EMPRESA MUNICIPAL MIXTA D'AIGÜES DE TARRAGONA, S.A.

PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA CONTRACTACIÓ DEL SUBMINISTRAMENT DE LLICENCIES DE PROGRAMARI DELS FIREWALLS, ELS MÒDULS IoT PER A LA DETECCIÓ D'ANOMALIES I DEL SERVEI D'OPERACIÓ I MANTENIMENT PROACTIU I REACTIU DE SEGURETAT (OPERMANT) PELS SISTEMES DE CONTROL INDUSTRIAL DE LES PLANTES DE DEPURACIÓ DE TARRAGONA I TARRAGONA-NORD I DEL CENTRE DE CONTROL OPERATIU DE L'EMPRESA MUNICIPAL MIXTA D'AIGÜES DE TARRAGONA, SA (EMATSA)

ÍNDEX

Contingut

1. OBJECTE

L'objecte d'aquest document és establir les especificacions tècniques per la contractació i execució del **Subministrament de llicencies de programari dels Firewalls, els mòduls IoT per a la detecció d'anomalies i el Servei d'Operació i Manteniment proactiu i reactiu de la seguretat (OPERMANT) dels Sistemes de Control Industrial (SCI)** de les plantes depuradores de Tarragona (en endavant EDAR Tarragona) i Tarragona Nord (en endavant EDAR Tarragona-Nord) i del Centre de Control Operatiu (en endavant CCO) de l'Empresa Municipal Mixta d'Aigües de Tarragona (en endavant EMATSA), amb la finalitat d'ajudar a donar resposta a les necessitats actuals en matèria de Seguretat a les que s'enfronta.

2. INTRODUCCIÓ I ANTECEDENTS.

L'Empresa Municipal Mixta d'Aigües de Tarragona, S.A., en endavant EMATSA, és una societat mixta l'objectiu social de la qual és la gestió de serveis i subministrament d'aigua en el terme municipal de Tarragona.

La principal activitat d'EMATSA és la gestió del Cicle Urbà de l'Aigua, des de la captació, la potabilització, la distribució, el manteniment de la xarxa de sanejament, el control d'abocaments i la depuració de l'aigua residual. EMATSA presta el seu servei en el terme municipal de Tarragona i àrea d'influència.

EMATSA es caracteritza per ser una empresa compromesa, mediambiental i socialment responsable. Prova d'això és que EMATSA té implantat un model de gestió únic i integrat que garanteix la cobertura de les necessitats i expectatives dels nostres grups d'interès, certificat d'acord a les normes de Qualitat (ISO 9001), Medi Ambiental (ISO 14001), de Gestió Energètica (ISO 50001), de Seguretat i Salut Laborals (ISO45001), d'Innocuïtat Alimentària (ISO 22000) i de Gestió de la Continuïtat del Servei (ISO 22301). En la seva estratègia i gestió operativa, la companyia inclou el compromís d'integrar els aspectes socials, laborals, ètics, ambientals, de seguretat i salut i de bon govern que, més enllà del compliment legislatiu, cerquin maximitzar l'impacte positiu envers la societat. EMATSA garanteix la disponibilitat dels seus objectius i metes amb la difusió de les seves polítiques i bones pràctiques a tots els grups d'interès entre els quals hi ha els seus proveïdors. Per aquest motiu, aquests darrers, hauran que conèixer, entendre i acceptar les polítiques definides, implantar les bones pràctiques i ajustar-se a aquests procediments.

D'acord amb la disposició del Real Decret 311/2022, del 3 de maig, per la qual es regula l'Esquema Nacional de Seguretat (ENS) en l'àmbit de l'administració electrònica, EMATSA disposa de la certificació ENS2 tan pels sistemes del Cicle Comercial com pel Centre de Control Operatiu, la qual cosa garanteix que els seus processos compten amb actuacions per a reforçar les capacitats de defensa en front a les ciberamenaces sobre el sector públic i les entitats col·laboradores que li subministren tecnologies i serveis.

A rel de la transposició de la Llei NIS (Real Decret-llei 12/2018, del 7 de setembre, de seguretat de las xarxes i sistemes d'informació), EMATSA és considerada un Operador Essencial. La finalitat d'aquesta llei és la prevenció i protecció eficaç contra possibles amenaces cap a les infraestructures que siguin catalogades com essencials, considerant la **Ciberseguretat**, **Seguretat Física** i **Continuïtat del servei** com els pilars de la protecció.

EMATSA, a l'igual que la resta d'empreses de serveis, s'enfronta a noves amenaces en matèria de cibercriminalitat. Els Sistemes de Control Industrial (SCI) són la base de l'operació de la majoria dels processos de la companyia y defensar-los i protegir-los de les amenaces és la prioritat d'EMATSA ja que, un atac ben organitzat, podria no sols canviar el comportament d'una màquina o procés, sinó que podria amagar aquest fet als operadors i tècnics i aconseguir alterar els valors de lectura de determinats indicadors perquè aquests semblin correctes.

Per tot això, al 2018, EMATSA va contractar un Servei d'Auditoria de ciberseguretat i un anàlisi GAP. L'objectiu d'aquest contracte era l'anàlisi de la situació en la que es trobava la societat en matèria de ciberseguretat, prenent como a base la normativa vigent, la LPIC, llei 8/2011 del 28 d'abril, la NIST-CSF, la IEC 62443-2-1 i la norma ISO 27002:2013. Un cop identificat en quin punt es trobava la societat es va haver de fer una labor de detecció i identificació dels seus punts dèbils i de les diferents mesures a implementar per elevar el nivell de seguretat en cas de ser aconsellable.

En base a aquest nivell de seguretat es va elaborar un pla d'acció amb una sèrie de projectes a implementar per poder aconseguir un estat objectiu de seguretat. Tots aquests projectes van en la línia d'aprovisionar solucions tècniques que permetin establir un sistema de gestió, control i seguiment de les dades que són registrades i processades durant les fases de producció, fent possible la detecció, seguiment, supervisió, control i resposta davant de qualsevol incident que pugui alterar la seguretat establerta, assegurant d'aquesta forma el correcte funcionament i ús dels sistemes

Un dels projectes sorgits del GAP va ser la implantació de la separació de xarxes dels entorns IT i OT d'EMATSA per tal de garantir millor la seguretat dels sistemes de control industrial de la companyia. En aquest sentit, és necessari dissenyar l'esquema de la xarxa, adquirir i implementar els elements de xarxa del tipus switch i Firewall d'última generació (Next Generation) per executar aquesta separació física, així com les llicències de programari pertinents que permetin inspeccionar el trànsit a nivell de comunicacions industrials a la capa 7 (capa d'aplicació), augmentant la capacitat de separar de forma física i lògica ambdues xarxes amb l'objectiu de protegir els sistemes essencials d'EMATSA de possibles ciberatacs. Un cop implementada la separació és necessari implementar un servei d'operació i manteniment proactiu i reactiu de la seguretat dels sistemes de control industrial. Es tracta d'actuacions preventives i de resposta, que disminueixin de forma eficaç la possibilitat d'aparició d'incidències de seguretat, actuant sobre elles i identificant punts de millora en la seguretat de la informació, analitzar i avaluar riscos i oferir respostes per neutralitzar possibles amenaces. Tot en un marc de govern de seguretat. Les solucions tècniques implementades requereixen d'una gran expertesa i d'alta disponibilitat de l'equip que la mantingui. Necessitem contractar el servei de manteniment i operativa diària al no disposar d'aquesta expertesa en el personal intern de la companyia.

EMATSA va implementar la infraestructura de separació de xarxes al CCO l'any 2021 i a l'EDAR Tarragona i EDAR Tarragona Nord l'any 2022. La segregació IT/OT d'aquestes plantes es basa en elements físics (firewalls) i de programari (AV i FireEye).

Els firewalls utilitzats requereixen llicències de programari per subscripció i suport del fabricant (PaloAlto) (vegeu Annex 1).

A més, la ciberseguretat i la monitorització d'aquestes plantes es gestionen mitjançant el contracte de servei OPERMANT, que finalitza el setembre del 2026.

Tot i que inicialment es van fer dues licitacions separades (una pel CCO i una altra per les EDARs) degut a la contractació en moments diferents, EMATSA ara inclourà la totalitat de les infraestructures a monitoritzar i gestionar en una única licitació. Aquesta decisió s'ha pres per guanyar en eficiència i comoditat en el seguiment dels contractes.

Per tot això, l'objecte d'aquesta licitació és establir les especificacions tècniques per la contractació i execució del **Subministrament de les llicencies del programari dels Firewalls, els mòduls IoT per a la detecció d'anomalies i del Serveis d'Operació i Manteniment proactiu i reactiu de la seguretat (OPERMANT) dels Sistemes de Control Industrial (SCI) de l'EDAR Tarragona i l'EDAR Tarragona-Nord i del CCO d'EMATSA,** amb la finalitat d'ajudar a donar resposta a les necessitats actuals en matèria de Seguretat a les que s'enfronta.

3. ABAST.

Amb l'objectiu d'incorporar la gestió de la seguretat en l'àmbit industrial, com a part general i necessària de l'empresa, aquest document descriu el **Subministrament de les llicencies del programari dels Firewalls, els mòduls IoT per a la detecció d'anomalies i el Servei d'Operació i Manteniment Proactiu i Reactiu de Seguretat (OPERMANT) en els Sistemes de Control Industrial (SCI) dels que disposen les instal·lacions dels centres de l'EDAR Tarragona i EDAR Tarragona-Nord i del CCO d'EMATSA** que permeten donar resposta als eixos de prevenció i protecció.

Amb aquest servei es preveu implementar un model de protecció dinàmic i continu **(abans, durant i després de possibles incidències)** que permeti:

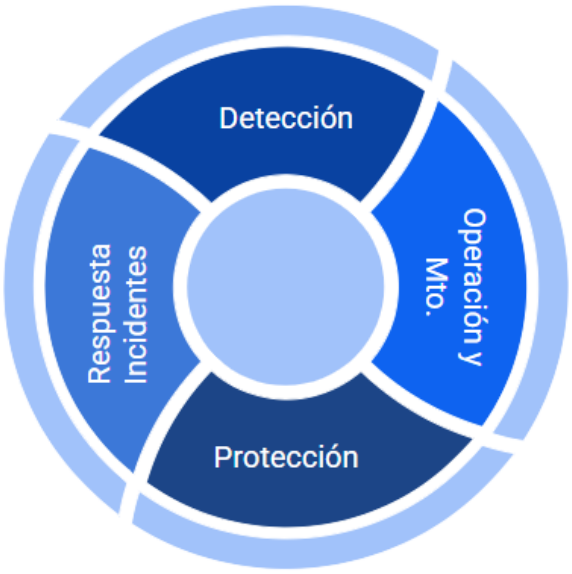
- Evolucionar cap a un model d'acord amb els reptes i objectius estratègics actuals.
- Donar visibilitat i control sobre l'estat de seguretat dels sistemes que permetin protegir els actius que els suporten, garantint així la correcta prestació dels serveis operatius.
- Establir mecanismes per anticipar-se a possibles esdeveniments que es puguin produir en els sistemes i que ajuden a prevenir possibles atacs.
- Gestionar tot el cicle de vida de vulnerabilitats i amenaces potencials.
- Promoure models i tècniques d'anàlisi i protecció de ciberamenaces.
- Elevar els estàndards operatius i les bones pràctiques en la gestió operativa, mitjançant millores derivades de *l'experiència i el saber fer* del sector, així com a través del treball d'enginyeria, benchmarking i transferència tecnològica des de l'àmbit exterior.
- Contribuir a garantir un servei continu (depuració d'aigua i distribució d'aigua), amb alts estàndards de seguretat i fiabilitat, a través de:
    - Garantir la disponibilitat d'infraestructures operatives;
    - Gestió adequada del manteniment en l'àmbit de la seguretat;
    - Generació d'informació oportuna i de qualitat de l'entorn tecnològic;
    - Optimitzar l'ús i robustesa de les solucions i eines tecnològiques presents a l'empresa.
- Tenir un marc de gestió adequat a l'empresa, actualitzat i alineat amb els estàndards internacionals.
- Establir un marc de coneixement de ciberseguretat en els àmbits tècnic i operatiu.
- Ser capaços de respondre a un marc regulatiu i/o normatiu.
- Compatibilitat total amb les eines i model de separació de xarxa existent.

El detall de la solució aplicada i l'abast que aquest servei ha de cobrir i protegir es detalla a **l'Annex 1** d'aquest document.

4. DESCRIPCIÓ DELS SERVEIS

En aquest apartat es descriuen els serveis, característiques i requisits que constitueixen l'objecte del Contracte i que s'han de proporcionar.
L'adjudicatari haurà d'aportar els coneixements i metodologies, així com recolzar-se en les eines necessàries per garantir el resultat òptim del projecte.

El servei inclou tant el suport tècnic proporcionat pel fabricant com el servei integral d'operació i gestió de les solucions implantades, dissenyat per garantir l'evolució i optimització contínua de totes les funcionalitats.



L'estratègia de seguretat ha de tenir com a pilars fonamentals la **detecció**, la **monitorització proactiva**, la **protecció** i la **resposta a incidents**, permetent disposar així d'un model de seguretat coherent i estructurat.

4.1. Servei de Detecció:

L'establiment d'un servei de detecció que permeti disposar de visibilitat i control de totes les capes de seguretat dels sistemes de control industrial és la peça fonamental en la que ha de basar-se la monitorització proactiva.
Una detecció a temps dels punts dèbils objecte d'atac, permeten a les companyies establir mesures de protecció i contenció per a que minimitzin o eliminin les possibles amenaces.
La detecció és, per tant, el punt de partida de la resta de serveis de protecció i resposta a incidents.
En aquesta línia, l'organització vol disposar d'un servei de detecció que permeti descobrir activitats inapropiades, incorrectes o anòmales des de l'interior i/o l'exterior dels sistemes.
Per això i tenint en compte l'evolució del malware és necessari que l'organització disposi d'un servei de detecció basat en 2 nivells:

4.1.1. Servei de Detecció BÀSIC (L1):

Servei de detecció fonamental que permeti disposar d'un nivell de coneixement general de les possibles activitats anòmales que es desenvolupin en l'organització.

Aquest tipus de detecció ha de basar-se en els següents requisits:

- Monitorització de Ciberseguretat suportada per enginyers especialitzats en modalitat 24x7x365.
- Detecció pro-activa d'incidents de Ciberseguretat en les seves etapes més inicials, també en modalitat 24x7x365.

- Inclusió de feeds d'intel·ligència IOCs (indicadors de compromís) i Monitorització proactiva basada en aquests.
- Capacitat d'anàlisis forense bàsic i investigació de possibles incidents.
- Correlació d'events de Ciberseguritat utilitzant tecnologies convencionals de SIEM.
- Capacitat per analitzar tendències que puguin derivar en noves tècniques d'atac.

4.1.2. Servei de Detecció DE MALWARE AVANÇAT (L2):

El servei ha de permetre la identificació de ciberatacs dinàmics i en multifase que no hagin pogut ser detectats mitjançant plataformes de seguretat basades en firmes.

En aquesta línia, l'organització requereix d'un servei de detecció de malware avançat que com a mínim permeti:

- Capacitat de detecció, prevenció i eliminació de codi maliciós convencional i avançat que permeti realitzar seguiment de l'evolució de l'amenaça.
- Capacitat de detecció en temps real, que proporcioni una visió primerenca de les possibles amenaces que es puguin produir.
- Detecció de APTs (Amenaces Persistents Avançades) dirigides i no-dirigides.
- Capacitat de valorar l'afectació provocada por un incident, el seu impacte i possible risc en el servei.
- Capacitat de detecció en temps real, aprenentatge automàtic i en format passiu (no-intrusiu).
- Capacitat de detecció d'intrusions.

4.2. Operació i Manteniment:

Realització de l'operativa relacionada amb les eines de Seguretat esmentades en l'Annex 1. Aquesta operativa inclourà:

- Creació, modificació de regles de FW per a permetre les comunicacions en entorn industrial.
- Resolució de problemes / Solucions alternatives relacionats amb regles de FW en l'entorn OT que no acaben de funcionar.
- Actualització de la versió del sistema operatiu dels FWs
- Revisió d'Alertes dels mòduls IoT i creació, modificació de regles per la neteja i manteniment de les Sondes.
- Manteniment de la sonda mòduls IoT i actualització del sistema.
- Creació i manteniment dels comptes del domini industrial, OAC, en el PAM corporatiu. Això correspon a les següents accions:
  - Creació i permisos de SAFE en entorn OAC
  - Creació/Actualització comptes OAC
  - Solucions alternatives de problemes relacionats amb el reconciliat dels comptes.
- Manteniment de la plataforma i actualització de la versió del sistema de las màquines de salt del PAM corporatiu.
- Manteniment i actualització del sistema de SFTP.
- Alta i modificació d'usuaris de SFTP i creació de directoris compartits en l'aplicatiu de SFTP.
- Manteniment de la plataforma i actualització de la versió del sistema de la solució de AV/EDR.
- Creació i manteniment de polítiques i jerarquia de directoris del sistema de AV/EDR.
- Afinació fina de polítiques de AV/EDR.
- Solucions alternatives i resolució de problemes derivats dels agents d'AV/EDR i la comunicació amb la consola.

- Capacitat d'aprenentatge (manual) del funcionament normal dels actius protegits i interpretació de la desviació.
- Gestió d'alertes i/o desviacions del funcionament normalitzat.
- Comunicació amb las diferents àrees de negoci que puguin estar involucrades en canvis d'infraestructures amb l'objectiu de normalitzar les conductes.
- Centralització d'events de Seguretat – Splunk.
    - L'eina SPLUNK serà usada per entregar el millor servei possible però el proveïdor no administrarà la plataforma, quedant aquest punt fora de l'abast d'aquest contracte.

L'equip tècnic designat assumirà les tasques d'operació i suport, tant preventiu com correctiu, de la plataforma d'accés remot Guacamole, utilitzada com a solució d'administració d'accessos en l'entorn OT. L'abast del servei inclou el manteniment de la plataforma en condicions òptimes, així com l'atenció i resolució de sol·licituds i incidències vinculades a la gestió de comptes i permisos d'accés, la rotació de credencials i el correcte funcionament general del sistema.

Es contempla també un servei preventiu orientat a garantir que el sistema de gestió d'accessos privilegiats es mantingui segur, actualitzat i plenament operatiu, incloent-hi:

- Monitorització de l'estat dels serveis.
- Verificació de la situació dels Safes, les polítiques i els comptes d'ús compartit.
- Coordinació amb EMATSA de les tasques de manteniment i/o actualització.

4.3. Protecció:

La informació i els actius que pertanyen a la companyia necessiten mesures de protecció adequades d'acord amb la seva importància, criticitat i exposició a amenaces.

La informació aportada pel servei de detecció ha de permetre establir un conjunt d'activitats que permetin controlar i gestionar la protecció dels punts dèbils trobats per a salvaguardar a la companyia de possibles amenaces potencials.

En aquesta línia el servei de protecció ha de realitzar, com a mínim, les següents activitats:

- Determinar i implementar contramesures necessàries per prevenir l'explotació de vulnerabilitats, amenaces, etc.
- Aplicar mesures correctives directament sobre els dispositius de Ciberseguretat que permetin bloquejar o mitigar un possible incident o amenaça.
- Bloquejar proactivament elements que comprometin la seguretat (IOCs).
- Operar i administrar activament els sistemes de Ciberseguretat actualment desplegats (Annex 1).
- Actualitzar de forma contínua les plataformes de Ciberseguretat gestionades (Annex 1).
- Parametritzar las plataformes de seguretat en base a necessitats del propi servei (Annex 1).
- Analitzar i millorar contínuament l'entorn securitzat amb l'objectiu d'implementar millores tan en la infraestructura com en les mesures de contenció.
- Avaluar el resultat dels incidents i/o ciberexercicis gestionats amb la finalitat d'aprendre i millorar les capacitats de protecció.

4.4. Resposta a Incidents (IR) Bàsica:

Moltes organitzacions aprenen a respondre a incidents de seguretat només després de patir atacs. Arribat aquest moment, els incidents sovint passen a ser molt més costosos del necessari.

La resposta apropiada a un incident ha de ser una part essencial de la directiva de seguretat general i de l'estratègia de mitigació de riscos.

El servei d'IR bàsic ha de realitzar tasques reactives respecte a incidents identificats, que causen un impacte en la disponibilitat, integritat o confidencialitat del nivell d'operació del servei de negoci.

Les accions a portar a terme en aquest servei són, entre altres:

- Prioritzar correctament el tractament dels incidents en base a l'impacte que aquest pot tenir sobre el servei.
- Obtenir mostres forenses en remot per a donar resposta a un ciberincident.
- Aïllar el dispositiu afectat dins de la xarxa.
- Identificar les amenaces basades en IOCs.
- Preservar tota la informació de les evidències adquirides durant la gestió de l'incident.

EMATSA compta amb un altre servei dedicat a IR, el SOC360, que coordinarà i assumir la responsabilitat de l'anàlisi i la resposta. Aquest servei aquí licitat haurà de donar suport a aquest nivell superior.
El servei haurà d'escalar al SOC360 les troballes o incidents categoritzats com a crítics en el mateix moment de la seva detecció (24x7x365). Events que potencialment puguin suposar un impacte molt alt per EMATSA o la resta de l'organització.

4.5. Servei d'Informes:

El prestador del servei generarà diferents informes de seguretat amb la informació facilitada per les eines gestionades **(Annex 1),** per mostrar:

- **Una visió global i executiva** de l'estat de la seguretat.
- **L'estat puntual** de les plataformes.

El servei ha de tenir com a mínim:

- Informes de l'estat de la seguretat i les seves possibles desviacions. Aquest informe haurà de servir també per fer un seguiment operatiu del servei (ANS) i, per tant, contindrà el detall dels indicadors i la planificació de les accions correctives, preventives i de millora acordades entre les parts, el seu grau d'avanç i d'implantació, així com els resultats obtinguts i l'impacte en l'operativa del Servei (Mensual).
- Informe de resultats d'actuació sobre un atac o incidència gestionats (**Incident classificat com a greu**).

5. ACORD DE NIVELL DE SERVEIS (ANS)

A continuació es mostra la modalitat i els nivells mínims de serveis (ANS) que el Prestador de Serveis ha de garantir per als serveis de monitorització proactiva.
En primer lloc, hem de diferenciar entre els ANS que es corresponen a l'administració i gestió de les eines d'EMATSA (Annex 1) i, d'altra banda, els ANS de seguretat del sistema i arquitectura tecnològica.

5.1. Gestió i manteniment de solucions tecnològiques (Annex 1):

El Prestador del Servei vetllarà pel bon funcionament del conjunt d'eines que EMATSA posa a la seva disposició per prestar el servei. Les diferents eines tenen diferents finalitats, però totes elles són necessàries per desenvolupar el servei subjecte a aquesta sol·licitud. Per tant, el Prestador del Servei ha de tenir responsabilitat tècnica sobre aquestes eines i serà mesurat segons disponibilitat.

Tipus de servei	Modalitat
Gestió i manteniment de les solucions tecnològiques	**24x7x365**

Si l'incident correspon a una fallada de maquinari o programari, l'equip del servei l'escalarà al fabricant per a la seva resolució, d'acord amb els paràmetres inclosos en la prestació del servei.

Si la resolució de l'avaria implica la presència del personal del fabricant, el personal

de servei l'atendrà en remot i EMATSA l'acompanyarà i supervisarà en tot moment durant la presència a les instal·lacions d'EMATSA.

5.2. Gestió de la ciberseguretat:

L'objectiu principal d'aquest servei és protegir en tot moment la infraestructura d'OT d'EMATSA de qualsevol amenaça cibernètica. Aquest servei es mesurarà en funció dels aspectes següents:

Tipus de servei	Modalitat
Servei de detecció, protecció i resposta a incidents	**24x7x365**
Gestió d'Incidències (ticketing i servei telefònic)	**24x7x365**

En ambdós casos (5.1 i 5.2) el model de gestió d'incidències és evolutiu des del nivell N1 (Baix) fins a N4 (Crític):

El nivell de servei dependrà de la priorització requerida en la gestió/resolució d'incidències, que al seu torn es regiran per l'Impacte i la Urgència. És a dir, els criteris a aplicar per prioritzar la gestió/resolució d'incidències són el resultat de la combinació entre aquests dos factors:

Impacte (grau d'afectació que la incidència té en el servei):

NIVELLS D'IMPACTE	
Impacte Crític	❖ Parada total d'un servei/aplicació CRÍTICA. ❖ Degradació o alteració (confirmada o possible) d'un sistema CRÍTIC amb afectació a l'operació.
Impacte Alt	❖ Degradació o alteració (confirmada o possible) d'un sistema CRÍTIC sense afectació al servei. ❖ Parada total o degradació d'un servei/aplicació NO CRÍTIC amb afectació.
Impacte Mig	❖ Degradació o alteració (confirmada o possible) en el funcionament d'un sistema NO CRÍTIC amb afectació al servei. ❖ Parada total o degradació d'un servei/aplicació NO CRÍTIC sense afectació massiva.
Impacte Baix	❖ La resta d'incidents i peticions de servei.

- Urgència (grau en què és possible retardar la solució):

NIVELLS D'URGÈNCIA	
Urgència Crítica	• L'usuari o departament no pot realitzar cap de les funcions principals que té assignades. ❖ L'usuari o departament no pot realitzar altres activitats fins a la resolució de la incidència.
Urgència Alta	• L'usuari o departament no pot realitzar alguna de les funcions principals que té assignades. ❖ L'usuari o departament pot continuar amb altres activitats fins a la resolució de la sol·licitud.
Urgència Mitja	• L'usuari o departament pot realitzar les principals funcions que té assignades però presenta dificultats (lentitud, errors puntuals,...). ❖ L'usuari o departament pot continuar amb altres activitats fins a la resolució de la sol·licitud.

Urgència Baixa	❖ Es veuen afectades funcions secundàries de l'usuari o departament que no impedeixen l'acompliment de les seves funcions principals.

La taula següent permet determinar el nivell de servei a aplicar en funció dels paràmetres establerts anteriorment:

URGÈNCIA / IMPACTE	Urgència Crítica	Urgència Alta	Urgència Mitja	Urgència Baixa
Impacte Crític	Crítica	Crítica	Alta	Mitja
Impacte Alt	Crítica	Alta	Mitja	Baixa
Impacte Mig	Alta	Alta	Mitja	Baixa
Impacte Baix	Mitja	Mitja	Mitja	Baixa

A més, per a cadascun dels nivells de servei requerits es defineix el següent indicador ANS:

• **Temps de resposta a incidències:** Temps que transcorre entre el registre d'entrada o la comunicació de la incidència (ticketing, trucada, etc.) o bé la notificació directa de la incidència per part de les eines a gestionar (Annex 1) pel Prestador del Servei (monitoratge actiu) i l'inici de la primera acció registrada. Es considera una acció registrada aquella en la que l'usuari rep un "input" després del registre d'entrada de la incidència, ja sigui en l'eina de ticketing o mitjançant algun altre mètode acordat amb EMATSA a l'inici del servei.

Indicadore ANS		Prioritat	Valor màxim	Valor Objetiu
Temps de Resposta	N4	Crítica	≤ 2 hores	≤ 45 min
	N3	Alta	≤ 8 hores	≤ 2 hores
	N2	Mitja	≤ 12 hores	≤ 8 hores
	N1	Baixa	Next Bussines day	Next Bussines day

El temps de resposta de cada incidència es calcularà com el temps que hagi passat des del registre de la incidència fins al primer "input" rebut pel client (una vegada que el Prestador del Servei hagi fet una primera anàlisi de la incidència); sense tenir en compte la confirmació del propi registre com a "input".

En funció de la prioritat de la incidència, s'establirà si s'ha complert o no el temps de resposta esperat (valor màxim), tal com s'indica a la taula. El % del compliment s'obtindrà dividint, segons la seva prioritat (N1, N2, N3 i N4), les incidències que han complert els temps previstos entre el total d'incidències obertes en el període considerat (mensual).

Pel que fa al "valor objectiu" establert per a cadascun dels nivells de prioritat indicats en la taula anterior, el servei prestat s'haurà d'aproximar al màxim a aquests temps de resposta, que es consideren un referent per a un servei d'alta qualitat. No obstant

això, només es tindran en compte els "valors màxims" fixats per als temps de resposta en el càlcul dels ANS, tal com s'explica en el capítol 13 d'aquest plec.

En qualsevol cas, després de la resolució de la incidència, s'haurà de documentar la intervenció a l'eina de ticketing per donar per resolta la incidència.

El servei també requereix gestió de problemes segons ITIL (com ara incidents repetitius). L'adjudicatari proposarà en la oferta la seva millor aproximació per al tractament i gestió de problemes de servei.

5.3. Peticions

El servei també atendrà i executarà les sol·licituds de canvi cursades per l'eina de ticketing i convenientment categoritzades. Aquelles peticions que tinguin una complexitat que impliqui un temps d'execució igual o inferior a tres (3) hores, seran assumides pel Prestador del Servei sense cap cost per EMATSA.
El servei serà de 8x5 i estarà subjecte als següents temps de resposta en funció del grau de prioritat que EMATSA hagi assignat a la sol·licitud de canvi:

Prioritat	Temps de Resposta
Alta	8 hores
Mitja	16 hores (2 dies)
Baixa	24 hores (3 dies)

A criteri del responsable del servei d'EMATSA es podrà prioritzar excepcionalment una petició que es consideri urgent i el servei OPERMANT haurà de prioritzar la seva execució.

6. EINA DE TICKETING

EMATSA utilitza una eina de Ticketing i aquest servei també l'ha d'utilitzar. L'actual eina de Ticketing per a EMATSA és Service Desk. Si en el futur aquesta eina es fa evolucionar, el servei s'adaptarà a la nova solució. És imprescindible mantenir una única solució per optimitzar l'esforç i aconseguir els objectius.
El prestador del servei utilitzarà l'eina indicada anteriorment per gestionar el treball relacionat amb el servei.
Els nivells de categorització del servei s'adaptaran a les categories definides a l'eina.
La pròpia eina generarà informes de seguiment del servei, així com informes de compliment dels l'ANS.

7. SOLUCIONS TECNOLÒGIQUES A GESTIONAR EN L'ÀMBIT DEL SERVEI

Com s'ha avançat en capítols anteriors, EMATSA proporciona una sèrie d'eines per a l'anàlisi i seguiment proactiu de la Ciberseguretat de la infraestructura tecnològica de la companyia. Aquestes solucions es detallen a l'Annex 1 d'aquest document.
Aquestes eines són la base tecnològica per al desenvolupament del servei.
L'administració i gestió de les mateixes s'inclou en el servei ofert i serà el Prestador del Servei qui les haurà de mantenir i evolucionar per aconseguir els ANS de Seguretat compromesos.
A més a més d'aquestes, el Prestador del Servei pot proporcionar tantes eines com consideri, sempre que s'incloguin en el servei i no generin costos addicionals fora de l'oferta.

8. MITJANS TÈCNICS I HUMANS

L'equip ha de tenir les competències i habilitats necessàries per desenvolupar amb garanties les activitats definides que permetin oferir la correcta prestació del servei, és a dir:

- Habilitats comunicatives i interpersonals.
- Capacitat per detectar i resoldre problemes
- Alta capacitat d'organització i control de la informació.
- Persones actives i amb iniciativa, per a la millora dels serveis.
- Orientació al treball en equip.
- Persones actives i amb iniciativa, hauran de col·laborar activament en la millora dels serveis.

9. EINES I EQUIPAMENT PER A LA PRESTACIÓ DEL SERVEI

Quan el Prestador del Servei es trobi a les instal·lacions d'EMATSA, aquesta proporcionarà a les persones que prestin el servei el següent (sempre que sigui necessari):

- Ubicació física adequada per al desenvolupament i prestació dels seus serveis.
- Infraestructura pel suport a les eines corporatives (servidors) i xarxa de comunicacions necessàries per a la prestació del servei.
- Accés a Internet a través de la xarxa d'àrea local, restringit a les estacions de treball que ho requereixin així com a les adreces o pàgines web necessàries per al desenvolupament del servei.

EMATSA no facilitarà:

- Ordinadors amb sistema operatiu i programari habitual d'oficina.
- Línies o terminals mòbils per a activitats relacionades amb la prestació del servei.
- Ordinadors portàtils (PC), ordinadors de mà (PDA).
- Accés a Internet a través de GPRS, UMTS.
- Eines vinculades al lloc de treball necessàries per a la prestació del servei.
- Cap altre recurs no especificat de forma explícita

10. SEGURETAT CORPORATIVA

Tant el Prestador del Servei com els seus treballadors han de complir les normes i reglaments interns que dicta l'àrea de Seguretat Corporativa, en matèria de Seguretat de la Informació i ús de les TIC, almenys:

- Acceptar les normes establertes en l'àrea de Seguretat Corporativa tant en el moment de la incorporació com després de cada canvi important en les polítiques, normes o reglaments.
- Complir totes les normes, polítiques i marcs normatius vigents durant el període del contracte.
- Permetre i facilitar la realització d'auditories de compliment de la normativa establerta per a la Seguretat Corporativa, interna o externa, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les actuacions dutes a terme per l'auditor per facilitar el seguiment de les mateixes i els seus possibles impactes no desitjats.
- Custodiar els equips, així com la informació que contenen relativa a EMATSA.

Al final del contracte, el Prestador del Servei estarà obligat a lliurar o a destruir, si se sol·licita, qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

11. UBICACIÓ DE LA PRESTACIÓ DEL SERVEI

El servei es presta, en la seva totalitat o parcialment, en remot. Atès el caràcter 24x7x365 del servei, EMATSA assumeix que el servei es presti a distància. L'oferta de l'adjudicatari definirà clarament en quines condicions la prestarà i aquestes condicions implicaran un compromís.
El Prestador del Servei ha d'assegurar-se que la gestió remota no minva ni empitjora la qualitat del servei.

12. TERMINIS D'EXECUCIÓ

- Subministrament i implantació: màxim fins a 4 setmanes des de la signatura de contracte. Es tracta d'una renovació de llicències ja existents i cal tenir en compte la caducitat de les actuals (veure detall Annex 1).
- Servei OPERMANT: Aquest s'iniciarà a partir de la data d'inici de contracte fins a un total de tres anys.

13. DOCUMENTACIÓ A ENTREGAR

Un cop finalitzada la fase d'implantació del projecte, l'adjudicatari tindrà l'obligació d'entregar a EMATSA un paquet complet de documentació en format digital. Aquesta documentació haurà de ser clara, concisa i fàcilment accessible, preferentment en format PDF o similar, per tal de garantir-ne la preservació i la consulta futura.
La documentació requerida inclourà, com a mínim, els següents elements essencials:

- Esquemes detallats de les infraestructures gestionades: S'hauran d'entregar diagrames complets de tota la infraestructura gestionada.
- Claus d'accés i llicències: Totes les claus de llicència, números de sèrie, claus d'activació i qualsevol altra credencial necessària per a l'accés, la gestió i l'ús del programari i del hardware. S'haurà de garantir que aquesta informació es lliura de manera segura i confidencial.
- Informació de contacte: Per tal de garantir una comunicació fluida i eficient en cas de necessitat, l'adjudicatari haurà de proporcionar una llista actualitzada de:
    - Telèfons de contacte: Números de telèfon directes i de suport (si n'hi ha) per a qüestions tècniques i administratives, incloent horaris de disponibilitat.
    - Correus electrònics de contacte: Adreces de correu electrònic genèriques i/o de persones de contacte clau per a la gestió d'incidències, consultes tècniques i comunicacions generals.

Aquesta documentació és crucial per a EMATSA per assegurar la correcta operació, el servei

14. CONDICIONS DE PAGAMENT I FACTURACIÓ

El pagament del preu es farà contra factura prèviament conformada d'acord amb el preu convingut. La factura o factures es presentaran obligatòriament en format electrònic, sense necessitat d'imprimir-les ni de desplaçar-se a les oficines d'EMATSA. EMATSA informarà a l'empresa contractista dels codis DIR que les empreses contractistes hauran d'incorporar necessàriament a la factura electrònica.
L'enviament de la factura a facturacioematsa@ematsa.cat només s'utilitzarà a efectes de còpia de cortesia o comunicació interna
Per ser admeses i conformades, les factures hauran d'incloure el número de comanda prèviament enviat per part d'EMATSA a l'adreça facilitada pel contractista

- La totalitat de conceptes de subministrament i implantació es facturaran en el moment en què aquesta finalitzi i s'hagi produït la comprovació per part d'EMATSA que la solució implantada és correcta i operativa.
- Pel que fa al servei OPERMANT, aquest es facturarà mensualment a la finalització de cadascuna de les mensualitats de durada del contracte a raó d'1/36 part del preu d'aquest servei

15. FASE DE DEVOLUCIÓ DEL SERVEI

Amb l'objectiu de facilitar el possible canvi de Prestador del Servei subjecte a aquesta Oferta, després de la finalització del període de contractació i amb la finalitat de minimitzar l'impacte en la continuïtat i qualitat dels serveis i facilitar la recepció al nou Proveïdor (o a EMATSA), el Prestador del Servei dissenyarà un pla de finalització (Devolució) d'execució del Servei.
El Pla de Devolució s'ha d'actualitzar durant la vida del Servei en cas de canvis en l'organització del mateix, en el material de referència contractual o per reflectir altres canvis que afectin la reversió.
Durant aquest període de Devolució del Servei, el Prestador del Servei es compromet a col·laborar i prestar, si escau, els recursos humans i materials necessaris per a la realització de totes aquelles activitats dirigides a la planificació i execució del canvi.
Es pretén que el Prestador del Servei transfereixi els coneixements i l'experiència existents, de manera que pugui ser utilitzat com a recurs a disposició del personal d'EMATSA o de tercers (prèvia autorització del client).

La fase de devolució del servei té com a principals objectius els següents:

- Garantir la continuïtat i estabilitat del Servei durant el període de devolució.
- Transferir coneixement del Servei al Client o al nou Prestador del Servei que aquest assigni per la prestació posterior del Servei.
- Generar tota la documentació actualitzada de procediments, manuals, infraestructures i desenvolupaments informàtics associats a l'objecte del contracte.

La devolució del servei es farà durant la durada del propi contracte i es prolongarà, com a màxim, durant DOS (2) mesos.

16. PENALITZACIONS

Aquest servei estarà subjecte als ANS de servei que definirà la qualitat que proporciona el prestador del servei. Les ANS se seguiran mensualment i seran una qualificació objectiva del desenvolupament del servei.
Quan el Prestador del Servei incompleixi les ANS establertes, les sancions financeres es poden aplicar d'acord amb els criteris següents:

Indicadors ANS		Prioritat	Valor màxim	% de Compliment mensual		Penalització (% sobre la facturació mensual)
				[1]	[2]	
Temps de Resposta	N4	Crítica	≤ 2 hores	90 %	66 %	P4= 5%
	N3	Alta	≤ 8 hores	90 %	66 %	P3= 2%
	N2	Mitja	≤ 12 hores	80 %	66 %	P2= 2%
	N1	Baixa	Next Bussines day	80 %	66 %	P1= 2%

Notes importants:

- Si en el càlcul de l'ANS mensual corresponent a un nivell de prioritat específic (Ni) el nombre total d'incidències registrades d'aquest nivell és inferior o igual a 5, s'aplicaran els criteris de % de Compliment indicats a la columna [2]. Si el nombre d'incidències registrades és superior a 5, s'aplicaran els indicadors que figuren a la columna [1].
- El % del compliment s'obtindrà dividint, segons la seva prioritat (N1, N2, N3, N4), les incidències que han complert els temps previstos (Valor màxim) entre les incidències totals registrades amb aquesta prioritat en el mes en avaluació.
- Les penalitzacions mensuals (P1, P2, P3, P4) resultants del càlcul dels diferents ANS per nivell de prioritat (N1, N2, N3, N4) seran independents i s'acumularan en el mes, podent arribar fins al punt de penalitzar totes [fins a l'11% de la factura mensual]. Així, la penalització mensual total (PT) a aplicar serà el valor que resulta d'aplicar la fórmula següent: PT = P1 + P2 + P3 + P4.

En tot cas, quan es produeixin algunes de les circumstàncies següents,

- Incompliment tres (3) mesos consecutius en indicadors N4 o N3;
- Incompliment dels indicadors N4 o N3 en sis (6) mesos de còmput anual (12 mesos);

EMATSA estarà facultada per:

(i) rescindir el contracte, o
(ii) continuar amb la imposició de sancions en els termes anteriors.

Annex 1

SOLUCIONS TECNOLÒGIQUES DISPONIBLES I ACTIUS D'INFRAESTRUCTURA D'OT A LES EDARs I AL CCO D'EMATSA

Aquests sistemes formen part de l'àmbit del servei. La propietat és d'EMATSA i es posen a disposició del prestador del servei que haurà de vetllar per la seguretat de les infraestructures tecnològiques de l'àmbit d'OT d'EMATSA i gestionar-ne els incidents i els problemes relacionats amb ells.

Aquesta és la relació de solucions i actius de l'àmbit del servei i dels quals tindrà responsabilitat de gestió absoluta:

- **1 FIREWALL PALO ALTO PA-220R (CCO)**
  - Threat prevention subscription 3-year prepaid, PA-220R (P/N PAN-PA-220R-ATP-3YR-R) (llic 019101007484)

    Vigència llicència actual fins: 14/04/2027.
    Renovació sol·licitada: 15/04/2027 fins 31/01/2030
  - WildFire subscription 3-year prepaid, PA-220R (PAN-PA-220R-AWF-3YR-R) (llic 019101007484)

    Vigència llicència actual fins: 14/04/2027.
    Renovació sol·licitada: 15/04/2027 fins 31/01/2030
  - Partner enabled premium support 3-year prepaid, PA-220R (PAN-SVC-BKLN-220R-3YR-R) (llic 019101007484)

    Vigència llicència actual fins: 11/02/2027.
    Renovació sol·licitada: 12/02/2027 fins 31/01/2030

- **2 FIREWALL PALO ALTO PA-440 (EDARs)**
  - **1 a l'EDAR Tarragona**
    - Threat prevention subscription 3-year prepaid, PA-440 (P/N PAN-PA-440-ATP-3YR-R) (llic 021201088236)

      Vigència llicència actual fins: 06/09/2026.
      Renovació sol·licitada: 07/09/2026 fins 31/01/2030
    - WildFire subscription 3-year prepaid, PA-440 (PAN-PA-440-AWF-3YR-R) (llic 021201088236)

      Vigència llicència actual fins: 06/09/2026.
      Renovació sol·licitada: 07/09/2026 fins 31/01/2030
    - Partner enabled premium support 3-year prepaid, PA-440 (PAN-SVC-BKLN-440-3YR-R) (llic 021201088236)

      Vigència llicència actual fins: 06/09/2026.
      Renovació sol·licitada: 07/09/2026 fins 31/01/2030

  - **1 a l'EDAR Tarragona Nord**
    - Threat prevention subscription 3-year prepaid, PA-440 (P/N PAN-PA-440-ATP-3YR-R) (llic 021201088326)

      Vigència llicència actual fins: 06/09/2026.
      Renovació sol·licitada: 07/09/2026 fins 31/01/2030
    - WildFire subscription 3-year prepaid, PA-440 (PAN-PA-440-AWF-3YR-R) (llic 021201088326)

      Vigència llicència actual fins: 06/09/2026.
      Renovació sol·licitada: 07/09/2026 fins 31/01/2030
    - Partner enabled premium support 3-year prepaid, PA-440 (PAN-SVC-BKLN-440-3YR-R) (llic 021201088326)

      Vigència llicència actual fins: 06/09/2026.
      Renovació sol·licitada: 07/09/2026 fins 31/01/2030

La renovació de totes aquestes llicències són objecte d'aquest contracte, així com els serveis professionals de configuració de les llicències en els firewalls existents. La data de finalització de les llicències ha de ser 31/01/2030 per totes, d'aquesta manera quedaran igualades per futurs contractes.

- Mòdul IoT per a la detecció d'anomalies (IoT Device Security) per al firewall PALO ALTO PA-440 (EDAR Tarragona).
    - Es tracta d'una planta amb més de 150 dispositius connectats.

Es tracta de llicència nova, actualment no disposem d'aquest programari. La cobertura d'aquesta llicència haurà d'anar des de la data d'inici de contracte fins a 31/01/2030 moment en que finalitzen tota la resta.
El subministrament de la llicència d'aquest mòdul és objecte d'aquest contracte, així com els serveis professionals de configuració del mòdul en el firewall de l'EDAR Tarragona.

- **Antivirus i antimalware servidors SCADA i EQUIPS INFORMATICS**
    - 4 servidors existents on s'ha de gestionar l'antimalware **Trellix.**
    - 7 WorkStations existents on s'ha de gestionar l'antimalware **Trellix**.

La renovació d'aquestes llicències NO són objecte d'aquest contracte, sí la seva gestió durant la duració del contracte i dins del servei OPERMANT

Aquesta llista és l'existent (excepte els subministraments detallats) a data de la publicació del plec de licitació, però durant la duració del contracte de prestació del servei es poden produir canvis tan per afegir alguna solució com per a substituir-la. El servei haurà d'assumir aquests canvis sempre que l'esforç de gestió no suposi una variació significativa.

Tarragona, en la data de signatura electrònica.