MERCADOS DE ABASTECIMIENTOS DE BARCELONA, S.A.
"MERCABARNA"

PLEC DE PRESCRICIONS TÈCNIQUES PER A LA CONTRACTACIÓ DE LA RENOVACIÓ, ACTUALITZACIÓ I MANTENIMENT DEL SISTEMA DE CIBERSEGURETAT INTEGRAL DE MERCABARNA (4 LOTS):

LOT 1: LLICÈNCIES DE PROGRAMARI DE CIBERSEGURETAT
LOT 2: SERVEI DE SOC EXTERNALITZAT
LOT 3: CONSULTORIA ESTRATÈGICA I FORMACIÓ EN CIBERSEGURETAT
LOT 4: RENOVACIÓ DE TALLAFOCS PERIMETRALS

EXP. 2025NSP0006

Contingut

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DE CONTRACTACIÓ DE LA RENOVACIÓ, ACTUALITZACIÓ I MANTENIMENT DEL SISTEMA DE CIBERSEGURETAT INTEGRAL DE MERCABARNA (4 LOTS) – EXP. 2025NSP0006

Amb la mera presentació de la seva oferta, l'empresa licitadora accepta les prescripcions tècniques establertes en aquest plec. Qualsevol proposta que no s'ajusti als requeriments mínims establerts en aquest plec quedarà automàticament exclosa de la licitació.

1. Objecte de la contractació

La finalitat del present Plec de Prescripcions Tècniques (en endavant, **PPT**) és establir les característiques tècniques i requeriments funcionals per a la renovació i contractació d'elements que garanteixin la seguretat i la continuïtat de negoci de Mercados de Abastecimientos de Barcelona, S.A. (d'ara endavant **MERCABARNA**). Amb la contractació d'aquests elements es busca garantir la seguretat de les infraestructures, comunicacions i serveis digitals prestats per MERCABARNA i millorar les capacitats de prevenció, detecció i resposta davant d'incidents de Ciberseguretat.

Es proposa la prestació de serveis horitzontals de Ciberseguretat que augmentin la capacitat de vigilància i detecció d'amenaces en les transaccions dels sistemes d'informació i comunicacions de MERCABARNA, així com la millora de la capacitat de resposta davant de possibles atacs. Es pretén perseguir la protecció en l'àmbit de la seguretat perimetral davant de ciberamenaces, així com la seva correcta configuració, administració, control i gestió.

Es marca com un altre dels objectius l'evolució cap a un model integral que afavoreixi la coordinació interdepartamental davant d'incidents de seguretat complexos i la compartició i l'intercanvi d'intel·ligència de Ciberseguretat, fixant l'ús de les eines implantades, processos i serveis de vigilància, prevenció, detecció, anàlisi, resposta i assessorament.

Amb l'abast de la proposta es contribuirà a millorar la situació de seguretat de MERCABARNA i el grau de coneixement. A més, s'actuarà com a element facilitador per al compliment de la regulació en matèria de seguretat de la informació, concretament de l'Esquema Nacional de Seguretat (ENS) o la seva possible substitució mitjançant la transposició de la NIS2. Així mateix, es pretén obtenir més visibilitat i informació sobre vulnerabilitats, fallades de configuració i incidents, alhora que es millorin les capacitats de protecció i resposta. Garantir la comunicació d'incidents de seguretat al Centre Criptològic Nacional, mitjançant la implantació d'eines de comunicació d'incidències i seguir amb la formació i coneixements dels tècnics de MERCABARNA per afrontar amb garanties els nous reptes plantejats pels escenaris nous a Ciberseguretat.

2. Naturalesa i règim jurídic

Aquesta licitació es justifica en el fet que MERCABARNA està compresa dins dels sectors estratègics definits a la legislació sobre protecció d'infraestructures crítiques, d'acord amb allò establert a l'article 19.4 de la Llei 5/2014, de 4 d'abril, de Seguretat Privada. Així mateix, es fonamenta en la necessitat de comptar amb una o diverses empreses externes especialitzades,

atès que MERCABARNA no disposa dels mitjans humans i materials suficients i adequats per garantir el compliment de les exigències normatives aplicables.

En aquest sentit, d'acord amb el que preveu la Llei 8/2011, del 28 d'abril, per la qual s'estableixen mesures per a la protecció d'infraestructures crítiques, en connexió amb el Reial decret Llei 12/2018, del 7 de setembre, de Seguretat de Xarxes i Sistemes d'Informació, MERCABARNA ha d'adoptar mesures específiques de protecció. D'acord amb l'article 16 del Reial Decret Llei 12/2018, els operadors de serveis essencials estan obligats a implementar mesures tècniques i organitzatives adequades i proporcionades per gestionar els riscos que afectin la informació utilitzada als seus sistemes, a fi de prevenir i minimitzar l'impacte de possibles incidents.

Així mateix, de conformitat amb el que disposa el Reial Decret 43/2021, de 26 de gener, que desenvolupa el marc estratègic de seguretat de xarxes i sistemes d'informació, i el Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), MERCABARNA ha de garantir el compliment dels requisits de protecció i de seguretat a les seves infraestructures. A més, en relació amb les xarxes i serveis de comunicacions electròniques essencials per a la seva activitat, és aplicable el Reial decret Llei 7/2022, de 29 de març, que estableix mesures per garantir la seguretat a les xarxes 5G.

D'altra banda, en el context europeu, la Directiva (UE) 2022/2555, coneguda com a NIS2, va entrar en vigor el gener del 2023 i ha de ser transposada a la legislació espanyola abans del 17 d'octubre del 2024, tot i que a data d'aquesta licitació encara no s'ha executat aquesta transposició, s'espera que s'efectuï amb caràcter immediat. Aquesta nova directiva estableix requisits més estrictes de Ciberseguretat per als operadors de sectors crítics.

Tot això sense perjudici del deure de notificar incidents a les autoritats públiques competents i als equips de resposta a incidents de seguretat informàtica (CSIRT) de referència nacional. L'article 19 del Reial Decret Llei 12/2018, de 7 de setembre, estableix aquesta obligació de notificació per als operadors de serveis essencials. Així mateix, l'article 11 del mateix Reial Decret Llei designa com a CSIRT de referència el CCN-CERT, del Centre Criptològic Nacional, i l'INCIBE-CERT, de l'Institut Nacional de Ciberseguretat d'Espanya. Finalment, l'article 9 del Reial Decret Llei 12/2018 atribueix a la Secretaria d'Estat de Seguretat, a través del Centre Nacional de Protecció d'Infraestructures i Ciberseguretat (CNPIC), la competència en matèria de seguretat de les xarxes i sistemes d'informació per als operadors de serveis essencials que també siguin designats com a operadors crítics d'acord amb la Llei 8/2010.

Addicionalment, la necessitat de reforçar la seguretat de les infraestructures crítiques i dels operadors de serveis essencials es veu accentuada amb la propera entrada en vigor de la Llei de Coordinació i Governança de la Ciberseguretat, actualment en fase d'avantprojecte. Aquesta normativa busca enfortir la protecció de les xarxes i sistemes d'informació, millorar la coordinació entre organismes públics i privats i establir mecanismes més eficaços de supervisió i resposta davant de ciberamenaces. Aquests objectius estan alineats amb la transposició futura de la Directiva (UE) 2022/2555 (NIS2), que amplia l'abast dels sectors regulats i imposa requisits més estrictes en matèria de Ciberseguretat i notificació d'incidents.

En aquest context, i d'acord amb el que disposa l'article 168.a).3r de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (LCSP), el procediment negociat sense publicitat és aplicable quan el contracte hagi estat declarat secret o reservat, o quan la seva execució hagi d'anar acompanyada de mesures de seguretat especials d'acord amb la legislació vigent. Atès que MERCABARNA es troba dins l'àmbit d'aplicació de la normativa de protecció d'infraestructures crítiques i Ciberseguretat, i en virtut de les exigències de seguretat que previsiblement es derivaran de la transposició de la NIS2, l'aplicació d'aquest procediment és justificada per garantir la protecció de la informació i l'adequada implementació de les mesures de seguretat necessàries.

El present contracte és susceptible de ser finançat pel Pla de Recuperació, Transformació i Resiliència, finançat per la Unió Europea a través dels fons Next Generation EU, així com altres subvencions de caràcter regional, nacional o de la Unió Europea. En cas que el contracte sigui finalment finançat a través de fons Next Generation EU, l'empresa contractista haurà de complir amb tots els requisits i obligacions relacionades amb els principis transversals que configuren el sistema de gestió del PRTR, definits en l'article 2 de l'Ordre HFP/1030/2021, de 29 de setembre, per la que es configura el sistema de gestió del Pla de Recuperació, Transformació y Resiliència:

- Fites i Objectius, així com els criteris per al seu seguiment i acreditació de resultats.
- Etiquetatge verd i digital.
- Anàlisi de riscos en relació amb possibles impactes negatius significatius en el medi ambient (do not significant harm, DNSH), el seguiment i verificació de resultats.
- Reforç dels mecanismes de prevenció, detecció i correcció del frau, la corrupció i els conflictes d'interès.
- Compatibilitat del règim d'ajudes d'estat i prevenció del doble finançament.
- Identificació del perceptor final dels fons, inclosos subcontractistes.
- Obligacions de comunicació.

L'empresa contractista accepta complir amb els requeriments que faci l'òrgan de contractació, de cara a donar compliment a les obligacions vinculades a la normativa dels fons Next Generation EU i del PRTR o d'altres vinculats a la subvenció que eventualment correspongui. Aquestes obligacions no seran de caràcter substancial sinó relatives a obligacions de comunicació, format de presentació de factures i forma d'acreditació de fites.

3. Divisió en lots

Per tal de poder aconseguir proveïdors en àrees específiques i obtenir una millor qualitat i eficiència en l'execució dels serveis o subministraments, de naturalesa diversa, es proposa la divisió en quatre lots aquesta licitació:

- **LOT 1** – renovació de les llicències, del suport i manteniment dels programaris de Ciberseguretat de MERCABARNA
- **LOT 2** – centre d'operacions de Ciberseguretat i serveis de resposta a incidents i vigilància digital

- **LOT 3** – consultoria estratègica, assistència tècnica per formacions, adequació normativa i certificacions
- **LOT 4** – renovació dels *firewalls* i del seu suport, manteniment i llicències

4. LOT 1: RENOVACIÓ DE LES LLICÈNCIES, DEL SUPORT I MANTENIMENT DELS PROGRAMARIS DE CIBERSEGURETAT EXISTENTS A MERCABARNA

4.1. Objecte

L'objecte d'aquest lot és la renovació o la contractació de les llicències de programari de Ciberseguretat i dels Serveis Associats de Suport i manteniment, a fi de garantir la continuïtat de negoci i la protecció integral de la infraestructura tecnològica de MERCABARNA.

4.1.1. Renovació llicències, suport i manteniment ANTIVIRUS EDR

L'objecte del present contracte és la renovació i suport d'una solució avançada de seguretat en endpoints EDR Crowdstrike Falcon Prevent & Insight (NG-AV + EDR) per fins a 200 endpoints, que proporcioni capacitats de detecció, protecció i resposta davant d'amenaces en els dispositius de l'entitat, amb especial atenció a atacs avançats, malware, ransomware, entre d'altres.

La solució haurà d'estar basada en un enfocament Endpoint Detection and Response (EDR) d'última generació, que combini tecnologies de prevenció, anàlisi de comportament, intel·ligència d'amenaces i resposta automatitzada, garantint la protecció dels equips d'usuari i servidors corporatius, tant en entorns locals com en mobilitat i cloud.

4.1.2. Renovació llicències suport i manteniment SIEM

L'objecte del present contracte és la renovació o contractació d'una solució de gestió d'informació i esdeveniments de seguretat (SIEM), juntament amb els serveis de suport i manteniment associats, per tal d'enfortir les capacitats de detecció, anàlisi i resposta davant d'incidents de Ciberseguretat a l'organització. Aquesta solució SIEM, haurà d'estar dimensionada per a un màxim de 250 endpoints.

La solució haurà de permetre la recollida, correlació i anàlisi centralitzada d'esdeveniments de seguretat provinents com a mínim de les fonts següents (Office365, DHCP, DNS, Firewalls, Crowdstrike, Active Directory, DSPM), així com la generació d'alertes i reports que donin suport a la gestió de riscos i el compliment normatiu.

Actualment MERCABARNA disposa de la solució SIEM Rapid7 InsightIDR, en cas que l'adjudicatari d'aquest lot proposi un altra eina, s'haurà de presentar una memòria tècnica detallada tant del producte com del projecte d'implementació i migració de la nova eina que tracti amb detall totes les fases del projecte i el objecte inclourà la implementació, configuració, integració de la nova eina amb totes les fonts de dades mencionades en aquest plec, així com la posada en producció del sistema.

Aquesta nova eina haurà de garantir que com a mínim dona cobertura a les actuals propietats de l'eina Rapid7, sent les més característiques:

- Plataforma unificada de seguretat que integra solucions crítiques en la monitorització, detecció, resposta i gestió de vulnerabilitats
- Escaneig de xarxa natiu, continu i automatitzat, amb capacitats de descobriment i anàlisi de vulnerabilitats de tota la infraestructura corporativa. Incloent protocols TCP/UDP, detecció de serveis exposats, segmentació interna i cobertura especifica de l'electrònica de xarxa
- Capacitats de tecnologia d'enganys integrades a la plataforma, permetent el desplegament de honeypots
- Agent únic als equips
- Anàlisis de comportament d'usuaris i entitats juntament amb telemetria de xarxa, endpoints i núvol amb mitigació de falsos positius
- Priorització basada en risk mitjançant CVSS, explotability, moviment lateral i Criticitat d'actius
- Capacitats de cobertura en entorns híbrids
- Threat intelligence integrada i actualitzada
- Visibilitat en temps real
- Llicenciament per actius
- Emmagatzematge il·limitat al núvol per a tots els esdeveniments de seguretat recopilats des de les diferents fonts de dades integrades, sense cap restricció en el volum d'informació enviat.
- Retenció per defecte dels esdeveniments durant un període de 12 mesos, complint així amb els principals estàndards normatius i d'auditoria.

4.1.3. Adquisició llicències, instal·lació, suport i manteniment d'un software per a la gestió integral de la dada

Adquisició de les llicències necessàries (dimensionades per a un màxim de 200 *usuàris*) d'un programari de tipus DSPM (*Data Security Posture Management*), protecció i gestió de dades i la implantació i suport d'una solució integral de gestió i protecció de dades que permeti a l'entitat disposar d'eines avançades per a:

- Localització, classificació i protecció de la informació sensible
- Control i auditoria d'accessos a dades
- Gestió centralitzada de permisos d'usuaris sobre recursos
- Monitorització i traçabilitat de l'activitat sobre la informació
- Compliment normatiu en matèria de protecció de dades i seguretat de la informació (RGPD, ENS, NIS2, ISO 27001 o altres aplicables)
- Tots els serveis utilitzats en núvol, allotjats dins d'Europa, acomplint RGPD

La solució haurà de proveir un sistema centralitzat, escalable i segur, que faciliti l'administració de les dades independentment de la ubicació (servidors locals, entorns cloud, dispositius corporatius, dispositius mòbils).

4.1.3.1. Necessitat de l'eina

La infraestructura tecnològica de MERCABARNA compta als seus sistemes d'informació amb nombrosos serveis que donen suport a la seva gestió. Entre aquests sistemes hi ha el Directori Actiu, que gestiona els comptes dels usuaris i que s'utilitzen per a l'autenticació i el control d'accessos a bona part de les aplicacions i els sistemes d'informació. D'altra banda, entre els serveis d'informació que manté MERCABARNA es troben en servidors de fitxers, que, a causa de la naturalesa dels serveis prestats per la MERCABARNA, es tracta d'informació molt sensible que ha de ser supervisada, gestionada i monitoritzada d'acord amb allò indicat a la normativa vigent.

La normativa sobre protecció de dades personals obliga a posar en marxa les mesures tècniques i organitzatives necessàries per garantir la màxima seguretat de les dades. Les mesures adoptades han d'incloure mecanismes per evitar el tractament il·lícit o no autoritzat d'informació personal, i la protecció davant de la pèrdua o destrucció de dades. Addicionalment, l'Esquema Nacional de Seguretat (ENS) imposa l'obligatorietat de mantenir un control adequat de les autoritzacions i control d'accés als sistemes, així com el registre de la seva activitat.

Així, a l'article 17 del capítol III (requisits mínims) de l'ENS sobre l'autorització i el control dels accessos, s'estableix:

L'accés controlat als sistemes d'informació compresos en l'àmbit d'aplicació d'aquest Reial decret ha d'estar limitat als usuaris, els processos, els dispositius o altres sistemes d'informació, degudament autoritzats, i exclusivament a les funcions permeses.

Igualment, a l'article 24 del mateix capítol, sobre el Registre d'activitat i detecció de codi nociu, s'estableix:

Amb el propòsit de satisfer l'objecte d'aquest Reial decret, amb plenes garanties del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge dels afectats, i d'acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i altres disposicions que siguin aplicables, es registraran les activitats dels usuaris, retenint la informació estrictament necessària per monitoritzar, analitzar, cada moment a la persona que actua.

Per complir aquestes obligacions normatives, MERCABARNA necessita eines i serveis associats, que permetin un control d'accés adequat, la classificació de la informació, el registre d'activitat i capacitats de generació d'alertes i informes sobre el Directori Actiu i els repositoris de fitxers de MERCABARNA.

4.1.3.2. Característiques de l'eina:

La solució haurà d'incloure, com a mínim les característiques següents:

a) Auditoria i traçabilitat dels arxius

- Registre d'accessos, modificacions, eliminacions i còpies fetes sobre fitxers i directoris
- Consola de cerca forense que permeti reconstruir l'historial d'accions per a finalitats de recerca d'incidents
- Capacitat de monitoratge en temps real i generació d'alertes

b) Classificació de la informació

- Identificació i classificació automàtica de dades sensibles o crítiques
- Etiquetatge de la informació segons nivell de confidencialitat i Criticitat
- Possibilitat d'aplicar polítiques de seguretat segons la classificació
- La solució ha de permetre la categorització massiva de documents en local mitjançant recursos GPU, evitant que les dades hagin de ser tractades fora de l'organització del CLIENT. La categorització dels documents es farà en base a la seva estructura i contingut.

c) Gestió de permisos i accessos

- Visualització centralitzada de permisos assignats sobre fitxers, carpetes i repositori
- Automatització de la concessió, revisió i revocació de permisos
- Detecció de permisos obsolets o inadequats i recomanacions d'ajustament

d) Gestió d'endpoints i activitat d'usuari

- Control de l'ús de fitxers des de dispositius locals o remots
- Seguiment de l'activitat de l'usuari en relació amb la gestió de dades (sense envair la privadesa, únicament amb finalitats de seguretat)
- Alertes davant comportaments anòmals

e) Acompliment normatiu

- Eines per donar suport al compliment del Reglament General de Protecció de Dades (RGPD)
- Adaptació als requisits de l'Esquema Nacional de Seguretat (ENS) i la Directiva NIS2
- Possibilitat d'exportar informes periòdics per a auditories

f) Requisits addicionals

- Arquitectura modular que permeti activar únicament els components necessaris.
- Escalabilitat per adaptar-se al creixement de l'organització.
- Integració amb directoris corporatius (ex. LDAP, Active Directory).
- Consola web d'administració segura amb autenticació multi factor.

- Documentació tècnica actualitzada de la solució.
- La solució ha d'estar inclosa al catàleg CPSTIC del Centre Criptològic Nacional — Categoria de productes i serveis de Conformitat i Governança de la seguretat, Família de Governança i Planificació de la Seguretat amb Categoria ENS Alta.
- La solució ha d'estendre la seva funcionalitat complerta sobre tots els repositori de informació de Mercabarna, incloent-hi OneDrive i Sharepoint, Exchange online, Repositoris cloud, Cabines d'emmagatzemament, Servidors de fitxers, PC's amb Windows 10 o 11 i Bases de dades.
- La solució haurà de ser vàlida per a un màxim de 200 usuaris amb accés a dades, sense limitació en el que es refereix a nombre i varietat dels repositori a gestionar, ni al volum contingut als mateixos.
- La solució haurà de tenir totes les seves funcionalitats sense limitacions independentment els llocs de treball comptin amb Windows 10 o 11.

L'adjudicatari haurà de proporcionar:

- Instal·lació, parametrització i integració de la solució a la infraestructura de l'entitat.
- Formació al personal tècnic de la solució
- Suport i manteniment durant la vigència del contracte (actualitzacions, pegats de seguretat, resolució d'incidències)
- Integració amb el SIEM existent a la entitat
- Garantia de continuïtat de servei i temps de resposta mínims (SLAs)

4.2. Durada del contracte

Totes les llicències estipulades en el LOT 1 tindran com a data d'inici prevista l**'1 de gener de 2026,** d'acord amb la planificació inicial, no obstant això, aquesta data podrà ajustar-se si les circumstàncies ho requereixen. I la seva durada serà de **5 ANYS, a excepció de les llicències del SIEM que tindran com a data d'inici al Maig de 2026**.

En cas que algun software es consideri de nova adquisició, l'adjudicatària tindrà 30 dies per a configurar i deixar operatiu el programa i integrat amb els diferents sistemes de MERCABARNA. Aquesta integració correra a càrrec del adjudicatari i haurà de ser verificada i aprovada per MERCABARNA.

4.3. Documentació a presentar

Amb la finalitat de verificar el acompliment dels requisits mínims d'obligat compliment, establerts al present document, l'oferta inclourà una memòria tècnica, amb com a mínim els següents apartats:

- Pla de suport i manteniment de l'eina EDR Crowdstrike
- Definició de SLA's i mètriques de l'eina EDR Crowdstrike
- Pla de suport i manteniment de l'eina SIEM
- Definició de SLA's i mètriques de l'eina SIEM
- Pla de suport i manteniment de l'eina DSPM

- Definició de SLA's i mètriques de l'eina DSPM

5. LOT 2. CENTRE D'OPERACIONS DE CIBERSEGURETAT I SERVEIS DE RESPOSTA D'INCIDENTS I VIGILÀNCIA DIGITAL

5.1. Objecte

L'objecte del present contracte és la contractació d'un servei de **Centre d'Operacions de Seguretat (SOC)** extern, que proporcioni la monitorització, correlació, anàlisi i resposta davant d'incidents de Ciberseguretat a partir dels esdeveniments generats per la infraestructura tecnològica de l'entitat i centralitzats a la solució SIEM implantada a l'organització.

El servei contractat haurà de garantir la detecció primerenca, investigació i resposta eficaç davant d'amenaces que puguin afectar l'entitat, classificada com a Infraestructura Crítica d'acord amb la Llei 8/2011 i la normativa del Ministeri de l'Interior, i complir les exigències de seguretat derivades de l'Esquema Nacional de Seguretat (ENS) i de la Directiva NIS/NIS2.

5.2. Abast

El servei de **Centre d'Operacions de Seguretat (SOC)** haurà de garantir una cobertura integral de monitoratge, detecció i resposta davant incidents de Ciberseguretat, d'acord amb la condició de l'entitat com a **Infraestructura Crítica**. L'adjudicatari haurà de cobrir, com a mínim, els apartats següents:

5.2.1. Monitoratge i detecció d'amenaces 24x7x365

L'adjudicatari haurà de proporcionar un servei de vigilància contínua, operant **tots els dies de l'any, en horari ininterromput**, per a la supervisió de la infraestructura tecnològica de l'entitat. El servei inclourà la **recollida i correlació d'esdeveniments en temps real** mitjançant el SIEM corporatiu i altres solucions de seguretat desplegades (EDR, DSPM, Firewalls, IPS, etc.). La finalitat és aconseguir la **detecció primerenca d'amenaces**, reduir el temps d'exposició dels incidents i disposar d'alertes prioritzades per criticitat, alineades amb el marc de referència **MITRE ATT&CK**.

El servei de monitorització s'haurà de proveir des d'un Centre d'Operacions de Seguretat (SOC) que permeti disposar de capacitats de detecció, prevenció i resposta davant de qualsevol tipus de ciberatacs, incidents de seguretat o intrusions, que posin en risc la integritat i seguretat de la informació, tractant de minimitzar l'impacte d'aquests incidents de seguretat, i analitzar possibles punts de millora i respostes per neutralitzar les amenaces. A causa de la Criticitat dels serveis que s'hauran de proporcionar a través del SOC, aquest haurà d'estar certificat a l'ENS almenys a nivell mitjà per a l'abast de la prestació, per alguna de les entitats de certificació acreditades per l'Entitat Nacional d'Acreditació (ENAC).

El servei de SOC es proporcionarà en mode 24x7 durant la vigència del contracte i s'entendrà com un servei integral que inclourà tots els costos relacionats amb els serveis professionals.

5.2.2. Resposta a incidents de seguretat

El servei haurà d'incloure la capacitat de **respondre de manera immediata** davant incidents de Ciberseguretat, seguint procediments estandarditzats de detecció, classificació, contenció, erradicació i recuperació.

L'adjudicatari es responsabilitzarà de coordinar amb el personal intern les accions de mitigació, proporcionant a més **informes post-incident** amb les causes arrel, evidències tècniques i recomanacions de millora.

Els **SLA de temps de resposta** seran definits en el contracte, havent de garantir un escalat àgil per a incidents crítics.

L'adjudicatari serà el responsable de realitzar una gestió, monitorització i operació activa dels incidents de seguretat durant la vigència del contracte, per això, haurà de treballar juntament amb les persones responsables de MERCABARNA per a la gestió dels incidents de seguretat que es produeixin.

A partir de la informació proporcionada pel servei de monitorització, l'adjudicatari haurà de registrar l'incident, analitzar-lo, categoritzar-lo i escalar-lo conforme al procediment de gestió d'incidents que s'indiqui des del personal responsable de sistemes de MERCABARNA. A continuació, s'indiquen els treballs que estan inclosos al servei:

- La integració amb el SIEM de MERCABARNA, actualment Rapid7 però com a resultat d'aquesta licitació pot esdevenir un altre i l'adjudicatari ha de poder integrar-se amb la solució resultant.
- Disponibilitat 24x7 mitjançant una línia de Resposta a Incidents, en tres torns rotatius per garantir la vigilància contínua. L'equip d'experts que assisteix a la hotline farà un primer triatge d'Incidents i iniciarà el procés intern per activar el Servei, elevant la sol·licitud a un Incident Handler.
- La detecció dels incidents de seguretat generats a partir del servei de monitorització.
- L'anàlisi de qualsevol incident de seguretat amb independència d'haver estat detectat pel mateix adjudicatari, de cara a determinar-ne el possible abast i/o escalat als grups d'actuació oportuns.
- Comunicació, tractament i registre de tots aquests incidents de seguretat segons els procediments establerts pel departament de sistemes.
- Consultoria sobre les mesures a aplicar per a la correcció de les vulnerabilitats detectades i que s'haurien d'aplicar a la infraestructura de MERCABARNA (les modificacions a aplicar a la nostra infraestructura estarien fora de l'abast d'operació i serien realitzades pel personal de MERCABARNA amb suport del personal d'operació del SOC de l'adjudicatari).
- El servei haurà d'evolucionar d'acord amb les modificacions que es produeixin en matèria de seguretat durant la vigència del contracte, adaptant-se a les noves situacions

i implementant aquelles mesures que siguin necessàries per garantir que el producte està actualitzat.

- Incident Handler dedicat, per coordinar la gestió de la crisi i donar suport a la resposta d'extrem a extrem. Això inclou l'assistència per a la contenció ràpida, la recuperació de dades segures i l'assistència amb la Comunicació d'Incidents Externa i Interna - als CERTs, LEAs i Stakeholders.
- Accés complet a l'equip d'experts per a l'anàlisi forense i malware, l'equip de Hunters & Intel·ligència.
- Assistència in situ quan correspongui (per exemple, recopilació de proves o coordinació de crisi in situ).
- Tots els serveis utilitzats en núvol, allotjats dins d'Europa, acomplint RGPD.

D'altra banda, l'adjudicatari haurà de treballar de forma coordinada amb l'adjudicatari dels altres lots amb la finalitat de garantir l'intercanvi d'informació necessari per a la protecció correcta de la infraestructura de MERCABARNA.

5.2.3. Gestió de vulnerabilitats

El servei SOC inclourà la realització d'**escaneigs periòdics de vulnerabilitats** sobre sistemes, aplicacions i xarxes de l'entitat. L'adjudicatari haurà de prioritzar els riscos detectats en funció de la seva **Criticitat tècnica i l'impacte potencial en l'organització**, recolzant-se en mètriques com el **CVSS**.

El servei contemplarà la generació d'informes periòdics, la integració de resultats en la plataforma SOC i la proposta de plans de resolució adaptats a la realitat tecnològica i operativa de l'entitat.

5.2.4. Intel·ligència d'amenaces (Threat Intelligence)

L'adjudicatari haurà d'aportar intel·ligència d'amenaces actualitzada, procedent de **fonts públiques, comercials i d'organismes oficials** (com el CCN-CERT), amb la finalitat d'enriquir la detecció i correlació d'esdeveniments.

Es requerirà la **generació d'informes estratègics i tàctics** que permetin a l'entitat anticipar-se a campanyes dirigides i millorar la presa de decisions en matèria de seguretat. L'adjudicatari haurà de garantir la capacitat d'**actualitzar en temps real indicadors de compromís (IoCs)** i aplicar-los sobre la infraestructura monitorada.

5.2.5. Threat Hunting proactiu

A més del monitoratge estàndard, el SOC haurà de comptar amb capacitats de **Threat Hunting**, és a dir, la recerca activa d'amenaces que puguin passar desapercebudes en els mecanismes automàtics de detecció.
Aquest servei inclourà la revisió de comportaments anòmals, l'anàlisi de telemetria avançada i la **proposta de nous casos d'ús** per reforçar les capacitats de detecció del SOC.

5.2.6. Servei de vigilancia digital i frau

El servei de SOC haurà d'incloure el servei de vigilància digital i frau, aquest servei està dissenyat específicament per a operadors d'infraestructures crítiques, per tal d'identificar i mitigar amenaces digitals que puguin comprometre la continuïtat del servei, la seguretat de la informació o la confiança dels usuaris. A través del monitoratge constant de fonts obertes, xarxes socials, fòrums, app stores i entorns deep/dark web, detectar campanyes de desinformació, suplantacions, fuites de dades sensibles i fraus dirigits. Aquesta capacitat proactiva permet reforçar la postura de Ciberseguretat, complir els requisits normatius (com NIS2) i protegir actius estratègics davant de riscos emergents.

5.2.7. Informes i reporting

Independentment que es pugui consultar la informació del sistema a través de quadres de comandament, l'adjudicatari haurà d'enviar informació sobre l'estat de la solució amb la periodicitat següent:

- Notificar immediatament per telèfon/correu aquells incidents greus de seguretat.
- Enviar un resum agrupat **mensual** (report mensual) per correu sobre l'estat general del monitoratge, indicant el nombre de sistemes que s'estan monitoritzant, el nombre d'esdeveniments de seguretat recollits, el nombre de sondes actives, el nombre d'esdeveniments/incidències de seguretat classificats per la seva Criticitat, incloent mètriques de detecció, gestió d'incidents, vigilància digital, frau i vulnerabilitats.
- **Informes trimestrals executius** amb tendències, anàlisi de riscos i recomanacions estratègiques per a la Direcció.
- **Informes ad hoc** en cas d'incidents crítics o a petició de l'entitat.

5.2.8. Pla de millora contínua

El SOC haurà de garantir un **model d'evolució permanent**, revisant i actualitzant de manera periòdica:

- Casos d'ús i regles de correlació.
- Procediments de resposta.
- Integracions amb noves eines de seguretat de l'entitat.
- Adaptació als canvis normatius aplicables (ENS, NIS2, PIC, RGPD).

5.2.9. Anàlisi forense digital sota bossa d'hores

S'inclourà en el contracte una **bossa d'hores anual d'anàlisi forense digital**, que es podrà activar a demanda i amb autorització prèvia de l'entitat.

Aquest servei cobrirà la investigació tècnica d'incidents mitjançant la **recuperació i anàlisi d'evidències** en endpoints, servidors o dispositius de xarxa. Els informes forenses elaborats hauran de ser complets i, si cal, amb **validesa legal** per a la seva aportació com a prova.

Complementàriament a les mesures de detecció i protecció, operació i resposta, cal comptar també amb serveis de resposta avançada que puguin proporcionar a MERCABARNA el suport i els coneixements tècnics necessaris per dur a terme investigacions forenses complexes i oferir capacitats de resposta i resolució immediates en situacions de crisi en què s'hagi compromès la seguretat.

Aquest servei s'ha dimensionat de manera orientativa en 32 hores anuals. MERCABARNA podrà consumir aquestes hores de manera flexible i podran ser acumulables en les següents anualitats en cas de no consum. MERCABARNA no te obligació de consum respecte a aquestes hores.

5.3. Estructura organitzativa del SOC

El servei haurà de comptar amb quatre nivells organitzatius, cadascun amb funcions clarament definides per garantir una resposta efectiva davant d'incidents de seguretat:

Nivell I – Analistes de Monitorització i Detecció

Responsables de la supervisió contínua d'alertes i amenaces, i filtrar la informació recopilada per la plataforma de monitorització per determinar si les alertes poden escalar a incidents de seguretat reals o si es tracta de falsos positius. A més, hauran de fer el seguiment de vulnerabilitats que afectin els actius identificats per la plataforma, així com el registre i la documentació d'incidències en els sistemes de gestió del SOC.

Nivell II – Analistes de Resposta i Gestió dels Incidents

Encarregats de respondre a incidents de seguretat després de l'anàlisi inicial, seguint una metodologia estructurada i procediments definits. La seva tasca inclou:

- Anàlisi detallada de l'incident, confrontant informació de diverses fonts per determinar-ne l'impacte en sistemes crítics i l'afectació de dades.
- Recomanació i aplicació de mesures de mitigació, proporcionant suport especialitzat en la contenció i la resolució d'incidents.
- Instal·lació, configuració i optimització de ferramentes de monitoratge d'amenaces i anàlisi de vulnerabilitats.
- Disseny i planificació d'escaneigs de seguretat a demanda, així com la creació de plantilles i informes d'anàlisi.

Nivell III – Experts en Seguretat i Resposta Avançada

Compost per especialistes altament qualificats en diferents àrees de la Ciberseguretat. Les seves funcions principals inclouen:

- Realització d'auditories tècniques per avaluar l'estat de seguretat de l'organització.
- Disseny de plans d'acció per a la millora contínua en la protecció d'actius.
- Anàlisi forense avançat, investigació d'incidents complexos, enginyeria de codi maliciós i resposta a ciberatacs sofisticats.
- Profund coneixement en xarxes, sistemes d'usuari, intel·ligència d'amenaces, tècniques forenses, infraestructura TI i aplicacions empresarials.

Nivell IV – Gestió i Coordinació Estratègica

Per garantir el correcte funcionament del SOC, caldrà comptar amb un mànager responsable de:

- Gestió i lideratge de l'equip, assegurant la coordinació entre els diferents nivells.
- Punt de comunicació per a incidents crítics, facilitant la presa de decisions i la interacció amb altres àrees de l'organització.
- Disseny i actualització del catàleg de serveis del SOC, assegurant-ne l'alineació amb els objectius estratègics de MERCABARNA.
- Optimització del rendiment de l'equip, garantint que les operacions s'executin de manera eficient i d'acord amb les millors pràctiques en Ciberseguretat.

5.4. Perfils professionals requerits

És requerirà una **experiència mínima de 3 anys** en funcions similars per a cadascun dels perfils. Tanmateix caldrà acreditar alguna de les següents **certificacions** per a els especialistes del SOC: CISM, CEH, OSCP o equivalents.

Perfil	Funcions i responsabilitats
Manager del Servei	Responsable de la supervisió i direcció del servei, interlocutor principal amb MERCABARNA, assegurant l'acompliment d'objectius, informes periòdics i gestió de millores
Especialista SOC – Nivell 3	Expert en anàlisis de Ciberamenaces, intel·ligència de seguretat i correlació d'esdeveniments a SIEM. Responsable de la estratègia de Ciberseguretat i suport a incidents d'alta Criticitat.
Especialista SOC – Nivell 2	Encarregat de la detecció, resposta a incidents i gestió de les amenaces en temps real, realitzant anàlisis forense i coordinació de mesures de protecció.
Especialista SOC – Nivell 1	Monitorització continua d'esdeveniments de seguretat, gestió d'alertes, anàlisis de logs i escalat d'incidents crítics

5.5. Durada del contracte

El servei de SOC haurà de començar el dia **1 de gener de 2026**, d'acord amb la planificació inicial, no obstant això, aquesta data podrà ajustar-se si les circumstàncies ho requereixen. I la seva durada serà de **3 ANYS, amb possibilitat de 2 pròrrogues addicionals d'un any cadascuna**. En cas que per canvi d'adjudicatari s'hagi de traspassar el servei a un nou adjudicatari, aquest disposarà de 30 dies per integrar el SIEM a el seu servei de SOC.

5.6. Acords de nivell de servei

El servei de Ciberseguretat SOC es gestionarà segons Acords de Nivell de Servei (SLAs - Service Level Agreements) amb l'objectiu d'establir compromisos clars en la qualitat del servei, garantir l'operativitat de les solucions de seguretat i mesurar l'eficàcia de la resposta davant d'incidents. Com a principals característiques, destaquem:

- Revisió periòdica de SLAs: El compliment dels SLAs serà revisat mensualment i semestralment, podent evolucionar de mutu acord entre les parts.
- Aplicació durant tot el servei SOC: Els SLAs aplicaran al servei de monitorització, detecció i resposta, assegurant la cobertura 24x7.
- Impacte de l'incompliment: L'incompliment dels SLA podrà derivar en penalitzacions segons les condicions del contracte.
- Informes de seguiment: Hauran de reflectir el nivell de compliment dels SLA i qualsevol desviació detectada.
- Penalitzacions: S'executaran sobre la base de la facturació mensual del servei, excloent-ne l'import de les llicències.

Definició de Temps de Resposta: Es considera temps de resposta el període transcorregut des de la identificació de l'incident fins a l'inici de les primeres activitats de diagnòstic i resolució.

Nivells de Temps de Resposta i Resolució segons criticitat:

Tipologia	Temps de resposta	Temps inici resolució
Alerta Mitja	16 hores	24 hores
Alerta Alta	4 hores	8 hores
Alerta Crítica	15 minuts	2 hores

5.7. Documentació a presentar

Amb la finalitat de verificar el acompliment dels requisits mínims d'obligat compliment, establerts al present document, l'oferta inclourà una memòria tècnica, amb com a mínim els següents apartats:

- Disseny del Servei SOC
- Governança del Projecte
- Rols i responsabilitats
- Pla detallat de treball
- Procediment de comunicació i coordinació entre SOC i equip intern
- Definició de SLA's i mètriques de servei

6. LOT 3. CONSULTORIA I ASSISTÈNCIA TÈCNICA PER A FORMACIONS, ADEQUACIÓ NORMATIVA I CERTIFICACIONS

6.1. Objecte

L'objecte d'aquest lot es disposar d'una bossa d'hores per a realitzar tasques dirigides a millorar i a conscienciar respecte la Ciberseguretat a MERCABARNA i al acompliment normatiu. Dins d'aquestes tasques, i sense caràcter limitant, es poden incloure certificacions en normativa de seguretat (ENS, NIS2, RGPD, PSO, PPE), auditories de Ciberseguretat tant interna, externa o especialitzades, formacions de Ciberseguretat, campanyes de conscienciació de pishing, formacions y consultoria estratègica.

6.2. Abast del servei

L'adjudicatari haurà de disposar de personal expert i certificat en Ciberseguretat, capaç de realitzar, com a mínim, les activitats següents, el dimensionament de les mateixes s'ha efectuat de manera orientativa per a que l'adjudicatari pugui entendre el Servei i fer-ne un dimensionament a nivell d'hores, MERCABARNA no té la obligació d'executar la totalitat de les tasques aquí indicades:

a) Acompliment normatiu i certificacions

- 3 renovacions de **ENS nivell Mitja** o, per defecte, **adaptació a la NIS2** durant la vigència del contracte.
- Assessoria continua en matèria de **ENS, NIS2, RGPD i normativa PIC**.

b) Auditories específiques

- 2 auditories de **Plan de Seguridad del Operador (PSO)**.
- 2 auditories de **Planes de Protección Específica (PPE)**.

c) Pentesting i probes tècniques

- 8 **exercicis de pentesting** (intern o extern).

d) Consultoria i formació

Bossa de **50 hores/any** destinada a:

- Consultoria estratègica en Ciberseguretat.
- Elaboració de polítiques i procediment.
- Formació i conscienciació del personal.

- Suport a la implantació de mesures tècniques i organitzatives.

Tots aquests serveis se consumiran a petició i prèvia aprovació de MERCABARNA. La dotació de la bossa d'hores s'ha fet de manera orientativa i, en cap cas, MERCABARNA està obligada al consum. La distribució de la mateixa durant la vida del contracte serà la següent:

CONCEPTE	3 ANYS	1 ANY	1 ANY
Renovació ENS o NIS2	2		1
Renovació PSO	1	1	
Renovació PPE	1	1	
Pentesting Inter/ Extern	6	1	1
Hores Consultoria	150	50	50

6.3. Durada del contracte

Els serveis de suport, consultoria, formació i tots els relacionats amb aquest lot, començaran el **1 de Gener del 2026** d'acord amb la planificació inicial, no obstant això, aquesta data podrà ajustar-se si les circumstàncies ho requereixen. I la seva durada serà de **3 ANYS**, amb possibilitat de 2 pròrrogues addicionals d'un any cadascuna.

6.4. Perfils professionals requerits

L'adjudicatari haurà d'assignar un equip de professionals altament qualificats amb experiència demostrable a Ciberseguretat, consultoria, compliment normatiu i protecció d'infraestructures crítiques.

Perfil	Funciones i Responsabilitats
Manager del Servei	Responsable de la supervisió i direcció del Servei, interlocutor principal amb MERCABARNA, assegurant el compliment d'objectius, informes periòdics i gestió de millores.
Especialista en acompliment normatiu i Govern	Responsable de l'adequació dels sistemes a les normatives com ENS, NIS2, RGPD, PSO, PPE. Elaboració d'informes de compliment i acompanyament en auditories.
Consultor/a sènior en Ciberseguretat	Especialista en Ciberseguretat responsable de l'elaboració de polítiques i plans estratègics.
Pentester / Analista tècnic	Responsable de l'execució d auditories de seguretat. Proves d'intrusió i anàlisi de vulnerabilitats a sistemes, xarxes i aplicacions.
Consultor/a junior	Especialista en Ciberseguretat amb menys de 3 anys de experiència.

6.5. Documentació a presentar

Amb la finalitat de verificar el acompliment dels requisits mínims d'obligat compliment, establerts al present document, l'oferta inclourà una memòria tècnica, amb com a mínim els següents apartats:

- Metodologia de treball
- Planificació i organització del servei
- Perfils professionals assignats
- Experiència i referències prèvies

7. LOT 4. RENOVACIÓ DELS TALLAFOCS, EL SEU SUPORT, MANTENIMENT I LLICÈNCIES

7.1. Objecte

L'objecte d'aquest lot es la renovació dels 2 Firewalls Watchguard M390, el seu suport, manteniment i llicències Watchguard Authpoint per a la franja de 51 a 100 usuaris concurrents.

7.2. Abast

7.2.1. Firewalls

L'abast inclourà la renovació triennal dels 2 Firewalls perimetrals actualment el model Watchguard M390. Tenint en compte que la primera renovació haurà d'executar-se durant el primer semestre del contracte, la segona renovació haurà d'ésser durant el primer semestre de l'any 2028.

Els Firewalls hauran de tenir iguals o millors característiques que els operatius al moment del canvi, sent models de la mateixa sèrie o superior, tanmateix hauran de ser nous, estar vigents en catàleg del fabricant, comptar amb el suport i garantia original del producte. No s'admetran productes re condicionats.

Aquests Firewalls hauran de tenir com a mínim les característiques dels Watchgurd M395, si bé s'espera que millorin les característiques:

- El dispositiu firewall ha de permetre la configuració de tres zones de seguretat: externa, privada i opcional (DMZ).
- El sistema del dispositiu firewall ha de ser compatible amb adreces IP estàtiques i dinàmiques (DHCP i PPPoE) a la interfície externa.
- El dispositiu firewall disposa de paràmetres de relé DHCP que permeten l'afegit de fins a tres servidors DHCP, amb la capacitat d'establir comunicacions concurrents amb fins a 3 servidors DHCP.
- El dispositiu firewall pot habilitar DHCPv6 a la interfície externa.
- El dispositiu firewall ha de suportar un rendiment mínim de 18 Gbps en mode firewall i 2,4 Gbps en mode UTM (combinant GAV i IPS).

- El dispositiu firewall ha de permetre un mínim de 4.500.000 connexions concurrents.
- El dispositiu firewall ha d'incloure polítiques de seguretat en application proxies preconfigurades amb valors segurs per defecte per donar suport als protocols habituals següents: (HTTP / HTTPS, POP3 / POP3S, IMAP / IMAPS, SMTP / SMTPS, FTP, DNS, SIP, H323).
- El dispositiu firewall ha de permetre l'autenticació mitjançant servidors RADIUS, SecureID, LDAP i Active Directory.
- El dispositiu firewall ha de ser compatible amb autenticació transparent amb servidors d'Active Directory (Single Sign-On).
- Eines per a protecció contra codi maliciós avançat:
    - Segon motor d'antivirus perimetral de nova generació (Intel·ligència Artificial)
    - Servei de sandboxing al núvol a Europa (RGPD)
    - Eina de detecció i resposta en lloc de treball per bloquejar codi maliciós avançat. Es valorarà que la solució sigui del mateix fabricant de la UTM
- Tots els serveis utilitzats en núvol, allotjats dins d'Europa, acomplint RGPD
- El dispositiu firewall ha de permetre establir llindars per a la detecció d'atacs de flooding i atacs de Denegació de Servei (DoS) i Denegació de Servei Distribuïda (DDoS).

Aquesta solució de seguretat ha de ser capaç de protegir cadascuna de les ubicacions contra les amenaces d'Internet mitjançant UTM (Unified Threat Management), combinant serveis de tallafoc, protecció antivirus, prevenció d'intrusions, filtratge de contingut, control de correu brossa, DLP, protecció avançada contra programari maliciós i VPN *site-to-site* per a usuaris remots, tot en un sol dispositiu.

- La solució UTM ha de donar suport a VPNs mòbils
- La solució de UTM ha de tenir els següents mecanismes d'autenticació:
  (3DES, AES 128 -, 192-, 256-bit)
- LA solució de UTM suporta, com a mínim el següent tipus de xifrat: (SHA-2, MD5, IKE Pre-Shared Key, 3rd Party Cert., AES with CBC and GCM
- La solució UTM pot classificar programes potencialment no desitjats (PUPs) com a programari maliciós
- El dispositiu UTM pot escanejar tots els fitxers comprimits (.zip, .tar, .rar, .gzip) amb múltiples nivells de compressió
- La solució UTM suporta el bloqueig automàtic de fonts conegudes d'atacs
- La solució UTM suporta un rendiment IPS d'almenys 3,3 Gbps
- La solució UTM Access Portal pot integrar-se amb els mecanismes d'autenticació existents al firewall, inclòs RADIUS, per a l'autenticació
- Ha de permetre als administradors executar un escaneig des del dispositiu firewall que genera un mapa visual de tots els nodes (endpoints) de la xarxa
- El dispositiu firewall suporta un mínim de 250 VLANs
- La solució UTM admet l'autenticació de Windows Active Directory.
- La solució UTM admet l'inici de sessió únic (SSO) per a inicis de sessió RDP

7.2.2. Bossa hores suport tècnic

S'oferirà una bossa d'hores per a suport tècnic tant dimensionada en base a 30 hores per any d'un tècnic amb, com a mínim, 3 anys d'experiència demostrable en la firewalls de la marca Watchguard. Aquesta bossa haurà de poder ser acumulable entre els anys i MERCABARNA no n'està obligada a el seu consum total o parcial.

7.2.3. Authpoint MFA

Renovació de les llicències Watchguard Authpoint MFA per a garantir la autenticació multi factor al núvol que permeti accedir als sistemes corporatius crítics mitjançant un segon factor d'autenticació, reduint dràsticament el risc d'intrusions.

7.3 Durada del contracte

El contracte de renovació, suport, manteniment i llicències, s'iniciarà **el 14 d'Abril del 2026**, data en que s'haurà d'activar els serveis i dur a terme la renovació dels Firewalls. La seva durada serà de **5 ANYS**.

7.4 Documentació a presentar

Amb la finalitat de verificar el acompliment dels requisits mínims d'obligat compliment, establerts al present document, l'oferta inclourà un resum executiu, amb com a mínim els següents apartats:

- Descripció de la solució tècnica proposada
- Planificació i organització del servei de renovació dels Firewalls
- Planificació i organització del servei de suport i manteniment de la solució
- Perfils professionals assignats
- Definició de SLA's i mètriques del servei de suport i manteniment

8. Condicions de la prestació de servei

Les condicions de prestació de servei se sustentaran en els punts següents:

- Els adjudicataris hauran de nomenar un interlocutor únic amb MERCABARNA, sent les seves responsabilitats fonamentals l'organització i la coordinació dels equips i les tasques de manteniment.

- A l'hora d'atenció i resolució d'incidències es distingirà entre temps de resposta i temps de resolució.
    - D'una banda, es defineix com a temps de resposta al temps màxim comptat a partir de l'avís d'incidència fins que el personal tècnic de l'adjudicatari contacti

amb el personal tècnic de MERCABARNA, inclosa la presència "in-situ" si fos necessari.

- D'altra banda, es defineix com a temps de resolució al temps comptat a partir del diagnòstic de la incidència pel personal tècnic de l'empresa adjudicatària fins que la incidència sigui resolta.

- L'horari normal de cobertura de servei a efectes del present PPT estarà comprès entre les franges horàries de 8.00 a 15.00 hores de dilluns a divendres en jornada laborable. Les situacions excepcionals detectades fora d'aquest horari i catalogades de criticitat alta hauran de ser ateses i resoltes segons SLA's definides.

- Els adjudicataris hauran de tenir disponibles tots els mitjans necessaris per donar servei, tant en horari normal com fora, i disposar dels mitjans de comunicació necessaris per a la seva localització.

9. Obligacions dels contractistes

LOT 1. Renovació de les llicències, del suport i manteniment dels programaris de Ciberseguretat existents a MERCABARNA

En cas que el contractista proposi un SIEM diferent a Rapid7 haurà d'estar en possessió de:

- **Esquema Nacional de Seguridad (ENS) Nivel ALT** Compliment amb el Real Decreto 311/2022, garantint els requisits de seguretat aplicables als sistemes d'informació del sector públic i empreses que presten serveis essencials.

LOT 2. Centre d'operacions de Ciberseguretat i serveis de resposta d'incidents i vigilància digital

L'adjudicatari del lot 2 haurà d'acomplir les següents normatives i estar en possessió dels següents certificats:

- **Esquema Nacional de Seguridad (ENS) Nivel ALT** Compliment amb el Real Decreto 311/2022, garantint els requisits de seguretat aplicables als sistemes d'informació del sector públic i empreses que presten serveis essencials.
- **ISO/IEC 27001** Sistema de Gestió de Seguretat de la Informació (SGSI), assegurant la confidencialitat, integritat i disponibilitat de la informació.
- **ISO 9001** Certificació de Gestió de Qualitat, garantint la millora continua i optimització de processos en la prestació de serveis.
- **ISO 14001** Certificació de Gestió Ambiental, assegurant el acompliment de normatives ambientals i sostenibilitat als processos operatius.

Pertinència a Xarxes i Organismes de Seguridad:

- **Red Nacional de SOC** Nivell OR. Integración en la Red Nacional de Centros de Operacions de Seguridad, garantint l'alineament amb les millors pràctiques i directrius nacionals en Ciberseguretat.

LOT 3. Consultoria i assistència tècnica per a formacions, adequació normativa i certificacions

L'adjudicatari del lot 3 haurà d'acomplir les següents normatives i estar en possessió dels següents certificats:

- **ISO/IEC 27001** Sistema de Gestió de Seguretat de la Informació (SGSI), assegurant la confidencialitat, integritat i disponibilitat de la informació.
- **ISO 9001** Certificació de Gestió de Qualitat, garantint la millora continua i optimització de processos en la prestació de serveis.

LOT 4. Renovació dels tallafocs, el seu suport, manteniment i llicències

L'adjudicatari del lot 4 haurà d'acomplir:

- Ser Partner Platinium de Watchguard

10. Diligència exigible

Els adjudicataris dels diferents lots, estaran obligats a garantir l'execució dels contracte amb la màxima diligència professional, assegurant que les activitats derivades del servei no comprometin la integritat, seguretat i disponibilitat de les infraestructures, actius i serveis de MERCABARNA.

En cas que hi hagi traspàs de llicències o serveis dels actuals adjudicataris a un de nou, ambdós adjudicataris hauran de garantir la continuïtat de serveis fins haver assolit el traspàs complert de totes les funcionalitats i serveis indicades als diferents contractes, sent transparent per MERCABARNA aquest traspàs.

Així mateix, els adjudicataris hauran d'executar els contractes en els termes previstos en aquest plec, assegurant una prestació de serveis competent i professional, complint amb els nivells de qualitat exigits i gestionant amb diligència els equips i les eines de MERCABARNA utilitzats en el marc del contracte.

A aquests efectes, els adjudicataris seran responsables de la qualitat tècnica dels treballs desenvolupats, així com de les prestacions i els serveis realitzats. També han de respondre per qualsevol conseqüència derivada d'omissions, errors, mètodes inadequats o conclusions incorrectes en l'execució dels contractes. En aquest sentit, s'exigeix que els adjudicataris actuïn amb la diligència esperada d'una empresa especialitzada en Ciberseguretat i compliment normatiu.

Els adjudicataris hauran de garantir la precisió i correcció de tots els documents i lliurables que aportin a MERCABARNA, comunicant immediatament qualsevol error detectat perquè es puguin prendre les mesures correctores oportunes. A més, seran responsable dels danys i perjudicis que puguin derivar-se de reclamacions realitzades per MERCABARNA, sempre que la causa estigui

directament relacionada amb errors en l'execució dels contractes, errors metodològics, males pràctiques o negligència dels adjudicataris o el seu personal.

11. Propietat intel·lectual

Tota la documentació que es generi com a part dels treballs inclosos a cada lot, es lliurarà en format electrònic i serà propietat de MERCABARNA, qui es reserva el dret de reproduir-los, publicar-los i divulgar-los, totalment o parcialment, sense que s'hi pugui oposar el autor material dels treballs.

Els adjudicataris de cada lot renunciaran de forma expressa a qualsevol dret que sobre els treballs realitzats com a conseqüència de l'execució del present contracte pogués correspondre'ls, i no podrà fer cap ús o divulgació dels estudis i documents utilitzats o elaborats en aquest contracte, bé sigui en forma total o parcial, directa o extractada, original o reproduïda, sense l'autorització expressa de MERCABARNA.

Pel que fa al llicenciament dels productes programari inclosos en els diferents lots, l'adjudicatari haurà de facilitar la documentació necessària on es acrediti el llicenciament de tots els productes inclosos al lot.

12. Confidencialitat de la informació

L'adjudicatari es compromet de manera expressa, tant durant la vigència del present contracte, com després de la seva extinció, a no difondre, transmetre, revelar a terceres persones qualsevol informació relativa amb MERCABARNA, a la qual tingui accés com a conseqüència de la realització dels treballs a desenvolupar a fi de cada un dels contractes, ni a utilitzar aquesta informació en interès propi o dels seus familiars o amics.

La prohibició establerta al paràgraf anterior s'estén a la reproducció en qualsevol suport de la informació a què tingui accés, procediments i sistemes d'organització, programes informàtics o qualsevol altre tipus d'informació interna, llevat que aquesta informació sigui estrictament necessària per al desenvolupament del contingut inherent a fi del contracte i es realitzi dins de l'àmbit del mateix. Tanmateix, totes les notes, informes i qualsevol altre document (incloent-hi els emmagatzemats en dispositius informàtics), elaborats pels recursos assignats durant la vigència del present contracte i que es refereixin a l'activitat de MERCABARNA.

La vulneració d'aquest compromís serà considerada causa justificada d'extinció d'aquesta adjudicació, sense dret a la percepció d'indemnització alguna.

En cas d'incompliment del compromís assumit i amb independència de l'extinció del contracte, MERCABARNA es reserva el dret de reclamar els danys i perjudicis que li poguessin causar com a conseqüència de la vulneració del deure de confidencialitat i secret professional pactat en aquesta clàusula.