PLEC DE PRESCRIPCIONS TÈCNIQUES PARTICULARS

PER A LA CONTRACTACIÓ DE

"Servei Gestionat de Centre d'Operacions de Seguretat (SOC) IT+OT 24x7x365"

Març 2026

INDEX

1. OBJECTE DEL PLEC

Aquest document constitueix el plec de prescripcions tècniques (PPT) que regeix el procediment de contractació i execució dels "**Servei Gestionat de Centre d'Operacions de Seguretat (SOC) IT+OT 24x7x365**", promogut per l'Ens d'Abastament d'Aigua Ter-Llobregat (ATL), amb la finalitat de garantir la protecció integral dels seus sistemes corporatius (IT) i dels seus sistemes industrials (OT), que suporten els processos essencials de **captació, potabilització i distribució d'aigua en alta**.

El SOC haurà de proporcionar capacitats professionals de **detecció primerenca**, **supervisió contínua**, **anàlisi avançat**, **resposta**, **recuperació** i **millora contínua** davant d'incidents de ciberseguretat que afectin ATL, tant en l'àmbit informàtic com en l'àmbit industrial.

L'objecte del contracte inclou expressament:

- L'operació completa del SOC en mode **24x7x365**.
- La supervisió i visibilitat completa tant d'entorns IT com d'entorns OT.
- La **gestió integral d'incidents IT i OT**, incloent contenció, erradicació, recuperació i coordinació.
- L'**anàlisi forense digital**, l'anàlisi de malware i les investigacions avançades.
- La correlació d'alertes multi-domini: identitat, xarxa, perimetrals, OT, etc.
- L'elaboració d'informes, documentació i evidències de seguretat d'acord amb l'Esquema Nacional de Seguretat.
- La vigilància digital de marca i superfície d'exposició.
- La coordinació amb serveis externs ja contractats per ATL (MDR, vulnerabilitats IT, SSE, etc.).
- La coordinació amb organismes oficials (CCN-CERT, OCC, etc.).

Totes les activitats de resposta a incidents i l'anàlisi forense estan completament incloses dins del preu del contracte, sense cap cost addicional.

2. INTRODUCCIÓ

2.1. Antecedents ATL

Ens d'Abastament d'Aigua Ter-Llobregat (ATL) és una empresa pública de la Generalitat de Catalunya, adscrita al Departament de Territori i Sostenibilitat creada segons el **Decret llei 4/2018, de 17 de juliol**, per el que la Generalitat assumeix la gestió directe del servei d'abastament d'aigua a les poblacions mitjançant les

instal·lacions de la xarxa d'abastament Ter-Llobregat. El Decret llei estableix que ATL és una entitat de dret públic de la Generalitat de Catalunya amb personalitat jurídica pròpia, autonomia administrativa i financera, i plena capacitat d'obrar per al compliment de les seves funcions.

2.2. Objectiu i missió d'ATL

ATL té com a principal objectiu el subministrament d'aigua en alta a les comarques de l'Alt Penedès, l'Anoia, el Baix Llobregat, el Barcelonès, el Garraf, el Maresme, la Selva, el 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 dels sistemes informàtics d'ATL.

En aquest sentit ATL necessita disposar d'un servei de manteniment per garantir el seu correcte funcionament.

Consegüentment, ATL publica aquest plec per a contractar els "**Servei Gestionat de Centre d'Operacions de Seguretat (SOC) IT+OT 24x7x365**".

3. ABAST DEL CONTRACTE

Els serveis que desitja contractar ATL inclouen la prestació íntegra d'un Servei Gestionat de Centre d'Operacions de Seguretat (SOC) IT+OT en modalitat 24x7x365, orientat a garantir la supervisió, detecció, anàlisi i resposta davant incidents que afectin tant els sistemes corporatius IT com els sistemes industrials OT que formen part dels processos de captació, potabilització i distribució d'aigua en alta.

Aquest servei inclourà totes les activitats necessàries per assegurar la protecció continuada dels entorns IT i OT, incloent supervisió, correlació, resposta, investigació avançada, gestió d'alertes, integració tecnològica i coordinació amb tercers.

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

OPERACIÓ DEL SERVEI

- Operació del SOC en modalitat **24x7x365**, incloent vigilància, triatge i resposta inicial.
- Supervisió continuada de totes les fonts IT i OT definides per ATL, amb l'ajuda del proveïdor.
- Correlació d'esdeveniments entre tots els dominis (xarxa, identitat, perimetral, O365, OT…).
- Coordinació directa amb els serveis de seguretat ja contractats per ATL:
  - servei **MDR** (no administració, només coordinació),
  - servei de **FW perimetrals**
  - servei de **FW segmentació**
  - servei de **gestió de vulnerabilitats IT**,
  - servei **SSE/CASB Netskope**.

GESTIÓ I RESPOSTA DAVANT INCIDENTS

- Detecció, anàlisi, classificació i gestió completa de **tots els incidents IT i OT**.
- Activació del **CSIRT**, incloent investigació tècnica avançada i validació d'impacte.
- **Anàlisi forense digital complet**, recollida i preservació d'evidències.
- Anàlisi de malware i generació d'IOC.
- Coordinació amb CCN-CERT (SAT-INET, SAT-ICS, LUCIA Federada).
- Contenció:
  - IT → pot executar-se directament,
  - OT → sempre amb aprovació prèvia d'ATL.

ADMINISTRACIÓ I SUPORT TÈCNIC DELS ELEMENTS DEL SOC

- Operació, manteniment i gestió de la plataforma **SIEM/SOAR** aportada pel mateix proveïdor.
- Integració i manteniment de totes les fonts de dades IT i OT definides a l'inventari.

- Desplegament, configuració, operació i manteniment de **totes les sondes OT industrials**, ja que ATL **no en disposa** actualment.
- Supervisió del correcte funcionament de les sondes governamentals **SAT-INET / SAT-ICS**.

SUPORT OPERATIU I COORDINACIÓ

- Suport al personal d'ATL en consultes, dubtes, interpretació d'alertes i revisió d'incidents.
- Coordinació operativa amb tots els proveïdors de seguretat que interactuen amb ATL (MDR, vulnerabilitats, SSE, FW's...).
- Acompanyament en la preparació d'auditories ENS/NIS2 (aportant evidències, però **sense realitzar l'auditoria**).
- Suport en la definició, revisió i millora dels procediments IT i OT vinculats al SOC.

GESTIÓ DE QUALITAT I MILLORA CONTÍNUA

- Revisió, tuning i optimització contínua de casos d'ús IT i OT.
- Revisió periòdica de regles de correlació i deteccions avançades.
- Proposta de millores en processos, eficàcia de detecció i temps de resposta.
- Participació en comitès mensuals i trimestrals.
- Gestió i control de la qualitat del servei.

CONSULTORIA I FORMACIÓ

- Consultoria **exclusivament orientada al SOC**, incloent millores, ajustos i evolució del servei.
- Sessions bàsiques de formació interna (procediments, gestió d'alertes, interpretació de dashboards).

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

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

4. SITUACIÓ ACTUAL

ATL disposa en l'actualitat de les següents **aplicacions** en producció que estan dins de l'**abast del contracte**:

IT (coordinació, no administració)
- Fortinet (segmentació, SD-WAN)
- WatchGuard
- FortiAnalyzer
- Active Directory (5 DCs)
- Office 365 (gestió externa pel CTTI)
- Cisco ISE (NAC)

- VMware vSphere
- SSE Netskope
- MDR Kaspersky

OT

- SCADA's distribuit
- Historian industrial
- 500 PLCs Siemens i Rockwell
- 30 servidors OT
- 70 PCs/HMIs de control
- Xarxes OT segmentades
- SAT-INET / SAT-ICS (gestió de les sondes per part del licitador)
- Sondes OT industrials aportades pel licitador

.

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

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

5.1. Serveis a cobrir pel adjudicatari

L'adjudicatari haurà de prestar, de manera integral, el conjunt de serveis que es detallen a continuació, amb l'objectiu de garantir una gestió professional, contínua i eficient de la ciberseguretat d'ATL en els àmbits IT i OT.

El servei es prestarà en modalitat **24x7x365**, i haurà d'estar dimensionat per assumir la gestió de tots els incidents, alertes i esdeveniments de seguretat sense dependència operativa del personal d'ATL.

Operació SOC 24x7x365

L'adjudicatari haurà d'operar un Centre d'Operacions de Seguretat amb cobertura permanent **24 hores al dia, 7 dies a la setmana i 365 dies a l'any**, assumint com a mínim les funcions següents:

- Monitorització contínua de totes les fonts de telemetria IT i OT, com a mínim les definides a l'abast del contracte.
- Recepció, registre i gestió de tots els esdeveniments i alertes de seguretat.
- Triatge inicial de les alertes, amb identificació de falsos positius i incidents reals.
- Classificació dels incidents segons criticitat, impacte i urgència, d'acord amb els SLA definits.
- Correlació d'esdeveniments procedents de múltiples fonts (xarxa, identitat, perimetral, correu, OT, etc.).

- Escalat estructurat dels incidents als nivells tècnics corresponents (Nivell 2, Nivell 3 o CSIRT).
- Documentació detallada de totes les actuacions realitzades, garantint la traçabilitat exigida per l'ENS.

El SOC haurà de disposar de personal qualificat en diferents nivells (L1, L2 i L3) i de procediments clarament definits per assegurar una resposta homogènia i consistent.

Gestió integral d'incidents i resposta (IT i OT)

L'adjudicatari serà responsable de la **gestió completa de tots els incidents de seguretat**, des de la detecció fins al seu tancament definitiu, incloent:

- Anàlisi tècnica de l'incident i validació de la seva naturalesa.
- Identificació dels actius afectats i de l'abast real de l'incident.
- Avaluació de l'impacte sobre els serveis IT i/o els processos industrials OT.
- Proposta de mesures de contenció, erradicació i recuperació.
- Coordinació de les accions necessàries amb els equips o proveïdors implicats.
- Seguiment de l'incident fins a la seva resolució.
- Elaboració de l'informe de tancament i de les lliçons apreses.

Model d'actuació acordat amb ATL:

- **Entorn IT:** el SOC podrà executar accions de contenció de forma directa sempre que estiguin prèviament definides als playbooks aprovats.

- **Entorn OT:** qualsevol acció de contenció o actuació que pugui tenir impacte en el procés industrial requerirà **aprovació prèvia i expressa d'ATL**.

Servei de resposta a incidents i anàlisi forense (CSIRT)

El servei haurà d'incloure capacitat CSIRT complet, sense limitació de nombre d'incidents ni costos addicionals, incloent:

- Activació del CSIRT a partir d'alertes del SOC, del MDR, de SAT-INET / SAT-ICS o per petició directa d'ATL.
- Recollida, preservació i custòdia d'evidències digitals.
- Anàlisi forense de sistemes, registres, trànsit de xarxa i artefactes.
- Anàlisi de malware i identificació de comportaments maliciosos.
- Identificació de moviments laterals, persistència i escalada de privilegis.
- Generació d'indicadors de compromís (IOC) per millorar la detecció futura.
- Elaboració d'informes tècnics detallats i informes executius.
- Anàlisi post-incident i definició de mesures preventives.

Aquest servei està completament inclòs en el preu del contracte, sense bossa d'hores ni facturació addicional.

Monitorització OT amb sondes industrials (aportades pel licitador)

Atès que ATL **no disposa de sondes OT industrials pròpies**, l'adjudicatari haurà d'assumir íntegrament:

- Proposta de la solució OT més adequada (Nozomi, Claroty, Dragos o equivalent).
- Subministrament del hardware, llicències i manteniment associats.
- Desplegament de les sondes a les 9 plantes industrials.
- Configuració d'inventari OT passiu (actius, topologia, comunicacions).
- Monitorització passiva del trànsit ICS.
- Detecció d'anomalies, canvis no autoritzats i comportaments sospitosos en PLCs, SCADA i Historian.
- Integració de totes les alertes OT al SIEM/SOAR del SOC.
- Manteniment i actualització de les sondes durant tota la vigència del contracte.

La monitorització OT haurà de ser **estrictament passiva**, sense escanejos actius ni actuacions intrusives.

Gestió de les alertes SAT-INET i SAT-ICS

L'adjudicatari haurà d'assumir la **gestió completa de les alertes generades per les sondes governamentals SAT-INET i SAT-ICS**, incloent com a mínim les activitats següents:

- Recepció, monitorització i registre de totes les alertes i notificacions procedents de **SAT-INET** (àmbit IT) i **SAT-ICS** (àmbit OT).
- Anàlisi tècnica i contextualització de les alertes rebudes, valorant-ne la criticitat, l'impacte potencial i la seva relació amb els actius i processos d'ATL.
- Correlació de les alertes SAT-INET / SAT-ICS amb la resta de fonts del SOC (SIEM, MDR, OT, identitat, perimetral, etc.).
- Gestió dels incidents derivats de les alertes, seguint els procediments de triatge, escalat i resposta definits en aquest plec.
- Coordinació amb **CCN-CERT**, incloent:
  - gestió de comunicacions,
  - seguiment de casos,
  - resposta a requeriments d'informació,
  - i tramitació mitjançant la plataforma **LUCIA Federada**, sempre amb coneixement i validació prèvia d'ATL.
- Documentació completa de totes les actuacions realitzades, garantint la traçabilitat i l'evidència necessària d'acord amb els requisits de l'**ENS nivell ALT**.

L'adjudicatari serà el **responsable operatiu** de la gestió d'aquestes alertes dins del SOC, sense que ATL hagi d'assumir tasques de monitorització o anàlisi de primer nivell associades a SAT-INET o SAT-ICS.

Vigilància digital (Digital Risk Protection)

L'adjudicatari haurà de prestar vigilància digital sobre:

- Marca i reputació, suplantacions.
- Dominis sospitosos / typosquatting.
- Phishing i frau.
- Credencials filtrades (pastes, dark web, etc.).
- Alertes immediates davant riscos crítics.
- Informes mensuals i recomanacions.

Takedown: si es demana, s'executarà sota demanda i d'acord amb la legalitat aplicable, sense incloure assessorament legal.

Informes, governança i seguiment

El servei haurà d'incloure:

- **Informe diari** (resum d'activitat SOC i incidents).
- **Informe mensual** (KPIs/SLA, tendències, vulnerabilitats, incidents, millores).
- **Informe trimestral** (maduresa, evolució i roadmap).
- **Comitè operatiu mensual** i **comitè estratègic trimestral** (model simplificat per equip reduït d'ATL).
- Dashboards en temps real per a seguiment i visió CISO.

Integració amb eines i serveis existents d'ATL (coordinació, no administració)

ATL disposa de serveis ja contractats. El SOC haurà de **coordinar-se** amb:

- **MDR (Kaspersky)**: el SOC consumirà alertes, les correlacionarà i gestionarà els incidents amb el proveïdor MDR.
- **Gestió de vulnerabilitats IT** (tercer): el SOC consumirà informes/resultats, prioritzarà risc i farà seguiment d'accions, però **no administrarà** la plataforma ni executarà escanejos.
- **SSE Netskope** (tercer): el SOC consumirà alertes i telemetria, però **no administrarà** polítiques ni configuracions.

5.2. Requisits tècnics i arquitectura

Els requisits tècnics que es descriuen a continuació defineixen les característiques mínimes que haurà de complir el servei SOC IT+OT i les solucions tecnològiques aportades per l'adjudicatari, amb l'objectiu de garantir una operació segura, robusta, traçable i alineada amb els requisits normatius i operatius d'ATL.

- ***Requisits tècnics del servei:***

Requisits de plataforma SIEM/SOAR

L'adjudicatari haurà d'aportar una plataforma **SIEM i SOAR completament gestionada**, que constitueixi el nucli tecnològic del SOC. Aquesta plataforma haurà de complir, com a mínim, els requisits següents:

- Capacitat d'**ingesta multi-font**, tant d'entorns IT com OT.
- Normalització dels esdeveniments per facilitar la correlació i l'anàlisi transversal.
- Correlació d'esdeveniments en temps real, amb suport per a regles avançades i deteccions basades en comportament.
- Capacitats d'**orquestració i automatització (SOAR)** per reduir temps de resposta, especialment en entorns IT.
- Gestió completa del cicle de vida de l'alerta: recepció, anàlisi, escalat, resolució i tancament.
- Quadres de comandament personalitzables per a:
  - visió operativa del SOC,
  - visió executiva (CISO),
  - seguiment de SLA i KPIs.

- Integració amb fonts d'intel·ligència d'amenaces (TIP), tant pròpies del proveïdor com de tercers.
- Capacitat d'exportar evidències, informes i registres per a auditories ENS.
- Alta disponibilitat i continuïtat del servei.
- Retenció de logs i evidències d'acord amb els requisits de l'ENS nivell ALT.

La plataforma haurà de ser operada íntegrament pel proveïdor, sense necessitat que ATL assumeixi tasques d'administració.

Requisits d'integració de fonts IT

El SOC haurà d'integrar, com a mínim, les següents fonts IT:

- **FortiAnalyzer**, com a punt central de recepció de logs dels dispositius Fortinet.
- Tallafocs **Fortinet** (perímetre, segmentació i SD-WAN).
- Tallafocs **WatchGuard** associats a serveis VPN SSL.
- **Active Directory** (5 controladors de domini).
- **Azure AD / Entra ID**, únicament a nivell de telemetria disponible.
- **Office 365**, únicament a nivell de logs i alertes accessibles. (Si es possible)
- **Cisco ISE (NAC)**.
- **VMware vSphere**.
- **SSE Netskope**, com a font d'alertes i esdeveniments.
- **MDR Kaspersky**, com a font d'alertes EDR.

Consideracions específiques

- ATL no administra el tenant d'Office 365 ni Azure AD, ja que són gestionats pel CTTI.
- El SOC haurà d'integrar només la telemetria disponible, sense exigir privilegis d'administració ni capacitats de gestió del tenant.

Requisits d'integració de fonts OT

Pel que fa a l'àmbit OT, el servei haurà de garantir la integració i explotació de:

- Alertes i inventari procedents de les **sondes OT industrials aportades pel proveïdor**.
- Telemetria i esdeveniments de **SCADA distribuït**, sempre que estiguin disponibles.
- Informació del **Historian** industrial, en cas que sigui accessible.
- Alertes procedents de les sondes governamentals **SAT-INET** i **SAT-ICS**.

Les alertes OT hauran de ser tractades amb el mateix nivell de rigor que les IT, però respectant les restriccions pròpies de l'entorn industrial.

Integració i tractament de les alertes CCN

El servei SOC haurà d'integrar tècnicament les sondes SAT-INET i SAT-ICS dins del SIEM/SOAR del proveïdor, de manera que:

- Les alertes siguin visibles en temps real al SOC.
- Es puguin correlacionar automàticament amb altres esdeveniments IT i OT.
- S'apliquin playbooks específics per a alertes CCN.
- Es garanteixi el compliment dels fluxos de comunicació amb CCN-CERT.

Requisits específics de seguretat OT

El proveïdor haurà de complir estrictament els requisits següents en l'operació OT:

- Monitorització exclusivament passiva del trànsit industrial.
- Prohibició d'escanejos actius o proves intrusives sense autorització expressa d'ATL.
- Existència de procediments específics OT per a:
  - gestió d'alertes,
  - investigació,
  - escalat,
  - contenció.
- Separació clara entre accions IT i OT.
- Execució de qualsevol acció OT només amb aprovació prèvia d'ATL.
- Documentació i traçabilitat completa de totes les actuacions.
- Alineació amb IEC 62443 i bones pràctiques ICS.

Requisits de gestió d'alertes i playbooks

El servei haurà de disposar de:

- Playbooks documentats per a tots els casos d'ús IT i OT.
- Definició clara de:
  - passos d'anàlisi,
  - criteris de decisió,
  - escenaris d'escalat,
  - punts d'aprovació (especialment en OT).
- Mecanismes de reducció de falsos positius.
- Revisió i ajust periòdic dels playbooks.
- Evidència documental de l'execució de cada playbook en incidents reals.

Requisits de traçabilitat, evidències i compliment ENS

El proveïdor haurà de garantir:

- Registre de totes les actuacions del SOC.
- Traçabilitat completa dels incidents.
- Custòdia d'evidències conforme a ENS.
- Capacitat d'exportar informes i evidències quan ATL ho requereixi.
- Suport documental a auditories ENS i inspeccions, sense executar auditories ENS.

Requisits de seguretat del propi proveïdor

L'adjudicatari haurà de garantir que la seva pròpia infraestructura i operació compleixen:

- Control d'accés fort (MFA) per al personal del SOC.
- Registre i auditoria de totes les accions del personal.
- Segregació de funcions.
- Pla de continuïtat del SOC i mecanismes de contingència.
- Gestió de confidencialitat i de subcontractació.

Requisits de reporting i quadres de comandament

El servei haurà d'incloure:

- Quadres de comandament en temps real.
- KPIs i mètriques mesurables.
- Seguiment de SLA.

- Informes:
  - diaris (operatius),
  - mensuals (executius i tècnics),
  - trimestrals (evolució i maduresa).

Exclusió explícita d'abast tècnic

Queden explícitament fora de l'abast d'administració directa del SOC:

- Administració del tenant Office 365 i Azure AD (CTTI).
- Administració del servei MDR/EDR.
- Administració de l'eina de vulnerabilitats IT.
- Administració de la plataforma SSE Netskope.
- Funcions pròpies d'un NOC o administració de xarxa.

5.3. Garantia dels treballs

Tots els treballs, canvis, configuracions o ajustos que l'adjudicatari posi en producció en el marc del present contracte disposaran d'una garantia mínima de correcte funcionament de tres (3) mesos, a comptar des de la data de la seva posada en producció.

Durant aquest període de garantia, l'adjudicatari es compromet a corregir, sense cap cost addicional per a ATL, qualsevol incidència, defecte o mal funcionament detectat en producció que sigui imputable a l'adjudicatari, ja sigui per acció o per omissió.

Aquesta obligació inclou la realització de totes les actuacions necessàries per restablir el correcte funcionament del servei, sense que aquestes actuacions puguin donar lloc a cap tipus de facturació addicional, ampliació de pressupost o consum de bosses d'hores.

Addicionalment, qualsevol actuació correctiva realitzada per l'adjudicatari com a conseqüència de la resolució d'una incidència disposarà d'una nova garantia de tres (3) mesos, a comptar des de la data de resolució efectiva de la incidència.

La garantia no serà aplicable únicament quan la incidència o defecte sigui conseqüència directa de canvis realitzats per ATL o per tercers aliens al contracte, sense la participació o validació prèvia de l'adjudicatari.

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.

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.

5.5. 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 a l'execució del servei objecte del present contracte, un equip de professionals adequadament qualificats, amb coneixements i experiència demostrables en operació de Centres d'Operacions de Seguretat (SOC), tant en entorns IT com OT, així com en la gestió d'incidents de seguretat, anàlisi forense i operació de plataformes SIEM/SOAR.

Els professionals adscrits al servei hauran de disposar d'experiència en la integració, monitorització i correlació de plataformes de seguretat, entorns corporatius i entorns industrials, així com en la coordinació amb serveis de seguretat gestionats per tercers.

Igualment, l'adjudicatari haurà de designar almenys un responsable del contracte, que es mantindrà durant tota la vigència del mateix i que actuarà com a interlocutor principal amb ATL.

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

Gestor del servei:

L'adjudicatari designarà un Gestor del Servei, que actuarà com a responsable operatiu del contracte i interlocutor principal amb ATL.
Les responsabilitats del Gestor del servei seran:

- Organitzar i coordinar l'execució del servei SOC IT+OT d'acord amb el que estableix el present plec.
- Posar en pràctica les indicacions i directrius del responsable del contracte designat per ATL.
- Representar l'equip de treball en les relacions amb ATL.
- Presentar per a la seva aprovació el programa de treball, planificació del servei i propostes de millora.

- Donar suport a la presa de decisions en els diferents àmbits del servei (operació SOC, incidents, OT, millora contínua).
- Realitzar el seguiment del servei, dels SLA i de la planificació de les activitats.
- Coordinar els equips SOC (L1, L2, L3), CSIRT i especialistes OT.
- Coordinar-se amb els serveis externs de seguretat d'ATL (MDR, vulnerabilitats IT, SSE/CASB).
- Garantir la qualitat del servei i la correcta comunicació amb ATL.

Es requereix:

- Experiència mínima de **5 anys** en la gestió de serveis o projectes de ciberseguretat.
- Experiència acreditada en operació de serveis SOC i/o serveis de seguretat gestionada.
- Coneixement de marcs ENS, NIS2 i gestió d'incidents de seguretat.

Analistes SOC (Nivell 1 i Nivell 2) / Personal de suport a plataformes SOC (SIEM/SOAR)

L'adjudicatari haurà de disposar d'analistes SOC suficients per garantir la cobertura del servei 24x7x365.

Les responsabilitats son:

- Monitorització contínua d'alertes i esdeveniments de seguretat.
- Anàlisi inicial, triatge i classificació d'alertes.
- Identificació de falsos positius.
- Investigació tècnica d'incidents de seguretat.
- Escalat d'incidents a nivells superiors quan correspongui.
- Execució dels playbooks definits.
- Documentació de les actuacions realitzades.
- Suport a la gestió d'incidents IT i OT, respectant les restriccions operatives.

Es requereix:

- Experiència mínima de **3 anys** en operació SOC, SIEM i gestió d'incidents.
- Experiència en entorns IT corporatius (xarxa, identitat, perimetral, correu).
- Coneixement bàsic d'entorns OT i de les seves restriccions operatives (per als perfils assignats a OT).

Especialistes SOC / Nivell 3 i CSIRT

L'adjudicatari haurà de disposar d'especialistes de Nivell 3 i capacitat CSIRT per a la gestió d'incidents avançats.

Les responsabilitats son:

- Investigació avançada d'incidents complexos.
- Anàlisi forense digital i de malware.
- Anàlisi de moviments laterals, persistència i escalada de privilegis.
- Suport a la definició i millora de casos d'ús i regles de correlació.
- Suport a incidents crítics IT i OT.
- Coordinació amb CCN-CERT (SAT-INET, SAT-ICS, LUCIA).

- Elaboració d'informes tècnics i executius post-incident.

Es requereix:

- Experiència mínima de **5 anys** en resposta a incidents i/o anàlisi forense.
- Experiència en plataformes SIEM/SOAR.
- Coneixement de marcs MITRE ATT&CK (Enterprise i ICS).
- Coneixement de seguretat en entorns industrials (per als perfils OT).

Especialista de seguretat en entorns OT / ICS

L'adjudicatari haurà de disposar de perfils amb coneixement específic en **seguretat OT**, que donin suport al SOC i al CSIRT.

Les responsabilitats son:

1. Suport a la monitorització i anàlisi d'alertes OT.
2. Gestió i explotació de sondes OT industrials.
3. Anàlisi d'anomalies en protocols industrials.
4. Suport a la definició de playbooks OT.
5. Coordinació amb ATL per a qualsevol actuació amb possible impacte industrial.

Es requereix:

- Experiència mínima de **5 anys** demostrable en entorns OT/ICS.
- Coneixement de PLCs (Siemens, Rockwell) i entorns SCADA.
- Coneixement de bones pràctiques IEC 62443.

El membres de l'equip es consideren obligació contractual essencial i, per tant, el seu incompliment comportaria la resolució del contracte, el compromís adscripció permanent a l'equip d'execució d'aquest contracte, durant la totalitat de la seva vigència, de l'equip tècnic que l'adjudicatari s'ha compromès a adscriure a l'execució dels treballs, que necessàriament ha de complir amb els requisits establerts en el PPTP d'aquesta licitació.

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

5.7. Organització i model de relació

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

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

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

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

5.8. Acords de Nivell de Servei (ANS)

El servei SOC IT+OT prestat per l'adjudicatari estarà sotmès al compliment d'**Acords de Nivell de Servei (ANS)**, amb l'objectiu de garantir la qualitat, continuïtat i eficàcia del servei, així com el compromís de l'adjudicatari amb la correcta prestació del servei a ATL.

Els ANS permetran mesurar de forma objectiva el nivell de qualitat del servei SOC, tant en l'àmbit **IT** com **OT**, i seran aplicables a totes les activitats de monitorització, gestió d'incidents, resposta, anàlisi forense, vigilància digital i coordinació amb tercers.

Els ANS es basaran, principalment, en els criteris següents:

- **Capacitat de resposta davant incidents de seguretat**, especialment aquells que afectin serveis essencials.
- **Qualitat de la gestió dels incidents**, evitant reaparicions i regressions.
- **Compliment dels temps de resposta i activació compromesos**.
- **Qualitat del servei prestat de manera continuada**, en un entorn SOC 24x7.

A títol orientatiu i no limitatiu, es fa constar que el volum d'incidents crítics registrats en els darrers cinc (5) anys ha estat inferior a **tres (3)**.

El ANS que seran d'aplicació son els següents:

<table>
<tr><th></th><th>Acords de nivell de servei (ANS)</th><th>Compromís</th></tr>
<tr><td>ANS 1</td><td>ANS 1 – Temps màxim de resposta inicial del SOC (24x7)
Aquest ANS mesura el temps màxim transcorregut entre la detecció o notificació d'una alerta o incident de seguretat i la primera actuació efectiva del SOC (anàlisi inicial, triatge o activació del procediment corresponent). Aquest temps fa referència a la primera acció del SOC, no al tancament complet de l'incident.</td><td>
<table>
<tr><th>Prioritat de l'incident</th><th>Temps màxim de resposta</th></tr>
<tr><td>Crítica</td><td>≤ 30 minuts</td></tr>
<tr><td>Alta</td><td>≤ 1 hora</td></tr>
<tr><td>Mitjana</td><td>≤ 4 hores</td></tr>
<tr><td>Baixa</td><td>Next Business Day (NBD)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr>
<td>ANS 2</td>
<td>ANS 2 – Temps màxim d'activació del servei CSIRT
Aquest ANS mesura el temps màxim de resposta per a la activació del servei CSIRT, en aquells incidents que requereixin investigació avançada, anàlisi forense o coordinació especial.
S'entén per activació del CSIRT l'inici efectiu de les tasques d'investigació avançada.</td>
<td>
<table>
<tr><th>Prioritat de l'incident</th><th>Temps màxim de resposta</th></tr>
<tr><td>Crítica</td><td>≤ 1 hora</td></tr>
<tr><td>Alta</td><td>≤ 2 hores</td></tr>
<tr><td>Mitjana</td><td>≤ 4 hores</td></tr>
<tr><td>Baixa</td><td>≤ 8 hores</td></tr>
</table>
</td>
</tr>
<tr>
<td>ANS 3</td>
<td>ANS 3 – Qualitat en la resolució d'incidents (no regressió)
Aquest ANS mesura la qualitat de les actuacions realitzades per l'adjudicatari durant la resolució dels incidents.
Es considerarà incompliment d'aquest ANS quan:
Una incidència resolta es reprodueixi per una causa imputable a una actuació incorrecta de l'adjudicatari.
Les mesures aplicades generin una nova incidència o afectin negativament altres components del servei SOC.
No es respectin els procediments i playbooks acordats.</td>
<td>Existència de regressions o reincidències atribuïbles a l'adjudicatari.</td>
</tr>
<tr>
<td>ANS 4</td>
<td>ANS 4 – Qualitat del servei continuat
Aquest ANS mesura la qualitat global del servei prestat de manera continuada, tenint en compte:
Compliment reiterat dels temps de resposta.
Correcta gestió de les alertes SAT-INET i SAT-ICS.
Qualitat dels informes lliurats.
Adequada coordinació amb els serveis externs d'ATL.
Compliment dels procediments operatius IT i OT.</td>
<td>Es considerarà incompliment quan es detectin desviacions reiterades o greus que afectin el nivell de servei acordat.</td>
</tr>
</table>

Acompliment dels ANS i aplicació de penalitzacions:

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

Total incompliments del mes	Penalització aplicada sobre l'import de facturació del mes
2 o menys incompliments	Sense penalització
3 incompliments	3%
4 incompliments	4%
5 incompliments	5%
6 o més incompliments	6%

6. ALTRES REQUISITS I CONDICIONS

6.1. Especificacions de RGPD i seguretat

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

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

6.2. Propietat intel·lectual i propietat de les dades

En el cas que l'objecte del contracte comporti realitzar obres o creacions subjectes a la normativa de propietat intel·lectual, el proveïdor cedirà a ATL gratuïtament i amb caràcter d'exclusiva, sense límit de temps i per a tot l'àmbit territorial universal, els drets d'explotació de la propietat intel·lectual de les obres realitzades per a la prestació de l'objecte contractual, en qualsevol forma i, en especial, en totes les seves modalitats d'explotació, inclosa l'explotació en xarxa d'Internet, del dret de reproducció, distribució, comunicació pública i transformació (actualització, traducció i qualsevol altra modificació que pugui derivar en una altra obra).

La cessió en exclusiva en els termes que estableix el paràgraf precedent s'efectua també als efectes que l'ATL, com a cessionària en exclusiva dels drets d'explotació dels drets d'autor de les creacions realitzades per a la prestació de l'objecte contractual (dibuixos, logotips, textos, eslògans, gràfics, etc.), pugui enregistrar-los, si s'escau, com a titular dels drets de la propietat industrial derivats de totes aquestes creacions (marca o nom comercial).

La cessió de drets prevista en aquesta clàusula s'aplicarà també en el cas d'elements creats o produïts (fotografies digitals, etc.) per persones o empreses que hagin estat subcontractades pel proveïdor, i a aquest efecte, el proveïdor haurà d'acreditar la cessió esmentada. Aquests drets es cediran a l'ATL també en exclusiva, sense límit de temps i per l'àmbit territorial universal en totes les seves modalitats d'explotació, inclosa la xarxa d'Internet: el dret de reproducció, distribució o comunicació pública.

A més, el proveïdor assumeix també l'obligació de respondre i indemnitzar contra tota responsabilitat de qualsevol naturalesa (incloses les quantitats reclamades per les societats de gestió col·lectiva de drets de propietat intel·lectual) originada o relacionada amb reclamacions que l'ATL pugui rebre sobre el fet que l'explotació dels treballs, peces, icones, materials i en general qualsevol creació produïda per a l'objecte d'aquesta contractació, infringeixin drets de propietat intel·lectual i/o industrial de tercers.

Així mateix, la propietat dels materials es cedirà pel proveïdor a l'ATL i ningú podrà fer-ne ús sense l'autorització d'aquest.

La signatura del corresponent contracte suposarà la formalització de les cessions previstes en aquesta clàusula.

Tanmateix, les dades que es generin durant l'explotació de les aplicacions implicades a aquest servei seran propietat d'ATL i en qualsevol moment. Aquestes dades no podran ser cedides ni mostrades a tercers sense autorització expressa d'ATL.

6.3. Confidencialitat

Les dades a les quals s'hagi tingut accés durant la realització dels treballs, seran considerades, a tots els efectes, de caràcter confidencial, essent d'aplicació el que la llei ha establert per l'ús d'aquest tipus d'informació, i hauran de lliurar-se en la seva integritat a ATL, o bé certificar la seva total destrucció.
Les dues parts s'obliguen a tractar de manera confidencial i a no divulgar a tercers les dades, la documentació i la informació de l'altre part. Els deures de secret i no difusió subsistiran fins i tot quan hagin finalitzat les relacions contractuals mútues.
L'adjudicatari es compromet a guardar el més absolut secret sobre tota la informació a la qual tingui accés en compliment d'aquest contracte, especialment la de caràcter personal, i a subministrar-la només a personal autoritzat per ATL. Aquest compromís

afecta tant a les dades que estan en documents en paper, com en qualsevol altre tipus de suport, així com aquelles que s'obtinguin per mitjans telemàtics. En cap cas es podrà copiar, utilitzar amb una finalitat diferent a la que figura en aquest plec o cedir a tercers, ni tan sols per a la seva conservació, les dades o els arxius.

De la mateixa manera, i en el que respecta a la informació que cadascuna de les parts rebi de l'altre com "informació confidencial", les dues parts es comprometen mútuament a retornar-la, esborrar-la o destruir-la, de la manera que indiqui l'altre part per escrit i sigui quin sigui el mitjà en el que està enregistrat.

L'adjudicatari es compromet a la no difusió de cap tipus de codi d'accés o qualsevol altre tipus d'informació que pugui facilitar l'entrada als sistemes d'ATL, així com a no fer un ús incorrecte dels permisos i privilegis que es concedeix al seu personal per a l'execució d'aquest contracte.

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

6.4. Relació amb proveïdors

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

6.5. Seguretat i salut

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

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

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

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

7. PRESSUPOST DE LICITACIÓ

Totes les mencions d'aquest Plec a quanties, imports, valors, pressupostos o equivalents s'entendran referides sense IVA, llevat que es disposi altrament.

L'adjudicatari mensualment certificarà els treballs realitzats, que serà el que s'utilitzarà per a la valoració i facturació dels treballs mensuals. El preu mensual inclou els serveis de suport de l'equip assignat, i els servei de 24X7, a més de la resposta a incidents i anàlisi forense.

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 384.780,00 € IVA inclòs (318.000,00 € IVA exclòs). Respecte el pressupost del contracte, que distribuït segons la següent distribució pressupostària:

Concepte	***2026***	***2027***	***2028***	***IMPORT SENSE IVA***	***IVA (21%)***	***IMPORT AMB IVA***
Servei SOC IT/OT	39.750,00 €	159.000,00 €	119.250,00 €	318.000,00 €	66.780,00 €	384.780,00 €
TOTAL	***39.750,00 €***	***159.000,00 €***	***119.250,00 €***	***318.000,00 €***	***66.780,00 €***	***384.780,00 €***

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 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. Els costos de l'eventual implementació de la plataforma SOC quedaran mensualitzats al llarg de la durada de tot el contracte.

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

La proposta tècnica haurà de contenir, com a mínim, els continguts que es detallen a continuació i haurà d'estar **obligatòriament estructurada** segons l'ordre indicat.
El licitador podrà adjuntar tota la informació complementària que consideri d'interès, sempre que aquesta no substitueixi ni alteri l'estructura mínima exigida.

0. Resum executiu.

El licitador haurà d'incloure un **resum executiu dirigit a la direcció**, amb una extensió màxima de **tres (3) pàgines**, on es presentin de forma sintètica els aspectes més rellevants de la proposta.
El resum executiu haurà d'incloure **obligatòriament**:

- La manera com el licitador enfocarà la prestació del servei SOC IT+OT per a ATL.
- La visió global del servei proposat i la seva adequació a ATL com a operador essencial del sector de l'aigua.
- Els principals **elements diferencials** de la proposta.
- El **valor afegit** que aporta el licitador respecte als requisits mínims del plec.
- Una breu descripció del model d'operació 24x7 i de la gestió d'entorns IT i OT.

1. Proposta tècnica.

Descripció tècnica de la oferta, incloent els principals aspectes com:

1.1. Organització i model de relació: El licitador haurà de descriure l'organització del servei i el model de relació proposat amb ATL, incloent com a mínim:

- L'estructura organitzativa del SOC (L1, L2, L3 i CSIRT).
- Els rols i responsabilitats de cada perfil assignat al servei.
- El rol del gestor del servei com a interlocutor principal amb ATL.
- El model de relació amb ATL, tenint en compte que ATL disposa d'un equip intern reduït.
- Els mecanismes proposats per garantir el compliment del servei, incloent:
  - reunions operatives,
  - reunions estratègiques,
  - canals de comunicació i escalat.
- La coordinació amb serveis de seguretat ja contractats per ATL (MDR, vulnerabilitats IT, SSE/CASB).

- El model de coordinació amb organismes oficials (CCN-CERT, LUCIA).

1.2. Metodologia, planificació i lliurables: El licitador haurà de descriure la metodologia proposada per a la prestació del servei SOC IT+OT, incloent com a mínim els aspectes següents:

Metodologia

- Descripció de la metodologia de treball aplicada a un servei SOC 24x7.
- Gestió del cicle de vida de les alertes i incidents.
- Metodologia de resposta a incidents IT i OT.
- Enfocament específic per a entorns OT (monitorització passiva, no intrusiva).
- Integració del servei CSIRT dins del SOC.
- Enfocament de millora contínua del servei.

Planificació

- Descripció de la fase de transició i presa de control del servei.
- Planificació de la integració de fonts IT i OT.
- Estratègia de desplegament de sondes OT a les 9 plantes.
- Gestió de canvis i evolució del servei durant la vigència del contracte.

Lliurables

El licitador haurà d'indicar, com a mínim:

- Llistat d'informes operatius, mensuals i executius.
- Contingut dels informes post-incident.
- Quadres de comandament i KPIs.
- Documentació de procediments i playbooks.
- Documentació d'evidències per ENS i NIS2.

Mecanismes de seguiment del servei

- Control i seguiment dels SLA/ANS.
- Mecanismes de control de qualitat.
- Gestió de desviacions i accions correctores.

Gestió de riscos

- Identificació de riscos associats al servei SOC.

- Mesures preventives i correctores.
- Gestió de riscos específics IT i OT.

Diagrama d'activitats

- Diagrama o esquema de les activitats del servei.
- Etapes de presa de control del servei.
- Transferència de coneixement.
- Operació ordinària i fase de devolució.

2. **Valor afegit.**
   El licitador podrà descriure les millores o serveis addicionals que proposi aportar, sempre que no suposin cap cost addicional per a ATL ni alterin l'abast mínim definit al plec.

   En particular, es valorarà com a **valor afegit**:

   - Propostes de millora del SOC més enllà dels requisits mínims.
   - Evolució avançada de casos d'ús IT i OT.
   - Capacitats addicionals de detecció o correlació.
   - Propostes de millora en la gestió d'entorns OT.
   - Ampliació del suport durant el període de transició o estabilització.
   - Lliurables addicionals útils per a ATL.
   - Iniciatives de proactivitat o innovació dins l'àmbit del SOC.

Sant Joan Despí, a data signatura digital

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