PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS

PER A LA CONTRACTACIÓ DEL

"Subministrament, instal·lació d'equipament, manteniment i segmentació de la xarxa de seguretat IT-OT"

Setembre 2024

INDEX

1. OBJECTE DEL PLEC

Aquest document constitueix el Plec de Prescripcions Tècniques (PPT) que regeix el procediment de contractació i execució del "**Subministrament, instal·lació d'equipament i manteniment de la xarxa de seguretat IT-OT**", promogut per l'Ens d'Abastament d'Aigua Ter-Llobregat (ATL).

2. INTRODUCCIÓ

2.1. Antecedents ATL

L'**Ens d'Abastament d'Aigua Ter-Llobregat** (ATL d'ara en endavant) és una entitat de dret públic participada 100% per l'Administració de la Generalitat de Catalunya, creada pel **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 (DOGC 19.07.2018).

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 que té per objecte la prestació del servei públic d'abastament d'aigua potable per a l'abastament de poblacions mitjançant la xarxa Ter-Llobregat.

2.2. Objectiu i missió d'ATL

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

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

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

La xarxa de distribució que gestiona ATL té més de 1000 quilòmetres de canonades, més de 60 estacions de bombament. Per a produir l'aigua, ATL disposa de quatre infraestructures principals: quatre estacions de tractament d'aigua potable i dues

plantes dessalinitzadores. Quant a capital humà, ATL compta amb una plantilla de més de 250 professionals.

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

Entre aquests mitjans, les tecnologies d'informació i comunicacions han esdevingut una eina clau a qualsevol empresa per complir els seus objectius amb excel·lència, contant amb la necessitat d'una evolució i adaptació continua d'aquestes aplicacions als nous canvis i evolucions de l'entitat. I en aquest cas, destaquem la necessitat de garantir la disponibilitat de la xarxa de comunicacions d'ATL.

Consegüentment amb tot això, ATL publica aquest plec per a contractar el "**Subministrament, instal·lació d'equipament i manteniment de la xarxa de seguretat IT-OT".**

3. ABAST DEL CONTRACTE

L'abast del contracte contempla la renovació de la xarxa de seguretat IT/OT d'ATL amb l'objectiu de securitzar i segmentar la xarxa d'ATL i consisteix en el servei i subministrament, instal·lació, i suport a la configuració i manteniment de la nova solució, complint els requeriments tècnics i condicions que garanteixin:

- ❏ L'adquisició del material necessari i suport a la configuració necessària dels mateixos per a la seva integració amb la xarxa d'ATL i segmentació de les xarxes.
- ❏ Manteniment i suport associats a l'equipament adquirit, que asseguri els nivells de servei i seguretat en les millors condicions i la major qualitat.
- ❏ Un model de relació que permeti disposar d'unes eines de gestió i d'uns mecanismes de control i seguiment.

4. SITUACIÓ ACTUAL

Les infraestructures de xarxa suposen un element indispensable dins de la corporació ja que entre d'altres, permeten la connectivitat dels actius (PLCs, sistemes, càmeres de videovigilància,...), així com serveis crítics existents a les seus remotes.

ATL es troba en fase de redefinició de l'arquitectura de seguretat dels diferents entorns necessaris de la seva operativa diària.

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

- Adquirir els equipaments detallats en el **punt 5.1 d'aquest document**

ATL té set centres de treball, cadascun dels quals disposa d'una xarxa local. Aquestes seus es comuniquen entre elles formant, juntament amb la xarxa d'estacions remotes, el que s'anomena la WAN d'ATL.

Es disposa d'un Centre de Processament de Dades per a cadascuna de les seus principals. S'està segmentant la xarxa IT a cada seu (mitjançant VLANs), respecte el Control d'Accés a la Xarxa, es disposa d'un sistema NAC basat en tecnologia CISCO on es gestiona l'accés a la xarxa. ATL disposa d'una xarxa de Fibra Òptica (F.O.) pròpia, principalment per connectar els edificis centrals de les diferents seus amb la resta dels edificis annexes dins del mateix "campus".

A més, actualment ATL disposa de més de 250 seus remotes. Es tracta de seus menors, ubicades generalment fora del rang d'accés a la xarxa cablejada del operadors.

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 fan utilitzant una aplicació ITSM (EasyVista).

La gestió del suport i manteniment de xarxes d'ATL es realitzarà sobre el seu propi parc d'equipaments i programari.

5. CARACTERÍSTIQUES TÈCNIQUES

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

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

1. Adquisició, instal·lació, segmentació i configuració dels nous/actuals equipaments de xarxa segons les directrius del equip intern d'ATL
2. Serveis de manteniment i explotació d'aquests elements conjuntament amb l'equip intern d'ATL

5.1. Adquisició, instal·lació i configuració de nous equipaments de xarxa

Aquest contracte preveu el servei i subministrament de tallafocs que permetin:

- Un aïllament i segmentació òptims dels diferents entorns existents (IT/OT) de la xarxa d'ATL.
- Una integració òptima amb la resta d'elements ja existents a la xarxa ATL, la qual està basada en tecnologia CISCO pel que fa a l'accés i en tecnologia Fortinet pel que fa a les comunicacions entre les diferents seus. En particular les eines actualment en ús dels fabricats esmentats són FortiManager i FortiAnalyzer pel que fa a Fortinet, i DNA Center i CISCO ISE pel que fa a CISCO. L'abast del projecte ha d'incloure totes aquelles subscripcions

necessàries (detallades en l'escandall d'elements a adquirir a continuació) durant el termini de 3 anys així com les possibles ampliacions en el llicenciament dels elements ja existents per assegurar la integració òptima entre els nous elements i els preexistents.

La topologia de cada seu serà igual pel conjunt de centres de treball i haurà d'incloure 2 equipaments físics d'idèntiques característiques per assegurar l'alta disponibilitat a cadascuna de les seus per a cada un dels dos entorns: IT & OT.

Les característiques mínimes dels equips així com les subscripcions i llicències associades, les ha determinat l'equip intern d'ATL a través d'un estudi previ de les volumetries aproximades de cada seu:

HARDWARE:

Centre treball	*Caracteristiques similars*	*Equips*
Firewall Segmentació SJD	FortiGate 901G. Hardware plus FortiCare Premium and FortiGuard Enterprise Protection o similar	2
Firewall Segmentació CRD	FortiGate 401F. Hardware plus FortiCare Premium and FortiGuard Enterprise Protection o similar	2
Firewalls Segmentació ABR i PRT	FortiGate 121G. Hardware plus FortiCare Premium and FortiGuard Enterprise Protection o similar	4
Firewalls OT SJD, CRD, ABR i PRT	FortiGate 121G. Hardware plus FortiCare Premium and FortiGuard Enterprise Protection o similar	8
Cables DAC connexió firewalls (25G)	25 GE SFP28 passive direct attach cable 3m for systems with SFP28 slots. o similar	8
Cables DAC connexió firewalls (10G)	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots. o similar	48
TOTAL		***72***

Llicències/Bundles de seguretat

Ampliacions/Subscripcions	*Caracteristiques similars*	*Unitats*
Ampliació FortiManager (element ja existent)	Subscription license for 10 devices/vdoms managed by FortiManager VM S-series, including FortiCare Premium.	1
Ampliació FortiAnalyzer (IT) (element ja existent)	Subscription license for 50 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service.	1
Ampliació FortiAnalyzer (OT) (element ja existent)	OT Security Service for 50 GB/Day subscription including	1

	advanced OT analytics, risk and compliance reports, event handlers, and use-case correlation rules	
Subs OT Firewalls OT SJD, CRD, ABR i PRT	FortiGuard OT Security Service (OT dashboards and compliance reports, OT application and service detection, OT vulnerability correlation, OT virtual patching, OT signatures - Application Control and IPS rules) o similar en base al FW proposat	8
Subs OT Firewalls existents (TRD, LLC i PST)	FortiGuard OT Security Service (OT dashboards and compliance reports, OT application and service detection, OT vulnerability correlation, OT virtual patching, OT signatures - Application Control and IPS rules)	6
Subs IoT Firewalls existents (TRD, LLC i PST)	FortiGuard Attack Surface Security Service (Security, Compliance and Risk Ratings, IoT Detection and IoT Vulnerability Correlation)	18
Subs OT Firewalls existents Trinitat	FortiGuard OT Security Service (OT dashboards and compliance reports, OT application and service detection, OT vulnerability correlation, OT virtual patching, OT signatures - Application Control and IPS rules)	2
Subs IoT Firewalls existents Trinitat	FortiGuard Attack Surface Security Service (Security, Compliance and Risk Ratings, IoT Detection and IoT Vulnerability Correlation)	6
TOTAL		***43***

5.1.1. Adquisició equipament: requisits tècnics

L'equipament a subministrar haurà de complir els següents requeriments tècnics mínims, establerts en base a un estudi previ de les volumetries de tràfic actual a cada centre de treball.

Característiques generals

Descripció	FW segmentació SJD	FW segmentació CRD	FW Segmentació ABR/PRT
Firewall Throughput (1518 / 512 / 64 byte UDP)	164 / 163 / 153 Gbps	79.5 / 78.5 / 70 Gbps	39 / 39 / 28 Gbps

IPsec VPN Throughput (512 byte)	55 Gbps	55 Gbps	35 Gbps
IPS Throughput (Enterprise Mix)	26 Gbps	12 Gbps	5.3 Gbps
NGFW Throughput (Enterprise Mix)	22 Gbps	10 Gbps	3.1 Gbps
Threat Protection Throughput (Ent. Mix)	20 Gbps	9 Gbps	2.8 Gbps
Firewall Latency	3.78 / 2.5 µs	4.19 µs / 2.5 µs	3.17µs
Concurrent Sessions	16 Million	7.8 Million	3 Million
New Sessions/Sec	720.000	500.000	140.000
Firewall Policies	10.000	10.000	10.000
Max G/W to G/W IPSEC Tunnels	2.000	2.000	2.000
Max Client to G/W IPSEC Tunnels	5.000	5.000	16.000
SSL VPN Throughput	10 Gbps	3.6 Gbps	1.5 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10.000	5.000	500
SSL Inspection Throughput (IPS, avg. HTTPS)	16.7 Gbps	8 Gbps	3 Gbps
Application Control Throughput (HTTP 64K)	74.8 Gbps	28 Gbps	6.7 Gbps
Max APs (Total / Tunnel)	1 024 / 512	512 / 256	128 / 64
Max Switches	96	72	32
Max Tokens	5.000	5.000	5.000
Virtual Domains (Default / Max)	10 / 10	10 / 10	10 / 10
Interfaces	4x 25 GE SFP28, 4x 10 GE SFP+, 1x 2.5GE RJ45, 8 x GE SFP, 17x GE RJ45	8x 10GE SFP+ , 8x GE SFP, 18 x GE RJ45	4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP
Local Storage (SSD)	960 GB	960 GB	480 GB

- ❏ Equipament recollit a la Guia de Seguretat de les TIC (CCN-STIC 105) - https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-

publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file.html

- ❑ Gestió
  - La gestió és de fàcil ús i intuïtiva.
  - Capacitat de gestió dels equips mitjançant accés via web (https) i terminal (ssh) per la total configuració de les polítiques de seguretat de la plataforma.
  - Tots els canvis efectuats en els tallafocs son aplicats de forma immediata, sense necessitat de compilar o similar.
  - Creació de diferents tipus d'usuari per l'administració podent aplicar diferents rols o perfils, així com definir xarxes d'origen confiables. Permet la possibilitat de crear usuaris de tipus REST-API.
  - Suport de SNMP i sFlow.
  - Exportació de logs vía SYSLOG, FTP, SCP i TFTP.

- ❑ Networking
  - Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR.
  - Suport Dual Stack IPv4 e IPv6 simultàniament.
  - Network address translation NAT IPv4, NAT64 i NAT66.
  - DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.
  - 802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE).
  - 802.3ad Capacitat de crear enllaços LACP per l'agregació de ports.
  - Capacitat de balanceig de servidors a nivell 4 per tots els serveis, com també possibilitat de fer SSL off-loading pel tràfic HTTPS.
  - Suport d'VXLAN i VXLAN VTEP per l'extensió de xarxes de nivell 2 entre xarxes de nivell 3.
  - Funcionalitat integrada de Traffic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest Traffic Shaping ha de basar-se en aplicacions i URLs a nivell global de perfil o per Ip.

- ❑ Alta disponibilitat
  - La funcionalitat d'alta disponibilitat està disponible sense necessitat de llicencia.

- Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixt. El mode mixt implica poder tenir tallafocs virtuals actius i passius de forma barrejada, es a dir, el màster de certs tallafocs virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs es màster de la resta de tallafocs virtuals alhora.
- La transferència de servei d'un equip a l'altre sense talls, ni pèrdua de les connexions TCP, ni aturada de servei.
- Les configuracions es poden traspassar de manera automàtica entre els dos equips.
- Capacitat de funcionament en mode actiu/actiu sincronitzant sessions entre els dos nodes però mantenint adreçament IP diferenciat en les interfícies de cada node del clúster.

❑ VPN

- El dispositiu admet un mínim de 500 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.
- El sistema proposat compleix els estàndards de la indústria, sense el suport extern addicional de maquinari o mòduls: IPSEC VPN (IPv4 i IPv6), PPTP VPN, L2TP VPN, SSL VPN i GRE sobre IPSEC.
- El sistema suporta 2 modes de funcionament SSL VPN:
  - Sense client - Accés web: per a clients remots que només necessiten un navegador i no requereix la instal·lació de cap agent, per tal d'accedir via web a: HTTP / HTTPS Servidor intermediari, FTP, Telnet, SMB / CIFS, SSH, VNC i RDP.
  - Mode túnel: per a equips remots que executen una varietat d'aplicacions de client i servidor.

- Suport d'agregació de túnels VPN i balanceig per packet podent així afegir l'ampla de banda dels accessos VPN IPsec entre seus.
- Capacitat d'integració del mateix fabricant de doble factor d'autenticació via token mòbil, així com per SMS i correu electrònic, integrat en la mateixa plataforma de seguretat. Aquest token també s'ha de poder fer servir per l'accés a la GUI dels equips tallafocs.

Controladora d'accés segur integrada

- El sistema és capaç d'actuar com controladora de punts d'accés wireless així com de switches del mateix fabricant.
- La capacitat mínima de punts d'accés a gestionar ha de ser de 30, i de switchs de 16.
- La gestió dels APs i Switches es farà des de la mateixa interfície gràfica i CLI des de la qual es gestiona el Firewall.

SD-WAN

- Balanceig intel·ligent de connexions físiques i lògiques, indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
- Permet, com a mínim, com a connexions físiques i lògiques que es poden afegir a l'SD-WAN és de 256.
- Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols http, ping i TWANP. El numero de validacions és de com a mínim 100.
- Verificació de paràmetres de qualitat en temps real: jitter, packet loss i latència per línia.
- Configuració de polítiques de SD-WAN intel·ligent basat en origen (usuaris AD i direcció IP), en el destí (direcció IP, aplicacions i/o serveis d'Internet/aplicacions) i en la línia amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latència, tràfic de pujada/baixada o ampla de banda, així com una combinació per pesos.

Característiques Seguretat (amb subscripció)

- Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant els següents paràmetres de coincidència:
- Origen (totes les opcions):
- Capacitat de definir una i/o més d'una Interface d'origen, incloent "any". Així com també "zones".
- Capacitat d'utilitzar direccions ip, rangs i/o xarxes, FQDN, països, serveis d'internet i direccions ip's reconegudes com origen de xarxes TOR, proxies anònims (aquestes direccions han d'actualitzar-se

automàticament), així com els objectes exportats dels connectors esmentats a l'apartat de característiques generals de l'equip.

- Capacitat d'utilitzar usuaris/grups locals o AD.
- Capacitat per declarar horaris o "schedule" tant per dia/hora com a data màxima de venciment.
- Capacitat de selecció del servei a utilitzar.

❑ Destí:

- Capacitat de definir una i/o més d'una Interface de destí, incloent "any". Així com també "zones".
- Capacitat d'utilitzar direccions ip, rangs i/o xarxes, així com objectes FQDN, països i serveis d'internet.

❑ Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant la següent parametrització:

- Seleccionar quin tràfic s'analitzarà a nivell 4 i quin a nivell 7, per política, sense excepció.
- La configuració del NAT sortint s'ha de poder configurar dintre de cadascuna de les polítiques de seguretat, de forma granular.
- Les diferents funcionalitats de seguretat avançades de nivell 7 s'activaran de forma individual a nivell de política, mai a nivell global. A més aquestes es gestionaran amb perfils per tal de ser granulars en els permisos. Aquestes funcionalitats son: antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, i DLP.
- Decidir a nivell de política quin tràfic SSL serà desxifrat pel seu anàlisis i quin només a nivell de certificat.
- A nivell de logging, cal que la solució permeti activar el logging de només nivell 7, o tant de nivell 4 més nivell 7. Cal també fer captura de packets en la pròpia política.

❑ Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar llindars per serveis publicats on poder filtrar per direccions ip o països per: *ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, udp_flood, udp_scan, udp_src_session, udp_dst_session, icmp_flood, icmp_sweep, icmp_src_session,*

icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session i sctp_dst_session.

- ❑ Capacitat de definir polítiques a nivell d'Interface per tal de denegar tràfic i no ser processat per la política de seguretat global. S'han de poder utilitzar direccions IP's, països, així com rangs i xarxes ip com a origen.

- ❑ Per tal d'evitar l'accés de xarxes botnet, els tallafocs te una base de dades de reputació dinàmica que bloquegi els accessos a nivell d'Interface.

- ❑ Visualització del número d'usos i quantitat de tràfic de cada regla de seguretat, de forma àgil tant en la pròpia secció de polítiques de seguretat, això com també dintre de la configuració de cada política . També cal veure l'ultima vegada que se ha utilitzat.

Control d'aplicacions

- ❑ Capacitat per identificar un mínim de 1900 aplicacions actives actuals (incloent aplicacions web 2.0), com per exemple distingir Facebook, d'una sub-aplicació Facebook-chat o post.
- ❑ La solució classifica les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).
- ❑ Aplicar tècniques d'identificació d'aplicacions a tots els ports TCP / UDP i no només en els més comuns.
- ❑ Capacitat per identificar les aplicacions sota túnels HTTPS.
- ❑ Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat. Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

IPS

- ❑ Capacitat per protegir tant servidors com clients amb un mínim de 10000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior.

- ❏ Capacitat per identificar patrons d'atacs basats en comportament o rated-base, per tal de bloquejar intents d'atacs un cop superat el llindar d'ús en un temps determinat.
- ❏ Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

Antimalware

- ❏ Capacitat de detecció de malware (virus, grayware, worns, etc…) basat en firmes conegudes o mètodes avançats de detecció.
- ❏ Suport de sandboxing en el cloud, amb un tamany mínim de fitxer de 100 MB indistintament del tipus de fitxer.
- ❏ Capacitat per l'eliminació del contingut dinàmic (macros, javascript, URL) explotable dintre de documents ofimàtics i pdf, que es distribueixen per protocols SMTP, IMAP i http.
- ❏ Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejant mitjançant malware de repositoris externs de threat inteligence.

Webfilter

- ❏ Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar: block, monitor i aplicació de quotes de temps o tràfic per categoria.
- ❏ Suport de protocols http v1.0, 1.1 i 1.2.
- ❏ La base de dades de categories web caldrà consumir-se com un servei cloud en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les URL's el més actualitzat possible.
- ❏ Suport per restringir l'accés a Youtube i Google en mode "safe search".
- ❏ Suport de rating per imatges per URL.
- ❏ Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia.

Altres funcionalitats de nivell 7

- ❏ Altres funcionalitats de nivell 7 que la proposta ha d'incloure son:
  - DLP.
  - DNS Filter.

- ICAP.
- Web application firewall.

Funcionalitats IoT

- ❏ Servei IoT Detection ajuda a reduir significativament la superfície d'atac en descobrir, identificar i protegir els dispositius d'Internet de les coses (IoT) presents a la xarxa. El servei inclou una biblioteca local (instal·lada) de dispositius d'IoT que s'amplia i s'actualitza regularment (actualment amb una biblioteca superior a 565.000.000 de dispositius IoT descoberts i identificats). Mentrestant, el servei utilitza un conjunt ric de firmes de vulnerabilitat IPS d'IoT, desenvolupades i seleccionades per detectar i bloquejar possibles amenaces cibernètiques dirigides a dispositius d'IoT.

Funcionalitats OT

- ❏ El servei de seguretat industrial proporciona firmes especialitzades del sistema de prevenció d'intrusions (IPS) per detectar i bloquejar el trànsit maliciós que amenaça aplicacions i dispositius en entorns de fabricació, plantes, seguretat i altres entorns de tecnologia operativa (OT) (actualment amb més de 3.100 regles de protocols específiques, més de 690 regles IPS específiques, més de 1.090 regles de virtual patching específiques i més de 980 regles de detecció d'aplicacions específiques). En combinació amb FortiGate NGFW, el trànsit de xarxa maliciós és bloquejat abans que els perpetradors que busquen controlar o interrompre les operacions puguin causar danys. A més, el servei pot actuar com un pegat virtual per proporcionar protecció de seguretat immediata fins que el proveïdor pugui desenvolupar i implementar un pegat. Protocols i firmes suportats:
- ❏ Allen-Bradley DF1, Allen-Bradley PCCC, BACnet, CC-Link, CN/IP CEA-852, CoAP, Common Industrial Protocol (CIP), DICOM, Digi ADDP, Digi RealPort (Net C/X), Direct Message Profile, DNP3, ECHONET Lite, ECOM100, ELCOM 90, Emerson DeltaV, Ether-S-Bus, Ether-S-I/O, EtherCAT, Ethernet POWERLINK, EtherNet/IP, FactorySuite NMXSVC, FL-net, GE EGD, GE SRTP (GE Fanuc), HART-IP, HL7, IEC 60870-5-104 (IEC 104) , IEC 60870-6/TASE.2 (ICCP), IEC 61850 MMS, IEC 62056 DLMS/COSEM, IEC TR 61850-90-5 R-GOOSE, IEC TR 61850-90-5 R-SV, IEEE 1278.2 DIS, IEEE C37.118 Synchrophasor, ISO 9506 MMS, KNXnet/IP (EIBnet/IP), LonTalk

IEC14908-1 CNP, Mitsubishi MELSEC, Modbus TCP, Moxa Modbus RTU, , Moxa UDP Device Discovery, MQTT, MTConnect, Niagara Fox, oBIX, OCPP, Omron FINS, OPC AE, OPC DA, OPC HDA, OPC UA, OpenADR, OSIsoft PI, Profinet CBA, Profinet IO, RealPort DNP3, Remote Operations Controller (ROC), Rockwell FactoryTalk, RTPS, SafetyNET p, Schneider UMAS, Siemens LOGO, Siemens S7, Siemens S7 1200, Siemens S7 Plus, Siemens SIMATIC CAMP, STANAG 4406 Military Messaging, STANAG 506, Triconex TriStation, Veeder-Root ATG Access, Vnet/IP. Entre molts d'altres.

❑ 5.1.2. Serveis de disseny de l'arquitectura de xarxa, configuració i integració

Aquest contracte preveu la instal·lació i configuració necessària per establir una arquitectura segura, segons les directrius que es donaran des de l'equip intern d'ATL. A mode de resum, les directrius seguiran les següents línies mestre:

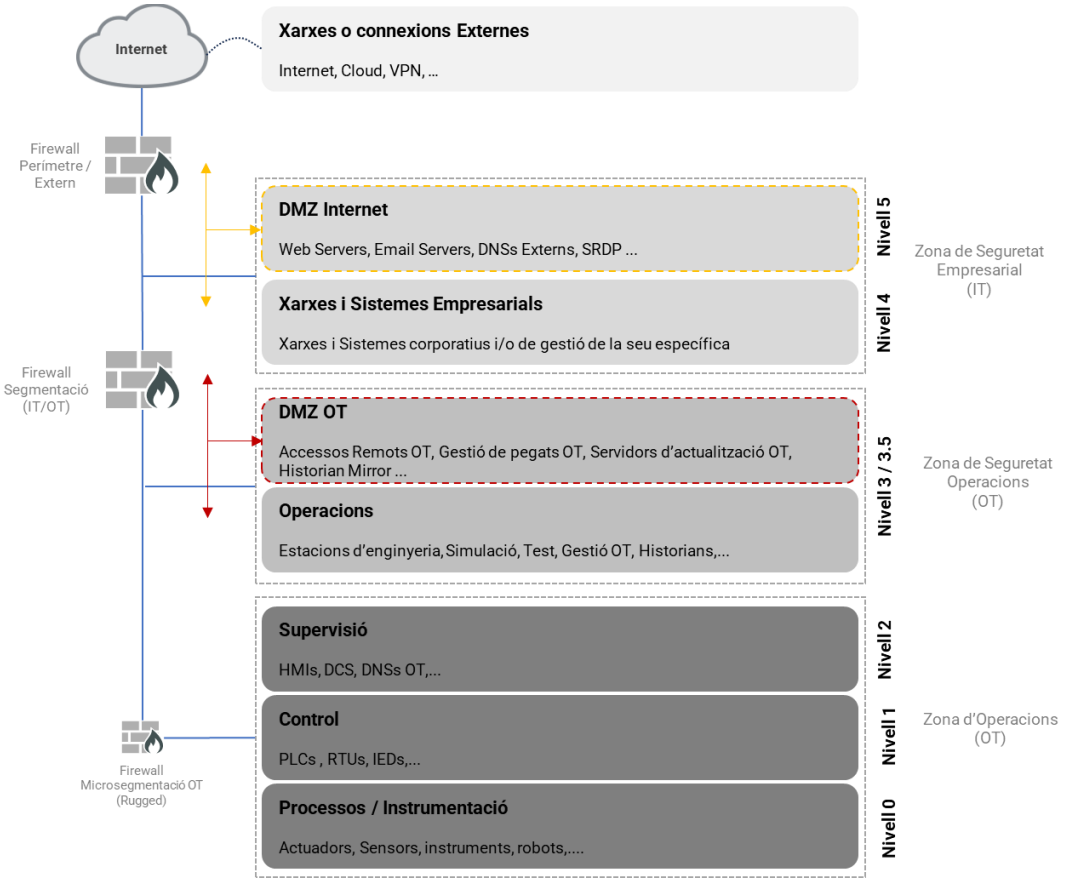
1. Separar la xarxa IT i OT tenint en compte la següent metodologia que es basa en el compliment de les següents normatives i estàndards:
    a. Esquema Nacional de Seguretat nivell alt (ENS) i NIS2
    b. ISO/IEC 27001
    c. IEC 62443
    d. ANSI/ISA-95/99, Model Purdue
    e. Guies bones pràctiques i *papers* de fabricants i organitzacions rellevants (ex. MITRE, NIST,...) en l'àmbit de la ciberseguretat i xarxes (específicament per a la segmentació i control d'accés a xarxes (IT i OT).
2. Acabar de segmentar la xarxa IT de la resta d'entorns existent a la xarxa d'ATL (on es troben elements OT i IoT)

3. Protegir i segmentar la xarxa OT seguint el model Purdue, NIST SP800-82, IEC 62443 i el model de referència SANS ICS410 que fan molt èmfasi en la segmentació de la xarxa i el control de la comunicació entre segments i/o zones, per tal de contenir dins d'una mateixa zona en cas d'infecció a través de 5 nivells.

    a. Separar els plans d'encaminament de la xarxa IT i OT, tant a nivell dels Routers principals de les seus, com sobre la xarxa SD-WAN.

    b. Separar els equips de comunicacions segons l'àmbit del servei (IT o OT).

A mode d'exemple es desitja implementar una arquitectura similar a la següent:



A més es preveuen les tasques següents:

- Aplicar els mecanismes de seguretat específics en els mateixos tallafocs on s'implementarà la segmentació, mitjançant polítiques que s'evolucionaran durant el transcurs del projecte, així com posteriorment a càrrec d'ATL o el proveïdor que proporcioni el servei, com poden ser:
    - Serveis IPS tant per IT com específics per OT.
    - Protecció anti-malware, antivirus, Botnets, CDR.
    - Servei Sandbox.
    - Filtratge DNS.
    - Servei de prevenció de Malware inline basat en IA.
    - Control i filtratge basat en aplicacions
    - Polítiques GeoIP
    - Inline CASB
    - Serveis específics per a OT:
        - Virtual Patching
        - Detecció de dispositius i protocols OT
        - Correlació de vulnerabilitats OT
        - Signatures OT (per a IPS)
    - Serveis específics per a IoT:

        - Virtual Patching
        - Detecció de dispositius IoT
        - Correlació de vulnerabilitats IoT
    - Signatures IoT (per a IPS)

- Visites de replanteig de cablejat.

- Instal·lació del cablejat necessari entre els elements d'un mateix CPD.

- Instal·lació i configuració de la nova infraestructura amb l'actualització del firmware a les últimes versions (segons indiquin les matrius de compatibilitat al moment de l'entrega).

- Configuració de les regles necessàries als tallafocs.

- Instal·lació i configuració de l'eina central de monitoratge, configuració i orquestració del sistema.

- Instal·lació i configuració de l'eina central d'analítiques i enregistrament de logs.

- Definició i implementació dels indicadors de qualitat del servei (QoS, consum ample de banda, latències, rendiment,...)

- Establiment d'un model base de funcionament ordinari del sistema per tal d'identificar les alertes que facilitin la gestió del servei així com de la seguretat.

- Integració òptima amb la xarxa actual d'ATL, contemplant tots els escenaris corresponents d'interconnexió amb xarxes de tercers.

- Realització de les proves de contingència i rendiment per validar l'operativa del servei d'interconnexió instal·lat.

- Interconnexió amb altres elements de xarxa existents.

- Formació in-situ sobre la solució tecnològica implantada per personal amb experiència sobre l'entorn desplegat.

- Creació de la documentació del projecte.

- Definit el model de gestió de relació amb tercers, per gestió d'incidències, canvis i/o evolutius.

- Serveis de suport físic i remots dels problemes que puguin sorgir durant el període de garantia.

Les tasques d'instal·lació es realitzaran a l'hora designada per ATL en funció de l'afectació als serveis. Com a requeriment serà necessari deixar el cablejat correctament pentinat i etiquetat al rack on es faci la instal·lació.

La solució implementada ha de quedar certificada pel proveïdor i/o fabricant tant en la part de software com en la de hardware.

5.2. Servei de manteniment i explotació post posta en marxa

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

Manteniment correctiu

Cobrir totes les tasques necessàries per diagnosticar i resoldre les incidències vinculades a tota la infraestructura de segmentació implementades i operatives en el moment del contracte. El SLA establert per aquest servei es de 24x7x4h.
Tasques destacar:

- Resoldre incidències de mal funcionament, configuració errònia o averia d'equips
- Utilitzar les eines de gestió i seguiment establerts a ATL i mantenir la informació actualitzada a nivell mensual.
- Quan les accions correctives impliquin un impacte important quant a esforços i temps, el proveïdor haurà de plantejar solucions parcials o temporals que puguin resoldre momentàniament necessitats urgents del negoci.
- Les tasques hauran de ser remotes per tal de mitigar l'incident en el menor temps possible, i presencial en el cas que així ho requereixi com pot ser incomunicació d'una seu o averia d'equips o components.
- Gestió d'incident amb el fabricant, ja sigui via tiquet (cas), telèfon...per tal de resoldre incidents software o hardware.

L'adjudicatari facilitarà el primer nivell de diagnòstic (connectivitat d'elements, comprovació de connectors, comprovació de fuetons...). S'inclou la substitució de connectors i fuetons sempre que es detecti que sigui necessari. En cas de detectar problemes amb el cablejat i/o fibres òptiques el licitador serà l'encarregat de resoldré el problema realitzant les tasques adequades (reparació).

La gestió d'incidents es realitzarà de forma remota, en cas de no ser possible, els tècnics s'hauran de desplaçar als centres de treballs per fer actuacions "in situ".

L'horari de cobertura del servei de suport per incidències crítiques (apartat 5.8 Acords de nivell de servei) serà de 0 a 24h de forma ininterrompuda de dilluns a diumenge tots els dies de l'any.

Monitorització:
Monitorització de la infraestructura, seguiment d'alarmes per tal de prevenir incidències o atendre incidències de forma proactiva.
El SLA establert per aquest servei es de 24x7.

Manteniment preventiu

Cobrir totes les tasques necessàries per diagnosticar i resoldre les incidències vinculades a tota la infraestructura de segmentació implementades i operatives en el moment del contracte. El SLA establert per aquest servei es realitzarà mitjançant planificació de les tasques entre el proveïdor (Service Manager) i ATL.
Tasques destacar:

- Actualitzacions crítiques de firmware (minor i major) per a resolució de vulnerabilitats o avançar possibles mal funcionaments.
- Revisions semestrals:
  - regles i polítiques capa 4/7
  - regles i polítiques (IDS / IPS)
- Revisions trimestrals:
  - Estat global equips i accions correctores
- Administrar i configurar llicències
- Administrar connexions d'usuari
- Gestió de còpies de seguretat de les configuracions i pla de restauració.
- Assegurar un rendiment correcte de funcionament dels entorns
- Manteniment i gestió de l'inventari de les garanties de tots els equips inclosos en el contracte.

Administració (peticions)

Servei que té com a principal objectiu la gestió i implementació de canvis a través de peticions. Aquest servei permet delegar per part de ATL l'execució dels canvis necessaris per al correcta funcionament.
Tasques a destacar:

- Revisió de configuracions realitzades per ATL
- Resolució de dubtes de configuració
- Configuració LAN: IP, Ports, VLANs, ACLs …
- Configuració Firewalls: configuració VPNs, revisions polítiques per a implementació de nous serveis ATL, revisions alertes menors.
- Supervisió estat equips / serveis en cas de tall elèctric planificat (o no).
- En general, configuracions o canvis sobre l'entorn gestionat, que requereixi canvis d'abast petit. No inclou nous projectes o configuració de noves funcionalitats d'equips o serveis existents que requereixin una reconfiguració parcial o total.

  - **Eines associades al servei:**
    - Eina de tiqueting (EasyVista)
    - Observium
    - SIEM
    - FortiManager
    - FortiAnalyzer
    - Nagios

Gestió i control de la qualitat

Dins d'aquest àmbit es contemplen les activitats que han de garantir la qualitat del servei i de les solucions lliurades. Entre aquestes activitats destaquen la definició i execució dels plans de proves, la formació i gestió del canvi, la gestió del coneixement i actualització de bases documentals i l'establiment de mecanismes per l'avaluació del servei.

Gestió del servei

L'adjudicatari serà responsable de realitzar una correcta gestió del contracte i del servei prestat a ATL, gestionant l'equip de equip de treball assignat, fent el seguiment d'activitats i garantint l'acompliment de la qualitat i nivells de servei compromesos.

Tasques a destacar:

- Gestió de l'equip propi de treball.
- Planificar tasques per garantir un correcte acompliment del servei.
- Seguiment dels nivells de servei acordats.
- Gestió de riscos i plans de mitigació.
- Revisió de possibles desviaments i definició de plans d'actuació.
- Establir i seguir el model de govern del servei (reunions periòdiques, informes seguiment mensuals).
- Utilitzar les eines de gestió i seguiment de peticions establerts a ATL i mantenir la informació actualitzada.

Activitats documentals

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

- Esquemes de xarxa, configuració, instruccions operatives, etc.
- Informes de seguiment

5.3. Productes a lliurar

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

Productes / serveis

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

Documentació

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

5.4. Garantia de l'equipament

- Garantia equipament: 3 anys Next business day (NBD).

5.5. Durada i etapes del servei mixt

La durada d'aquest contracte és de quaranta-vuit (48) mesos a comptar des de l'acta d´inici. Tenint en compte que els primers 12 mesos corresponen a l'adquisició i desplegament del equipament i els 36 posteriors corresponen a l'explotació i manteniment del servei gestionat.

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

Les dues fases identificades són les següents:

1. Adquisició, configuració i instal·lació de nous equipaments/actuals de xarxa amb una durada de 12 mesos (inclou període d'aprovisionament). Dintre d'aquests 12 mesos s'estableix com a termini de lliurament d'equipament un màxim de 3 mesos.
2. Manteniment servei amb una durada de 36 mesos posteriors a la primera fase indicada anteriorment.

L'adjudicatari haurà de garantir un horari de cobertura d'atenció de 24X7 per les incidències crítiques segons especificacions de l'apartat 5.8 Acords de nivell de servei.

5.6. 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.

5.7. Equip de treball

L'adjudicatari haurà de destinar per l'execució del servei els professionals adequats amb coneixements i experiència en l'execució de projectes i manteniment de xarxa.

Igualment, el licitador designarà un responsable del contracte (podrà recaure aquesta figura en la del 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 3 perfils o rols, que son:

Cap de projecte:

Les responsabilitats del Cap de projecte seran:

- Gestió global el projecte.
- Planificació, coordinació i supervisió del projecte.
- Definició i execució del pla de comunicació amb ATL.

Es requereix:

- Titulació d'enginyer superior de telecomunicacions o similar.
- Una experiència mínima de 5 anys en gestió de projectes d'entorns de xarxa IT/OT.

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.

Es requereix:

- Titulació d'enginyer superior de telecomunicacions o similar.
- Una experiència mínima de 5 anys en gestió de serveis de suport i manteniment d'entorns de xarxa IT/OT.

Arquitecte de xarxa IT/OT (nivell 3)

Les responsabilitats de l'arquitecte seran:

- Identificació millores i propostes de disseny de l'arquitectura de la xarxa de comunicacions.
- Garantir el nivell de servei, dissenyar criteris de monitorització i criteris de control dels serveis prestats.
- Suport a l'evolució de la xarxa per donar resposta a les noves necessitats i als resultats de la monitorització.

Es requereix:

- Titulació d'enginyer superior de telecomunicacions o similar.
- Una experiència mínima de 5 anys en gestió de serveis de suport i manteniment d'entorns de xarxa IT/OT.
- Certificació oficial del fabricant proposat.

Tècnic de xarxa IT/OT(nivell 2)

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

- Tasques d'operació, implementació solucions i noves configuracions.
- Desplaçament a seus ATL.
- 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:

- Titulació d'enginyer superior de telecomunicacions o similar
- Una experiència mínima de 3 anys en suport i manteniment d'entorns de xarxa IT/OT.
- Certificació oficial del fabricant proposat.

5.8. 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.

5.9. Acords de Nivell de Servei (ANS) i penalitzacions

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:

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

S'han establert dos agrupacions segons la fase del contracte (projecte o manteniment) reflectits a les següents taules:

ANS DE PROJECTE

ANS	Acord de nivell de servei	Descripció	Compromís
ANS-P1	Terminis d'execució	Incompliment dels lliurables segons les fites marcades en la planificació de cadascuna de les fases del projecte	< 10 dies
ANS-P2	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 DE MANTENIMENT

	Acords de nivell de servei	Acords de nivell de servei (ANS): descripció	Compromís
ANS 1	Temps màxim de resposta a la comunicació d'incidències	Temps màxim de resposta conforme s'ha creat la incidència i s'ha donat la corresponent confirmació de rebuda.	< 1h
ANS 2	Temps d'inici de resolució incidències critiques	Temps des de la comunicació de la sol·licitud d'incidència, fins que l'equip de suport es trobi en disposició de resoldre-la.	< 4h
ANS 3	Temps d'inici de resolució incidències no critiques	Temps des de la comunicació de la sol·licitud d'incidència, fins que l'equip de suport es trobi en disposició de resoldre-la.	NBD

ANS 4	Temps màxim de resolució d'incidències critiques	Temps màxim de resolució, per a corregir i implementar una solució correctament. Serà el temps que trigui l'adjudicatari a donar i implementar una solució davant una incidència informada per ATL. Es contarà el temps des de que es dona l'avís i que la incidència està resolta o, cas que sigui complexa, es doni una solució pal·liativa provisional.	< 24h
ANS 5	Temps màxim solució d'incidències no critiques	Temps màxim de resolució, per a corregir i implementar una solució correctament. Serà el temps que trigui l'adjudicatari a donar i implementar una solució davant una incidència informada per ATL. Es contarà el temps des de que es dona l'avís i que la incidència està resolta o, cas que sigui complexa, es doni una solució pal·liativa provisional.	< 72h
ANS 6	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 7	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

Nivells de priorització

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

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

Nivell d'urgència	Descripció
Molt Urgent	Sistema aturat. Afecta de manera generalitzada a molts usuaris i no existeix cap via alternativa de cobrir les necessitats.
Urgent	Incidències que impedeixen el funcionament correcte de l'aplicació a alguns usuaris i pot haver alguna via alternativa temporal.
Normal	Incidències que provoquen una degradació del funcionaments de la aplicació que impedeix a alguns usuaris treballar amb la productivitat habitual. Tenen una relativa afectació en el funcionament diari. o requisits/peticions que no es consideren crítiques per a l'organització

Baixa	Es tracta de millores de la aplicació, ja siguin tècniques o funcionals. Fins el dia de la petició es venia funcionant habitualment sense.

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

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

Acompliment dels ANS (Acord nivell de servei) i aplicació de penalitzacions:

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

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

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

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

CAS A:

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

En cas de igualar o superar el nombre de 3 incompliments crítics del mes serà causa suficient per procedir a la rescissió del contracte per part d'ATL.

CAS B:

Total incompliments NO CRÍTICS del mes	**Penalització aplicada sobre l'import de facturació del mes**

2 o menys incompliments	Sense penalització
3 incompliments	3%
4 incompliments	4%
5 incompliments	5%
6 o més incompliments	6%

6. ALTRES REQUISITS i CONDICIONS

6.1. Especificacions de RGPD i seguretat

Els desenvolupaments realitzats i lliurats hauran de complir amb el Reglament (UE) 2016/679, General de Protecció de Dades ("RGPD"). 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

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

El pressupost de licitació del contracte serà de 482.689,57 € IVA inclòs (398.917 € IVA exclòs). Aquest import considera la durada de 48 mesos de contracte, contemplant tots els objectius i abast descrit a aquest plec.

Respecte el pressupost del contracte, que distribuït segons la següent distribució pressupostària:

Concepte	**2025**	**2026**	**2027**	**2028**	**Total (sense IVA)**	**Iva (21%)**	**Total amb IVA**
Equipament, subscripcions i garanties	305.181 €				305.181 €	64.088,01 €	369.269,01 €
Serveis per la instal·lació i configuració del projecte de segmentació (12 mesos)	39.586 €				39.586 €	8.313,06 €	47.899,06 €
Serveis gestionats (36 mesos)		18.050 €	18.050 €	18.050 €	54.150 €	11.371,50 €	65.521,5 €
TOTAL	**344.767 €**	**18.050 €**	**18.050 €**	**18.050 €**	**398.917 €**	**83.772,57 €**	**482.689,57 €**

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

No s'admetran revisions de preu.

8. FACTURACIÓ

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

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

9. PROPOSTA TÈCNICA (Judicis de Valor)

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

1. PLA DE PROJECTE

Projecte de desplegament i posada en marxa (CJV1)

- Planificació detallada de lliurament, garantia de subministrament, configuració de la solució i pla de proves.
- Anàlisi riscos.
- Lliurables: relació de lliurables

2. PLA DE MANTENIMENT (SERVEI GESTIONAT)

Servei de suport i manteniment (CJV2)

- Pla de manteniment: detall de les operacions periòdiques, KPI's i relació d'informes de seguiment.
- Equip de treball manteniment: perfils i dedicacions per l'execució del servei de manteniment.

3. PLA DE FORMACIÓ

Pla de formació (CJV3)

Descripció del pla de formació proposat:

- Metodologia i temari
- Número d'hores de formació prevista.

Sant Joan Despí, a data signatura digital

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