents en la resta del parc. Es realitzarà el desplegament dels agents per part d'ATL en la resta dels endpoints verificant la seva aparició i visibilitat des de la consola de gestió.
- Supervisió i suport davant dificultats d'instal·lació. L'adjudicatari supervisarà durant el temps d'instal·lació de la resta dels agents el comportament de la infraestructura i farà costat al personal d'ATL en el desplegament dels agents davant qualsevol dubte o dificultat que pogués aparèixer en el procés.

Formació i traspàs del coneixement

Realització de les activitats necessàries pel traspàs de coneixement als usuaris de l'eina.

Les activitats vinculades a aquest tema seran:

- Traspàs de coneixement tècnic del desplegament. Detall de les configuracions i arquitectures desplegades com a part del projecte de manera que sigui conegut pel personal tècnic que s'encarregarà de la gestió i operació posterior.
    - Explicació dels components de l'arquitectura desplegats, les seves funcions i interrelacions.
    - Inventari de components i les seves configuracions i parametritzacions concretes.
    - Configuració de la consola.

- Traspàs de coneixement d'administració. Capacitats i gestió operativa i administrativa de la solució desplegada aquest projecte.

    - Descripció de les tasques administratives més comunes:
        - Creació de nous escanejos.
        - Reports i dashboard
        - Desplegament de nous components
    - Indicacions i recomanacions en la gestió.

5.1.2. Gestió continua de les vulnerabilitats

Configuració inicial

Fase ja contemplada en la part inicial del servei:

- Desplegament i configuració inicial

- Preparació del servei

Gestió del inventari

Revisió de tot el inventari:

- Inclou la classificació dels actius i actualitzar tots els actius durant el servei.
- Comprovació periòdica de l'inventari d'actius d'ATL. (Comunicació constant amb el client).
- Els gestors d'actius identificaran els actius d'ATL, independentment de la seva ubicació i del tipus d'infraestructura existent
- Descobriment dels actius (fent ús d'eines automàtiques).

Classificació i normalització

- Caracterització, normalització, classificació, priorització dels actius de l'inventari tant noves incorporacions com actius continus.
- Revisió contínua dels paràmetres dels escanejos per a la millora contínua de detecció de vulnerabilitats i eliminació automàtica de falsos positius.

Detecció de vulnerabilitats

Procés continu de detecció de vulnerabilitats

- Executar el procés d'escaneig configurat en l'eina.
- Supervisió del procés d'escaneig per especialistes.
- Interacció amb els equips involucrats durant l'escaneig per a notificar el treball, incidents, afectacions etc.
- Notificació del començament i del final de l'escaneig.

Anàlisis

Revisió de resultats. Una vegada finalitzin els escanejos, s'abordi una fase d' "Avaluació". Aquesta consisteix en una anàlisi en profunditat, de les vulnerabilitats identificades. Aquest procés estarà basat en l'experiència de l'equip, així com en les proves manuals que es llancin sobre els actius més crítics.

Al seu torn, realitzar una anàlisi exhaustiva de les possibles agrupacions de vulnerabilitats per solucions de remediació, que permetin minimitzar el conjunt de tasques a tractar.

D'altra banda, també es farà un treball de "Priorització" segons criteris de risc – NVD, OWASP, CWE o altres-, i impacte de les vulnerabilitats en ATL. Addicionalment, s'introduirà un anàlisi de l'entorn i de la complexitat d'explotació de la vulnerabilitat, fent ús a més de la vulnerabilitat en si, CVSS, la criticitat de l'actiu, etc. i s'inclourà també una anàlisi de la probabilitat de l'amenaça.

Per a l'anàlisi de la probabilitat de l'amenaça l'adjudicatari estudiarà:

- Els atacs més comuns (actuals, en l'entorn i tipus de client) d'acord amb el repositori intern de coneixements de l'adjudicatari.
- Anàlisi conjunta amb ATL dels seus feeds d'intel·ligència (amenaces, exfiltració d'informació, etc.).
- Anàlisi conjunta amb ATL dels seus incidents i alertes, per a determinar tipologies d'atacs que reben sovint i la tipologia de vulnerabilitats més explotades

D'aquestes fonts es podrà triar el Top ten de vulnerabilitats a prioritzar. Amb totes aquestes anàlisis es podrà proposar un sistema de priorització alineat directament amb l'entorn i amenaces actuals.

Tractament i validació de les correccions

Durant tot el cicle de la gestió de vulnerabilitats es realitzarà un seguiment de l'estat de les correccions, i compliments d'aquestes. Es donarà suport a la comprensió d'aquestes, possibles solucions i mesures compensatòries en els casos que no sigui possible.

A més, les tasques de correcció són responsabilitat d'ATL. Una vegada remeiat es comprovarà en la següent fase d'escaneig.

Activitats documentals

L'adjudicatari haurà de mantenir la documentació relativa al servei, tant funcional com tècnica i de seguiment.

- Informes tècnics automàtics de l'eina.
- Pla de remediació adequat a les capacitats reals d'ATL i al risc.
- Preparació de la presentació executiva i taller tècnic:
    - Les situacions de vulnerabilitat i evolució durant els serveis
    - Principal problema dels serveis
    - Informació detallada sobre cada actiu
    - Vulnerabilitats evolució de noves vulnerabilitats.
    - Anàlisis acumulatives.
    - Evolució dels plans de remediació
    - Plans incomplets
    - Compensatori
- Seguiment periòdic de les vulnerabilitats
    - Aclariments de dubtes
    - Seguiment
    - Millores

Millora continua del servei

Durant tot el cicle del servei de treballessin en paràmetres que permetin mesurar l'evolució d'aquest i el seu paper en les millores en el client. Per tant, es definiran, avaluaran i mesuraran:

- KPI i KGI
- Noves plantilles i metodologies d'escaneig
- Solucions per els principals problemes en els plans de remediació
- Pròximes passes i cicles

5.2. Requisits tècnics

L'adjudicatari serà responsable de proposar i implantar una solució software per a la implantació del model dissenyat i un servei de suport a aquest. L'aplicació haurà de ser una solució de mercat de reconegut prestigi en la gestió de les vulnerabilitats del sistemes TI. Els requisits mínims a complir per la solució seran els següents:

Requisits tècnics i relatius a funcionalitats IT

- La solució ha d'integrar plenament l'exploració i el compliment de llicències per a incloure combinat i consolidació de dades, anàlisis i consultes.
- La solució ha d'incloure motors o escàner actiu i opcional passiu per a aconseguir plena visibilitat de les vulnerabilitats i el compliment.
- La solució ha de proporcionar l'exploració basat tant sense agents com mitjançant agent.
- La solució ha de proporcionar normalització de registres (logs) integrat i en temps real i recopilació d'aquests esdeveniments per a reporti i anàlisis forense.
- La solució ha de comptar amb un esquema llicenciament flexible per rangs de direccions IPs. Quant a l'escaneig d'aplicatius Web, el llicenciament haurà de ser basat en FQDNs.
- La solució ha de ser on-*prem per a la gestió de vulnerabilitats de xarxa, i tots els seus components han de ser instal·lats dins de la infraestructura del client.
- La solució ha de proveir mecanismes per a prioritzar eficaçment la mitigació de les vulnerabilitats, sobre la base de la probabilitat d'impacte real que aquestes tinguin.
- La solució ha de proveir com a opcional un modulo que permeti classificar als actius (equips) per la criticitat que aquests tenen per a l'organització. A més, que permeti mesurar el risc que té l'organització sobre la base de la criticitat dels actius i l'impacte real que tenen les seves vulnerabilitats.
- La solució ha de proporcionar un servidor o consola centralitzada per a la recollida i gestió de la informació de seguretat que resideix localment o dins de la xarxa de l'organització.
- Per a l'anàlisi de vulnerabilitats d'aplicatius Web basats en OWASP Top 10, s'haurà d'emprar un Web Application Scanner que estigui situat en la cloud del proveïdor, perquè d'aquesta manera la visió de la vulnerabilitat Web sigui semblant a la de l'atacant. Haurà de ser possible incorporar un o diversos Web Application Scanners en la xarxa interna si així ho requereix el servei.
- La solució ha de proporcionar la capacitat per a desplegar una arquitectura per nivells (multi-*tenant).
- La solució ha de centralitzar i automatitzar l'actualització de vulnerabilitats i amenaces en els seus sensors diàriament.
- La solució ha de proporcionar un procés d'actualització fora de línia (Offline) per a actualitzar el sensor per a xarxes o segments aïllats.

- La solució ha de proporcionar un model d'emmagatzematge integrat que no es basi o requereixi llicenciament de base de dades d'un tercer.
- La solució ha de ser configurable per a retenir resultats per un període de temps després de la qual cosa els resultats s'expirin i siguin purgats de la base de dades automàticament segons definit i configurable.
- La solució ha de proporcionar una completa API per a scripting automatitzat de digitalització i l'exportació de les dades de seguretat.
- La solució ha de ser compatible amb una varietat de plataformes per al motor d'exploració a incloure Windows, Linux, Mac US, així com dispositius virtuals o basades en maquinari.
- Un dispositiu virtual (Virtual Appliance) ha d'estar disponible per als motors d'anàlisis i consoles, sense cap mena de cost addicional per distribució.
- Un servei opcional d'escaneig allotjat externament que és ASV PCI ha d'estar disponible per a la digitalització de les xarxes perimetrals.
- La solució ha de ser compatible amb diversos motors d'anàlisis distribuïdes geogràficament o lògicament gestionats per una consola centralitzada.
- La solució ha de proporcionar llicències flexibles de desplegament de l'escàner amb la capacitat d'implementar escàners addicionals sense cost addicional per sensor.
- La solució ha d'oferir la possibilitat de configurar els ports, protocols i serveis per a les connexions amb escàners desplegats en tota la xarxa. Així permetent utilització de mitjans alterns d'autenticació entre la consola central i el sensor.
- La solució ha de ser configurable per a permetre l'exploració d'estrangulació per a evitar la generació de trànsit suficient per a interrompre la infraestructura de xarxa normal o reduir impacte en l'amplada de banda.
- La solució ha de proporcionar la capacitat de suportar línia d'exploració (manual import) i els resultats que importen en el servidor per sensors no manejats.
- La solució ha de permetre l'entrada i l'emmagatzematge segur de credencials d'usuari, incloent-hi els comptes locals i de domini de Windows, Unix i el seu i suo a través de ssh. Detall el mètode utilitzat per a xifrar aquestes dades.
- La solució ha de proporcionar la capacitat d'elevació de privilegis contra objectius dels usuaris normals arran d'accés / administrativa. Ha de secundar SUDO, SU o una combinació d'aquests.
- La solució ha de suportar un nombre il·limitat de credencials "ssh".
- La solució ha d'integrar-se amb cofres digitals de credencials, per a la utilització i administració de credencials.
- La solució ha de ser compatible amb un descobriment actius, capaç que no ocupi contra el consum de llicències adquirides. Detall a política d'escàner que compleixi.
- La solució ha de proporcionar una capacitat d'exploració activa i capacitat d'anàlisi de xarxa passiva per al descobriment d'actius.
- La solució ha de ser capaç de detectar dispositius mòbils. La solució ha de ser capaç d'integrar-se amb producte de seguretat OT per a possibilitar un punt de visió únic de l'estat de les vulnerabilitats i el risc per a IT i OT.
- La solució no ha de dependre de cap producte o parts d'un tercer per al descobriment d'actius, escaneig de ports, o la identificació del sistema operatiu. Ha d'estar nadiuament integrat a la consola de gestió central.
- La solució ha de proporcionar escaneig d'aplicacions de web estàtics integrat i descobriment de serveis de base de dades.
- La solució ha de ser capaç de detectar els serveis que s'executen en ports no estàndard.

- La solució ha de ser capaç de provar diverses instàncies del mateix servei que s'executa en diferents ports.
- La solució ha de ser capaç d'escanejar amfitrions morts (dispositius que no responen a un ping)
- La solució ha de secundar-se de l'ús opcional del comando netstat per a l'enumeració ràpida i precisa dels ports oberts en un sistema quan se subministren credencials.
- La solució ha de ser compatible amb l'ús de SMB i WMI per a la digitalització dels sistemes Windows.
- La solució ha de ser capaç d'iniciar automàticament els serveis de registre remot en els sistemes Windows quan executa una anàlisi amb credencials, després automàticament es detindrien els serveis de nou una vegada finalitzada l'exploració.
- L'escàner ha de ser compatible amb Secure Shell (SSH) amb la capacitat d'escalar privilegis d'anàlisis de vulnerabilitat i auditories de configuració en sistemes Unix.
- La solució ha de proporcionar la capacitat de sintonitzar polítiques d'anàlisis d'impacte mínim en les xarxes i els objectius.
- La solució ha de proporcionar la capacitat de detectar nous dispositius i enviar alertes vaig veure les notificacions de correu electrònic, registre del sistema, o la consola.
- La solució ha de proporcionar la capacitat per a posar en marxa de manera automàtica exploracions contra nous dispositius.
- El producte ha de recolzar l'ús d'un agent soluble per a l'auditoria.
- La solució ha de ser capaç de la detecció de la vulnerabilitat local i remota sense la necessitat d'un agent de client instal·lat en el dispositiu de destí.
- La solució ha de proporcionar una quantitat significativa de comprovacions de vulnerabilitat més enllà del sistema operatiu o plataforma Microsoft Windows.
- La solució ha de ser capaç de seguir els canvis de DHCP mitjançant l'associació dels resultats de l'anàlisi amb els noms de host del sistema.
- La solució ha de ser compatible amb la capacitat de preservar els resultats de l'anàlisi dels sistemes inactius per un període personalitzable i d'Identificació de les vulnerabilitats en el temps
- La solució ha d'incloure sortida detallada dels resultats d'exploració per a incloure informació tal com versions de llibreries DLL o executables esperats i els trobats.
- La solució ha de ser compatible o aprovat per CVE i proporcionar almenys 10 anys de cobertura de l'estàndard de CVE.
- La solució ha d'informar sobre les febleses conegudes en un objectiu donat, identificat per les organitzacions d'assessorament de seguretat (per exemple, Vulnerabilitats i Exposicions Comunes base de dades (CVE) o la base de dades de Open Source vulnerabilitat (OSVDB) o la Security Focus Bugtraq (BID) o qualsevol combinació d'ells).
- La solució ha de donar suport a la capacitat d'agregar opcionalment el servei reporti PCI Aproved Scanning Vendor (ASV) per a les revisions trimestrals.
- La solució ha de ser compatible amb l'escaneig de vulnerabilitats PCI DSS Compliance. El producte ha d'incloure plantilles d'escaneig per a PCI i PCI DSS predefinides que compleixin amb els criteris actuals de PCI DSS per a escaneig en xarxa. Ha d'existir funcionalitat per a filtrar totes les vulnerabilitats rellevants que no siguin PCI.
- La solució ha de proporcionar auditoria de pegats per als sistemes operatius de Microsoft i aplicacions, com Windows XP, Windows 7, Windows 2008, Windows 2012, Internet Explorer, Microsoft Office, IIS, Exchange, i altres més.

- La solució ha de proporcionar auditoria de pegats per als principals sistemes operatius Unix a incloure Mac US, Linux, Solaris, IBM AIX, HP-UX, i altres més.
- La solució ha de proporcionar revisió de pegats per a la infraestructura de xarxa per a incloure Cisco, Palo-Alt, Juniper i més.
- La solució ha de donar suport a l'exploració de SCADA i altres dispositius integrats o controls industrials per vulnerabilitat o compliment amb millors pràctiques.
- La solució ha de donar cobertura a aplicacions de tercers com Java i Adobe i altres.
- La solució ha de proporcionar una integració amb els sistemes d'administració de pegats per a l'auditoria i informes de pegats delta en els resultats de digitalització, a incloure Microsoft WSUS / SCCM, Redhat Satelite, IBM Tivoli Endpoint Manager, Altiris, VMware Go.
- La solució ha de proporcionar una integració amb els directors de dispositius mòbils (MDM) per al descobriment de dispositiu mòbil i la seva auditoria de risc.
- La solució ha de proporcionar capacitats d'auditoria per a dispositius i xarxes de control industrial o SCADA.
- La solució ha de proporcionar informació de reputació en processos trobats i l'amenaça en intel·ligència alimentada a la recerca de malware i xarxes de zombis durant l'anàlisi.
- La solució ha de proveir la puntuació de vulnerabilitat d'acord amb l'estàndard de la indústria acceptat, és a dir, el Common Vulnerability Scoring System (CVSS).
- La solució ha de proporcionar mecanisme de puntuació ponderada personalitzable basat en estàndards de la indústria acceptat com CVSS.
- La solució ha de proporcionar informació de explotabilidad contra les plataformes de validació com Core Impact, Canvas, i altres.
- La solució ha de proporcionar informació de explotabilidad per malware.
- La solució deu intel·ligentment seleccionar proves basades en la informació obtinguda de les anàlisis inicials per a intentar més proves sobre la base de la informació obtinguda prèviament sobre un dispositiu o equip donat. Per exemple basat en el sistema operatiu.
- La solució ha de realitzar el seguiment del cicle de vida de les instàncies de vulnerabilitat en què es refereix als hosts individuals, així com el medi ambient, per a incloure quan una vulnerabilitat va ser descoberta, ultima veus observada, i mitigat o prèviament-mitigat.
- La solució ha de ser compatible amb la vulnerabilitat i el compliment en exploració de servidors VMware utilitzant el API de VMware nadiu.
- La solució ha de permetre la detecció programada de dispositius.
- La solució ha de permetre que les proves seleccionades s'activin o deshabilitin durant les exploracions.
- La solució ha d'incloure la capacitat de desactivar els controls potencialment nocius de manera que siguin opcionals.
- La solució ha d'iniciar i detenir les cerques en el calendari sense interacció amb l'usuari de manera automàtica
- La solució ha de permetre la possibilitat de pausar i reprendre les exploracions de manera interactiva.
- La solució ha de permetre que les exploracions que no es completin dins d'un període de temps establert es traslladin al següent període programat.
- La solució ha de ser capaç d'acceptar objectes d'anàlisis en múltiples formats, incloent-hi els noms DNS, rangs d'IP i classes d'IP, i les llistes d'actius

predefinits. Per exemple 10.0.1.1 - 10.0.1.100. També ha d'admetre's la importació d'una llista d'IP contingudes en un arxiu font.

- La solució ha de secundar exploració IPv6, amb el descobriment passiu d'objectius utilitzant IPv6.
- La solució ha de proporcionar la capacitat d'excloure l'escaneig de dispositius perifèrics com les impressores o sistemes "embeded".
- La solució ha de proporcionar la detecció de la vulnerabilitat per a Novell Netware.
- La solució ha de ser capaç de basada en agents i sense agents l'auditoria de compliment amb controls de seguretat i millors pràctiques.
- La solució ha de tenir la funcionalitat "opcional" de monitoratge per mitjà d'un agent o client instal·lat en el dispositiu de destí.
- La solució ha de proporcionar una vista consolidada de tots els resultats d'auditoria de vulnerabilitat i compliment. Amb panells de control o Dashboards suggerits, i la capacitat de crear nous detalladament.
- La solució ha de proporcionar punts de referència de seguretat i auditoria de configuració per al compliment de les normes reguladores com PCI i altres indústries i proveïdors estàndard de millors pràctiques com a CIS o NIST.
- La solució ha de proporcionar punts de referència de seguretat i auditoria de configuració per a les millors pràctiques de proveïdors o fabricants com Microsoft, Cisco, PaloAlto i VMware.
- La solució ha de proporcionar auditoria de VMWare ESXi i vCenter utilitzant el SOAP API propi de VMware.
- La solució ha de proporcionar verificació dels sistemes operatius de Microsoft per a la configuració de seguretat i configuracions.
- La solució ha de proporcionar l'auditoria dels principals sistemes operatius Unix / Linux per a la configuració de seguretat i configuració d'aplicatius instal·lats.
- La solució ha de proporcionar auditoria de bases de dades per a la configuració de seguretat i configuracions.
- La solució ha de proporcionar auditoria d'aplicacions per a la configuració de seguretat i configuració.
- La solució ha de proporcionar auditoria d'infraestructura de xarxa o equips de comunicacions, per al seu enduriment de seguretat i practiques recomanades de configuració.
- La solució ha de proporcionar auditoria de paquets antivirus específics per: instal·lació, ultimes actualitzacions i l'estat d'arrencada del producte.
- La solució ha de proporcionar verificació de la informació d'identificació personal (PII) i altres continguts sensibles o sensitius.
- La solució ha de permetre que les plantilles utilitzades amb polítiques d'auditoria puguin ser personalitzables segons les necessitats específiques de l'organització. On es puguin definir controls interns per a sistemes de TU.
- La solució ha de ser validada per a NIST SCAP 1,2.
- La solució ha de ser capaç d'executar auditories de compliment dels controls esmentats en els DISA STIG del Departament de Defensa.
- La solució ha de facilitar l'automatització completa d'escaneig, informes i alertes.
- La solució ha de proporcionar vistes separades per a vulnerabilitats actives, passivament descobertes, associades a compliment i risc en dispositius mòbils.
- El descobriment de dispositius mòbils, no ha de dependre d'agents instal·lats en els dispositius, ni en sistemes de gestió com els MDM.

- La solució ha d'agregar els resultats de les exploracions individuals en vistes de vulnerabilitat acumulatius amb el filtrat i anàlisi per a permetre capacitats de desglossament i pivot.
- La solució ha de tenir vistes separades de vulnerabilitats actives i mitigades amb la migració automàtica de vulnerabilitats d'actiu a mitigat una vegada una anàlisi determina que la vulnerabilitat ja no és present.
- La solució ha de tenir la capacitat per a marcar una vulnerabilitat per haver estat mitigat amb anterioritat, però que ha aparegut de nou com podria ocórrer quan un sistema es restaura a partir de còpia de seguretat o una vella còpia d'una màquina virtual es torna a connectar.
- La solució ha de proporcionar un filtre ampli dels resultats de vulnerabilitat agregada amb capacitats de desglossament. Entre aquests es pot considerar si la vulnerabilitat és fàcil de comprometre, o si és present un "exploit", en eines per a fer proves de validació.
- La solució ha de proporcionar vistes de remediació que es prioritzen i siguin simplificades per a l'audiència de manera automàtica.
- La solució ha de proporcionar la possibilitat als usuaris autoritzats a executar exploracions de remediació individuals per a verificar vulnerabilitats s'han abordat correctament.
- La solució ha de proporcionar la capacitat d'automàticament agrupar objectius, utilitzant els resultats de l'anàlisi per a generar llistes d'actius dinàmiques.
- La solució ha de permetre a un usuari a acceptar el risc (fer una excepció) amb dates de caducitat configurables per una vulnerabilitat detectada, o a la exempció de risc (canviar els nivells de gravetat) a un nivell que no sigui el que el venedor ha definit perquè aquesta vulnerabilitat.
- La solució ha de proporcionar funcionalitat de tiquets de remediació integrada, que també pot enviar entrades als sistemes de 3a parts o altres fabricants.
- La solució ha de ser compatible amb l'assignació de tiquets als usuaris individualment.
- La solució ha de proporcionar capacitats d'alerta activada per vulnerabilitats i esdeveniments en diferents sistemes d'infraestructura.
- La solució ha d'admetre la definició d'alertes basades en l'anàlisi de vulnerabilitats o els resultats de l'auditoria de configuració.
- Les accions d'alerta han d'incloure: correu electrònic, creació i assignació d'un tiquet, inici d'un escaneig, generació d'un esdeveniment syslog i generació automàtica d'informes o reportis.

Requisits sobre condicions d'ús

- La solució ha de ser compatible amb la generació d'informes o reportis personalitzables ja sigui utilitzant plantilles subministrades pel venedor o sense plantilles.
- La solució ha de proporcionar la capacitat de filtrar els resultats en la presentació d'informes per una varietat de criteris per a incloure llistes d'o grups d'actius, repositoris, adreces d'IP, tipus de vulnerabilitat, text sense format, i els camps de dates.
- La solució ha de proporcionar informes integrats d'exploració, anàlisi de configuració, i de registres.
- La solució ha de proporcionar, en la capacitat de la presentació d'informes, automatitzar completament per a incloure l'execució programada i el lliurament d'informe posterior a l'exploració.

- La solució ha de proporcionar la capacitat de produir informes ad hoc durant la visualització dels resultats en la consola. Les exportacions de PDF i CSV estaran disponibles.
- La solució ha de ser compatible amb la capacitat de produir informes en els següents formats de reporti: PDF, CSV, XML
- La solució ha de proporcionar tendències adaptables dels resultats de l'anàlisi en informes amb resultats filtrats per a definir múltiples línies de tendència en un sol component gràfic.
- La solució ha de proporcionar taules de matriu que resumeixen els números a través de molts conjunts filtrades de resultats.
- La solució ha de proporcionar una alimentació automatitzada d'informes de plantilles per als temes de seguretat i compliment.
- La solució ha de proporcionar els informes de compliment normatiu, sense cost addicional. Això a incloure CIS, ISO2700, i PCI DSS entre altres.
- Els informes han de tenir la possibilitat d'incloure els noms de host (NetBIOS, DNS), juntament amb les adreces IP com a mínim.
- La solució ha de proporcionar la capacitat de xifrar i protegir amb contrasenya els informes generats de manera automàtica, abans de ser enviats per correu electrònic.
- La solució ha de proporcionar la capacitat de correu electrònic de manera automàtica per a reportis.
- La solució ha de proporcionar la capacitat d'empènyer informes que utilitzen els serveis de publicació web.
- La solució ha de permetre importació d'imatges personalitzades per a ser incloses en la personalització de reportis.
- La solució ha de proporcionar qualificacions d'alt nivell que mostri la maduris de les mètriques de seguretat i compliment.
- Les mètriques de seguretat han d'estar basades en normatives de seguretat com: PCI, ISO27000, NIST, CIS CSC, entre altres.
- Els controls definits dins de les mètriques de seguretat han de ser personalitzables, podent modificar punts de control, percentatges de compliment, rang d'equips o IPs a avaluar, etc.
- La solució ha d'incloure elements gràfics i panells de control personalitzables, llestos per a la visualització de les vulnerabilitats i l'estat de l'entorn avaluat.
- La solució ha de proporcionar tendències adaptables dels resultats de l'anàlisi en quadres de comandament, utilitzant resultats filtrats per a definir múltiples línies de tendència en un sol component gràfic.
- La solució ha de permetre que cada usuari defineixi en el seu perfil, múltiples quadres de comandament específics de l'usuari.
- Els elements del tauler del Dashboard han de ser totalment personalitzables mitjançant el filtrat, per a mostrar les dades sobre la base de la llista d'actius, vulnerabilitat o de control de la conformitat, el temps, la paraula clau de cerca, adreça IP, etc.
- Els quadres de comandament d'actualització de les dades han de ser configurable per a actualitzar en forma programada i ad hoc.
- La solució ha de proporcionar la capacitat d'importar / exportar les plantilles i presentació d'informes.
- La solució ha de proporcionar la capacitat de compartir les plantilles i presentació d'informes amb altres usuaris de la mateixa empresa.
- La solució ha de proporcionar la capacitat per a definir diversos elements visuals per a panells personalitzats a incloure gràfics "peu charts", gràfics de barres, matriu, i de tendències.

- La solució ha d'incloure un catalogo amb panells o Dashboards que es presentin com a plantilles exemple, i que siguin alineades entorn de diferents audiències, normes de compliment i els controls de seguretat.
- La solució ha d'adaptar-se a les opcions de disseny i format personalitzables per a panells o Dashboards.
- La solució ha de tenir capacitat d'integrar-se de manera nativa amb els principals fabricants de seguretat, comptant amb integracions tant en tecnologies SIEM, patching, ticketing, SOAR, etc.
- Les integracions que es realitzin mitjançant un connector desenvolupament pel fabricant responsable del servei no podran tenir cost.
- Haurà d'existir una API oberta i completament documentada per si cal desenvolupar codi per a la integració amb altres fabricants o serveis.

Model de llicenciat

El model de llicenciat ha de garantir la disponibilitat de totes les funcionalitats del programari implantat, obtenint un preu llicència/any establert, les xifres orientatives son:

- Llicències (600)

A més, ha de garantir el següent:

- El llicenciament estàndard de la solució ha d'incloure els següents components, sense la necessitat de llicenciar-se de manera addicional
  - Scanner Actiu
  - Funcions de Compliment
  - Agents
  - Dashboards i Reportis
  - API
- Ha de ser opcional afegir en la mateixa arquitectura scanner passius per a anàlisis de trànsit de xarxa en temps real.
- El llicenciament estàndard no ha de fer diferència si les direccions IPs considerades són públiques o privades.
- El llicenciament estàndard ha de permetre implementar múltiples Scanners i Agents sense cost addicional per cadascun d'ells.
- El llicenciament estàndard ha d'incloure la funcionalitat de normalització de logs.
- Quan s'analitzi un aplicatiu Web, la unitat de llicenciament haurà de ser el FQDN, incloent en la mateixa llicència tots els subdominis.

5.3. Garantia dels treballs

La implantació de la nova eina de gestió de vulnerabilitats haurà de contemplar una garantia de correcte funcionament de 3 mesos comptats a partir de la data de posada en explotació. Durant aquest període, s'han de resoldre satisfactòriament totes aquelles incidències o defectes detectats en el procés d'implantació imputades a ell per acció o per omissió.

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'acta d´inici.

Quant al dimensionament del volum d'hores requerides, s'estima un total de **400 hores de treball.** Aquesta estimació d'hores inclou totes les activitats descrites l'apartat de "Requisits del servei", contemplant els diferents perfils de professionals que siguin necessaris.

El volum d'hores indicat es el màxim contractat per **vint-i-quatre (24)** mesos. ATL, d'acord amb les seves necessitats, farà les seves sol·licituds al adjudicatari consumint d'aquestes 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 gestió de vulnerabilitats.

Igualment, l'adjudicatari designarà almenys un responsable del contracte (pot ser el 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 o 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 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 5 anys com a cap/responsable en projectes i serveis objectes del plec.

Tècnic de seguretat

Les responsabilitat del tècnic, inclou, entre d'altres:

- Anàlisi dels requeriments i necessitats que es plantegin en el contracte.
- Tasques d'operació, implementació solucions i noves configuracions
- 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 en l'execució de tasques tècniques, projectes tècnics i/o serveis tècnics de gestió de vulnerabilitats.
- Certificació: Ha de disposar de la certificació tècnica vigent del software proposat pel licitador, emesa pel propi fabricant.

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 garanteix un compromís del proveïdor amb el projecte.

Els ANS hauran de considerar 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.

Els ANS que seran d'aplicació son els següents:

	Acords de nivell de servei	**Acords de nivell de servei (ANS): descripció**	**Compromís**
ANS 1	Terminis d'execució	Incompliment dels lliurables segons les fites marcades en la planificació de cadascuna de les fases del projecte	< 10 dies
ANS 2	Qualitat de les proves	Incidències recurrents al llarg de tot el projecte d'implantació una vegada completades les proves i que haurien d'haver estat identificades i resoltes convenient.	< 10% del total d'incidències.
ANS 3	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'avís i que la incidència està resolta o, cas que sigui complexa, es doni una solució pal·liativa provisional.	< 24h
ANS 4	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
ANS 5	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 6	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

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 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

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 63.066,41 € IVA Inclòs (52.121,00 € IVA exclòs). Respecte el pressupost del contracte, que distribuït segons la següent distribució pressupostària:

Concepte	2026	2027	2028	Import Total (IVA Exclòs)	IVA 21%	Total Pressupost (IVA Inclòs)
Servei Gestió de vulnerabilitats *(Gestor del servei i Tècnic de seguretat)*	6.000,00 €	12.000,00 €	6.000,00 €	24.000,00 €	5.040,00 €	29.040,00 €
Adquisició Eina 2 anys	28.121,00 €	0,00 €	0,00 €	28.121,00 €	5.905,41 €	34.026,41 €
Total	***34.121,00 €***	***12.000,00 €***	***6.000,00 €***	***52.121,00 €***	***10.945,41 €***	***63.066,41 €***

24.000 €/ 400 hores = 60 €/hora (sense IVA)

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 acordar 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 llicenciament necessari per dur a terme el servei al llarg del contracte, es realitzarà en un únic pagament el primer mes de facturació.

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