EXPEDIENT PX SERV 04_24 (2024/00008714C)

PLEC DE CLÀUSULES TÈCNIQUES PARTICULARS PER A LA CONTRACTACIÓ MIXTA DE LA PRESTACIÓ DELS SERVEIS PER A LA MONITORITZACIÓ, LA GESTIÓ REMOTA I EL MANTENIMENT DELS ELEMENTS DE LA XARXA I DE LA CIBERSEGURETAT CORPORATIVA, AIXÍ COM DE LA RENOVACIÓ TECNOLÒGICA EN ELS EQUIPS DE XARXA OBSOLETS DE L'AJUNTAMENT DE GAVA (3 LOTS)

ÍNDEX

ANNEXOS:

Annex I. Inventari de programaris i equips de seguretat i de comunicacions, condicions de manteniment, gestió i SLA

Annex II. Gràfic d'enllaços Ajuntament de Gavà

Annex III. Actius candidats a integrar en la cibervigilància

PLEC DE CLÀUSULES TÈCNIQUES PARTICULARS DEL CONTRACTE MIXTE PER A LA CONTRACTACIÓ DE LA PRESTACIÓ DELS SERVEIS PER A LA MONITORITZACIÓ, LA GESTIÓ REMOTA I EL MANTENIMENT DELS ELEMENTS DE LA XARXA I DE LA CIBERSEGURETAT CORPORATIVA, AIXÍ COM DE LA RENOVACIÓ TECNOLÒGICA EN ELS EQUIPS DE XARXA OBSOLETS (3 LOTS)

EXPEDIENT PX SERV 04_24 (2024/00008714C)

OBJECTE GENERAL DEL CONTRACTE

L'**objecte** del contracte és la prestació del serveis de manteniment, monitorització i gestió dels elements de la xarxa corporativa i del sistema que gestioni els esdeveniment de seguretat d'aquests elements i d'altres diferents als elements de la xarxa, així com diferents serveis de ciberseguretat com el servei de seguretat de l'EndPoint, el servei de Centre d'Operacions de Segburetat (SOC), que va lligat al desplegament d'una eina de Gestió d'Esdeveniments i Informació de la Seguretat (SIEM).

En primer lloc, l'objecte del contracte és la prestació del **servei de manteniment, monitorització i gestió de la xarxa municipal, del sistema de telefonia IP corporativa i dels elements de seguretat corporatius tant software com hardware (perimetrals),** per un període de 3 anys. A aquest conjunt d'elements, en endavant, els podrem anomenar «xarxa» de l'ajuntament de Gavà. A l'Ajuntament de Gavà, el podrem anomenar, en endavant, Ajuntament.

També és objecte del contracte els **serveis de desplegament, manteniment, gestió i administració d'una solució de SIEM (Gestió d'Esdeveniments i Informació de la Seguretat) corporativa**, amb l'objectiu d'automatitzar al màxim possible la gestió dels esdeveniments de seguretat dels equips i sistemes corporatius (elements inclosos o no al conjunt «xarxa» esmentat en el paràgraf anterior), ser capaç de retenció d'evidències i logs de seguretat, efectuar l'anàlisi i correlació d'esdeveniments, generar alertes de seguretat a partir de l'anàlisi d'esdeveniments, i disposar de funcionalitats avançades com la detecció d'anomalies, l'anàlisi de comportament, o capacitats de resposta automatitzada, ja sigui de tipus SOAR (orquestració, automatització i resposta de seguretat) o – al menys - d'automatització de respostes mitjançant integració directe de SIEM i els sistemes corporatius si no es disposa d'un servei SOAR, entre d'altres capacitats i funcionalitats.

Conjuntament amb el desplegament anterior, i per un període de 3 anys, també és objecte del contracte els **serveis de SOC (Centre d'Operacions de Seguretat), que implementi els serveis propis d'un centre d'Operacions de Seguretat** com, per exemple, l'anàlisi, auditoria i assessorament en la ciberseguretat corporativa i en els actius implicats; el desplegament i optimització de la solució SIEM amb tots els requeriments propis de l'eina especificats més endavant; el disseny, implementació i integració de la monitorització de la seguretat dels actius implicats en l'eina en el SIEM; el disseny, implementació i integració dels casos d'ús, correlacions i workbooks; l'adopció de l'explotació del XDR corporatiu com un actiu més; les tasques de vigilància continua sobre la seguretat corporativa, mitjançant l'equip humà que implementi el servei de SOC i mitjançant l'eina SIEM desplegada; el servei de supervisió i monitorització 24x7 d'alertes del SIEM; l'execució d'operatives acordades (tiqueting i escalat), com poden ser tasques preventives, de detecció i de resposta; els automatismes que puguin ser integrats i oportuns per millorar la pro-activitat d'aquesta vigilància; la creació d'informes i propostes de millora en quan a la seguretat de forma

regular; evolució, creació i millora constant dels workbooks a implementar; el servei de resposta completa a un ciberincident greu en les condicions establertes més avall, el servei d'auditories i tests de seguretat, que sempre aportaran conclusions i indicacions per implementar les mesures correctives que se'n derivin de les seves conclusions; i, en general, totes aquells serveis propis d'un servei de SOC que es considerin adients i que el licitador ofereixi, més enllà dels esmentats i els requerits en l'apartat específic de servei SOC.

I, continuant amb aspectes de ciberseguretat, també és imprescindible i és objecte del contracte **la renovació de les llicències i el suport en l'eina de seguretat del punt final (End Point) corporatiu**, per un període de 2 anys.

Finalment, també és objecte d'aquest contracte una **renovació tecnològica dels equips de xarxa obsolets especificats**, així com d'equips de seguretat perimetral especificats que necessiten una renovació per motius operacionals (com és la capacitat de securitzar les comunicacions entre xarxes internes, i tenir capacitats computacionals suficient per fer-ho), com també l'ampliació del parc WiFi per a l'equipament seu dels mitjans de comunicació.

Tots aquests serveis són crucials per protegir la infraestructura de tecnologia de la informació i les dades sensibles que gestiona l'ajuntament l'ajuntament, així com per millorar les capacitats i prestacions en les comunicacions, tenint en compte la seva securització.

Donades les característiques de les prestacions a contractar s'estima convinent realitzar la divisió del contracte en (3) lots:

- LOT 1. Serveis de manteniment, monitorització i gestió dels elements de la xarxa corporativa i de la seguretat perimetral (tallafocs)
- LOT 2. Serveis de Ciberseguretat (SIEM i SOC)
- LOT 3. Renovació del sistema de seguretat XDR per als *End Point*

A continuació es detalla i fixen les prescripcions tècniques particulars que regiran en la contractació administrativa de contracte mixt per a la contractació de la prestació dels serveis per a la monitorització, la gestió remota i el manteniment dels elements de la xarxa i de la ciberseguretat corporativa, així com de la renovació tecnològica en els equips de xarxa obsolets(3 lots).

LOT 1. SERVEIS DE MANTENIMENT, MONITORITZACIÓ I GESTIÓ DELS ELEMENTS DE LA XARXA CORPORATIVA I DE LA SEGURETAT PERIMETRAL (TALLAFOCS).

Clàusula 1. Descripció i abast del servei

L'Ajuntament disposa actualment d'una xarxa corporativa de dades pròpia, suportada sobre tecnologies Ethernet, FO pròpia entre alguns edificis, VPN muntada amb electrònica pròpia sobre FTTH d'operadora per a la interconnexió d'altres edificis, interconnectant **36 edificis** corporatius, els quals donen servei a aproximadament **680 usuaris corporatius i 64 usuaris del servei d'aules**, més 3 ubicacions remotes a la via pública, connectades mitjançant tecnologia WiMAX, pera la gestió remota d'infraestructures municipals com són escales mecàniques i un ascensor públic. A banda, la majoria d'aquestes dependències i edificis també disposen de tecnologia WiFi gestionada.

<text complet disponible a la versió confidencial>

L'Ajuntament suporta, sobre la seva xarxa corporativa de dades, les comunicacions de veu IP entre els centres integrats en el sistema de veu *<text complet disponible a la versió confidencial>*, el tràfic corporatiu d'accés a Internet i comunicacions corporatives, i el tràfic dels serveis destinats als ciutadans esmentats anteriorment.

L'objecte específic d'aquest lot contractual són els serveis de gestió (gestió d'avaries i malfuncionaments i gestió del canvi), monitorització, manteniment i evolucions tecnològiques d'aquesta xarxa de telecomunicacions de l'Ajuntament i dels seus elements de seguretat perimetral corporatius, que podem resumir en els següents punts:

- **Monitorització** de tots els elements que conformen la xarxa municipal i que es descriuen i especifiquen al document «Annex I. Inventari de programaris i equips de seguretat i de comunicacions, condicions de manteniment, gestió i SLA.ods» del present plec de clàusules tècniques. Complementàriament, també s'aporta un altre annex al present plec de clàusules tècniques, anomenat «Annex II. Gràfic d'enllaços Ajuntament de Gavà.pdf», que descriu la tipologia física de la xarxa local i dels edificis que incorpora.
- **Manteniment** d'aquells elements que conformen la xarxa municipal i els elements de seguretat corporatius, que s'especifiquen, descriuen i s'identifiquen al mateix Annex I
- **Administració i gestió** remota de la xarxa municipal i dels serveis següents:
  - electrònica de xarxa
  - xarxa WiMax
  - xarxa Wifi
  - gestor d'ampla de banda
  - seguretat perimetral: firewalls, filtratge perimetral de navegació i d'altres mecanismes de protecció perimetral que s'implementen en l'equipament dedicat, i serveis VPN per a treballadors, equips i/o proveïdors
  - xarxes privades virtuals a la WAN municipal
  - comunicacions unificades / Telefonia IP

- **Servei específic 24x7 per les serveis centrals de la policia municipal, en matèria de telefonia i accés a la troncal de comunicacions i a Internet.**
- **Documentació i inventariat** dels elements de la xarxa i seguretat corporatius. Informes d'activitat.
- **Assessorament tecnològic i seguiment** del servei.
- **Renovació tecnològica d'equips de xarxa** obsolets especificats, així com **d'equips de seguretat perimetral** especificats que puguin entrar al seu final del cicle de vida durant el contracte o que necessitin una renovació per motius operacionals, com també l'**ampliació del parc WiFi** per a l'equipament seu dels mitjans de comunicació.

1.1 Servei de monitorització

Gestió automatitzada d'indicadors de funcionament i rendiment dels equips i components de programari que formen la xarxa de l'Ajuntament (relacionats a l'Annex I, i per als quals s'especifiqui individualment en aquest annex si es requereix o no aquest servei de monitorització), per detectar el més aviat possible les anomalies en el funcionament del programari i equips que conformen la xarxa, detectar desviacions dels estàndard de rendiment acordats amb l'Ajuntament, i generar les alertes corresponents pel contractista i per a l'Ajuntament via e-mail, a fi de restablir el servei en el temps acordat a l'Annex I per al servei de Manteniment dels equips.

El software de monitorització de rendiment de xarxes haurà de tenir, com a mínim, les característiques següents:

- Monitorització de disponibilitat i temps de funcionament.
- Monitorització de tràfic i utilització.
- Monitorització de l'estat general de cada element.
- Mapes de xarxa.
- Monitorització de temps de propagació en ambdós sentits en xarxes d'Àrea amplia.
- Generació d'alertes automàtiques definides segons paràmetres de llindars i enviament automàtic de les mateixes mitjançant correu electrònic.
- Que el sistema de monitorització permeti integrar-se, en general, amb tecnologies tipus SIEM mitjançant la injecta de logs dels esdeveniments en un sistema de recol·lecció de logs extern.

Tota la informació sobre disponibilitat dels enllaços i equips de la xarxa ha de ser mostrada en forma de mapa amb la topologia real de la xarxa, amb descobriment automàtic de dispositiu, sent fàcilment interpretable l'estat dels dispositius pel personal de l'Ajuntament, que rebran la formació adient, per interpretar aquests mapes d'estat de la xarxa. Aquests mapes haurien de ser consultables des de la xarxa municipal o des de fora amb les garanties de seguretat adequades pels tècnics designats per l'Ajuntament. S'ha de posar a disposició dels tècnics municipals una eina web amb informació online sobre l'estat dels equips, servidors i serveis monitoritzats.

Haurà de mostrar, de manera gràfica, la topologia de la xarxa; i amb codi de colors el seu estat de disponibilitat, enllaços i equips.

El sistema recollirà també un històric d'aquests indicadors.

La plataforma de monitorització hauria de estar preparada per fer també monitorització de rendiment de servidors, físics o virtuals, windows o linux, ja que hi han elements de l'Annex I a gestionar i monitoritzar que es basen en servidors virtuals, com per exemple els servidors virtuals que suporten la telefonia IP corporativa.

La posada en marxa del servei inclourà la parametrització de l'equipament i de les plataformes de gestió instal·lades a les dependències del client: presentació de dispositius, configuració vistes de negoci, configuració d'indicadors, configuració d'alertes i configuració de logs.

1.2 Servei de manteniment

Un dels objectius d'aquest contracte es garantir la màxima disponibilitat i eficàcia dels equipaments d'electrònica de xarxa de l'Ajuntament i dels components de programari associats a aquests sistemes de xarxa i als mecanismes de seguretat perimetral (*Annex I*).

Per això l'adjudicatari posarà tots els recursos materials i/o gestions necessàries per solucionar les possibles avaries o caigudes de rendiment dels elements identificats (relacionats a l'Annex I esmentat, i per als quals s'especifiqui individualment que es requereix aquest manteniment), ja siguin detectades per l'Ajuntament, o pel sistema de monitorització, en els temps especificats per a cada equip al mateix Annex I, a la seva columna SLA.

Les solucions podran consistir en la reparació o substitució per equips de prestacions equivalents o superiors a l'equip avariat, i la seva posterior instal·lació i posada en marxa de l'equip amb les configuracions anteriors de les que l'adjudicatari haurà de tenir còpia dins del servei de Inventariat de la Xarxa. Aquestes solucions s'implementaran mitjançant actuacions remotes o presencials de tasques de manteniment i/o de reparació, gestió de tasques de manteniment i/o reparacions amb els fabricants, enviament i recepció de material implicat, aportació de material de stock propi quan no sigui possible el contracte amb el fabricant per obsolescència, tasques d'instal·lació física si es requereix en l'acció de manteniment i/o reparació i, en general, tots els recursos materials i/o gestions necessàries per a tal solució. Previ acord entre les dues parts en cada cas concret, i amb l'objectiu d'agilitzar la subtitució d'equips en la resolució d'una avaria, el mantenidor també podrà disposar de l'stock del que disposa l'Ajuntament, com per exemple *<text complet disponible a la versió confidencial>*.

Per tant, és requeriment que adjudicatari activi contracte de manteniment amb els respectius fabricants per a la durada del contracte i per a tots els components per als que «es requereix manteniment» en l'Annex I, excepte per a aquells components per als no sigui possible el contracte amb el fabricant per obsolescència, cas en que el les tasques de manteniment s'efectuaran amb recursos propis de l'adjudicatari, com ja s'ha esmentat. Per el cas d'equips que arribin a la seva obsolescència durant la durada del contracte, és igualment requeriment que adjudicatari activi contracte de manteniment amb els respectius fabricants fins la data que el fabricant accepti. Més enllà de la data, les tasques de manteniment també s'efectuaran amb recursos propis de l'adjudicatari.

<text complet disponible a la versió confidencial>.

En el cas que sigui necessària una substitució d'equip o de component de programari per a la resolució de la incidència o avaria, tot els nous equips o components de programari instal·lats en aquesta resolució entraran a formar part del parc d'equipament de xarxa corporatiu i, per tant, entraran automàticament a formar part dels equips i components objecte dels serveis de monitorització, manteniment, gestió i administració, documentació i inventariat, assessorament i seguiment de la xarxa municipal, en detriment d'aquells substituïts que causin baixa en aquest inventari, per als quals es deixarà de requerir aquests mateixos serveis associats.

Com a mínim, aquest serveis consistiran en el diagnòstic remot de incidències i, en cas de averia, reposició de hardware amb la última configuració coneguda, i amb assistència de tècnic presencial si l'Ajuntament ho considera necessari; o en el cas l'avaria sigui sobre un component software i la seva resolució ho requereixi, reinstal·lació amb la darrera configuració coneguda, amb assistència de tècnic presencial si l'Ajuntament ho considera necessari.

Si un nou equip de substitució va associat a un programari i/o llicenciament del mateix, s'entén que aquest haurà d'estar també proveït i mantingut en configuració i llicenciament necessaris.

En quant al cas específic de l'electrònica de xarxa, molts dels equips relacionats en *l'Annex I* tenen en explotació alguns ports amb components inseribles tipus SFP / GBIC. Les avaries d'aquests components addicionals en explotació en aquesta electrònica també són objecte de manteniment en aquest contracte, tot i que no es detallen en l'esmentat *Annex I*. S'admetrà manteniment d'aquests components addicionals amb stock propi del licitador.

L'Ajuntament tindrà un accés via Internet a la gestió de les seves incidències, així com als identificadors/números de contracte de l'adjudicatari amb els fabricants. Això és necessari per que l'Ajuntament pugui validar que l'adjudicatari ha realitzat la contractació de cada manteniment amb el corresponent fabricant.

En el cas de que no sigui possible disposar o renovar algun manteniment amb el fabricant únicament per causa d'obsolescència de l'element, l'adjudicatari ho haurà d'indicar i haurà de respondre amb stock propi del mateix element o de prestacions superiors. És per això que es requereix, amb la memòria tècnica de l'oferta, que s'adjunti prova gràfica de l'stock propi (fotografies de l'stock propi) i documental (document EXCEL o PDF amb el llistat de l'stock propi) del que es disposi, en coherència amb la tipologia de marques i models del inventari indicat en l'Annex I (*<text complet disponible a la versió confidencial>*).

Els components de programari mantinguts hauran d'estar correctament llicenciats, amb contracte de manteniment i suport actiu amb el fabricant durant tot el període de validesa del contracte, amb les mateixes modalitats de llicenciament de las que es disposa a l'inici d'aquest contracte, o bé amb les modalitats actualitzades de llicenciament, si és que el fabricant així ho requereix.

Per al cas concret de la telefonia IP, però, *<text complet disponible a la versió confidencial>*.

Es farà una revisió preventiva anual, incloent: revisió d'equips, inventariat, actualitzacions de

firmware bàsiques per recomanació del fabricant.

L'incompliment en els temps de reposició dels equips estipulats a l'Annex I, comportarà les penalitzacions econòmiques que es determinaran en l'apartat corresponent del plec administratiu d'aquesta licitació.

1.3 Servei d'administració i gestió remota de la xarxa i dels serveis associats

Consistirà a la realització de canvis de configuració i suport a la explotació de la infraestructura relacionada a l'*Annex I,* en resposta a una sol·licitud de l'Ajuntament, o a la desviació en el comportament normal dels elements monitoritzats, detectada pel servei de monitorització, i referent a tots els serveis esmentats anteriorment en la introducció:

- electrònica de xarxa
- xarxa WiMax
- xarxa Wifi
- gestor d'ampla de banda
- seguretat perimetral: firewalls
- xarxes privades virtuals a la WAN municipal
- comunicacions unificades / Telefonia IP

El temps de resolució per peticions d'administració i gestió remota dels equips components de programari objecte del contracte serà com a màxim de NBD (següent dia laborable). Es valorarà la millora d'aquest temps de resolució.

Si el grau de criticitat d'un canvi programat ho requereix, l'adjudicatari desplaçarà un tècnic a l'Ajuntament.

Els serveis d'administració constaran, com a mínim, dels següents treballs:

- Gestió de peticions de canvis de configuració en la infraestructura IT de l'Ajuntament detallada a l'annex I.
- Gestió de mesures correctives davant una desviació en el comportament normal (canvis de configuració, canvis de firmware, etc.)
- Gestió de mesures correctives derivades d'auditories i tests de seguretat (canvis de configuració, canvis de firmware, etc.), sempre i quan aquestes actuacions puguin ser implementades amb els hardware i software de xarxa i seguretat contractats i gestionats pel licitador, amb l'objectiu de resoldre els problemes de seguretat diagnosticats en aquests tests. Si els resultats d'aquests test fessin palesa la necessitat de noves adquisicions de hw o sw addicional, o de la contractació de nous serveis, no inclosos en aquesta licitació, l'adjudicatari no tindrà l'obligació d'aportar aquestes solucions addicionals.
    - **NOTA: No és objecte d'aquest LOT 1 l'execució d'aquests tests i auditories, que es contracten en un altre lot d'aquesta mateix licitació. Només ho són les accions correctives sobre els equips i sistemes gestionats que es derivin d'aquests tests i auditories de seguretat, o qualsevol altre test o**

auditoria aportat per les agències de seguretat governamentals o per propi ajuntament de Gavà. Tanmateix, sí que es demana la pro-activitat en l'actuació sobre els sistemes gestionats en aquest LOT 1, per tal d'anticipar al màxim aquesta possible necessitat de canvi o actualització, tal com s'esmenta en el següent punt.

- Gestió anticipada proactiva, prèvia a una desviació en el comportament normal recomanades pel fabricant (actualització de firmware, pedaços de seguretat, actualització de versions, etc.).
- Realització d'activitats periòdiques programades proactives, com la comprovació periòdica de l'alta disponibilitat de dispositius crítics, canvi anual de passwords en dispositius, entre d'altres que l'adjudicatari cregui convenients.
- Còpies de seguretat i emmagatzematge remot de totes les configuracions dels equips, sistemes i programaris gestionats i/o mantinguts en aquest lot. És totalment requerit que l'adjudicatari faci periòdicament (mínim quinzenal) tasques de backup de totes les configuracions dels equips i sistemes administrats (electrònica, firewalling, antenes WIMAX i WiFi, serveis/aplicacions ToIP, etc.).
- Resolució de consultes tècniques en l'entorn administrat.

Qualsevol nova funcionalitat introduïda a qualsevol dels equips i programaris relacionats (ja siguin existents o de nova incorporació) ha d'estar contemplada en aquest servei d'administració i gestió remota.

1.4 Servei 24x7 per als serveis centrals de la policia

Per la policia municipal es prestarà un servei específic 24x7 per atendre avaries de telefonia i/o en l'accés dels usuaris i equips de la Policia Municipal a l'electrònica de l'edifici, a la troncal de comunicacions i a Internet, on resideixen eines de gestió policial claus per al funcionament d'aquest cos policial.

Les alarmes generades pel servei de monitorització que corresponguin als elements inclosos en aquest servei de la policia (elements diferenciats explícitament a l'annex I, a la columna «Servei Policia Municipal») generaran una resposta automàtica per part del contractista per tal d'atendre i solucionar la incidència.

Un grup restringit de personal municipal seran les autoritzades a comunicar-se amb el proveïdor per notificar una avaria, si és que no s'ha detectat ja prèviament. Es determinarà el protocol de comunicació d'incidències a seguir en aquestes comunicacions conjuntament amb l'empresa contractista (un correu electrònic específic, un número de telèfon específic, o el que s'acordi conjuntament).

Aquest servei entraria en funcionament a partir de les 15 hores i fins les 8 hores del dia següent laborable i els caps de setmana i festius les 24 hores.

Les incidències produïdes per als components identificats en el servei 24x7 per a la policia municipal han de tenir una resposta **immediata**, a banda de complir l'abast i condicions de servei especificats a l'apartat «Nivell de servei, horaris i canals de comunicació» conjuntament amb l'especificat a l'annex I.

1.5 Sistemes de seguretat perimetral

<text complet disponible a la versió confidencial>.

Per tant, també és objecte d'aquest contracte, i així es remarca en aquest apartat, la gestió remota, monitorització i manteniment d'aquests equips de seguretat perimetral (o dels nous que els substitueixin dins l'àmbit d'aquest contracte, indicats en l'apartat corresponent a renovació tecnològica), **però també l'assessorament tècnic continuat, suport, propostes de millora i implantació de les polítiques i mecanismes de seguretat que aquest equipament ens pugui dotar**.

Un dels objectius primordials de l'empresa contractista serà la gestió dels mecanismes de seguretat corporatius d'una forma proactiva i, per tant, **se li exigirà que faci proposta continuada de millora en l'aprofitament d'aquest equipament de seguretat perimetral i de tots els mecanismes de seguretat que pot assolir, essent un tema destacat en les reunions de seguiment mensual del servei.**

1.6 Renovació tecnològica d'equips de xarxa, d'equips de seguretat perimetral, i ampliació del parc de punts d'accés WiFi

<text complet disponible a la versió confidencial>

- **Serveis associats a aquestes renovacions tecnològiques**

Tot els equips (electrònica, tallafocs) substituïts i renovats, substituiran a tots els efectes del contracte del LOT 1 als equips retirats, en les mateixes condicions esmentades a l'Annex I, en quant a manteniment, monitorització, administració i gestió.

Anàlogament, tots els punts d'accés WiFi subministrats, s'incorporaran a tots els efectes dins el contracte del LOT 1, amb les mateixes condicions que la resta d'equips d'accés WiFi ja presents a l'Annex I, en quant a manteniment, monitorització, administració i gestió.

L'oferta ha d'incloure tots els serveis necessaris per deixar en explotació els nous equips. Per tant, ha d'incloure, com a mínim, els serveis de instal·lació i configuració de tots els switch, firewall i punts d'accés WiFi subministrats (incloent els nous punts de terra per a aquests punts WiFi), segons les especificacions del personal tècnic municipal i les configuracions acordades per ambdues parts, incloent la configuració de polítiques de seguretat perimetral, configuració de VPN, configuració de VLANs, entre molts d'altres aspectes, mantenint com a mínim els mateixos serveis i prestacions que actualment suporten els equips substituïts. Els equips han de quedar instal·lats i en funcionament, de manera que l'adjudicatari aporti tot aquell component addicional o petit material necessari (cargols, ancoratges, farratge, connectors, cablejats, nous punts de terra per als punts WiFi, etc.), que en cap haurà de subministrar l'ajuntament de Gavà. Anàlogament, els nous punts de xarxa instal·lats per als nous punts WiFi subministrats,

També ha d'incloure l'activació del servei de garantia, manteniment i gestió remota per als equips esmentats, amb un SLA equivalent als equips substituïts segons especificacions SLA de l'Annex I. Òbviament, aquest servei ha d'incloure sempre el servei de garantia i/o manteniment dels propis fabricants. Els nous equips s'incorporaran als inventaris dels equips sota el contracte amb l'adjudicatari del lot I a tots els efectes del mateix contracte.

➢ **Serveis addicionals d'adequació tecnológica**

Tot i que l'administració i gestió remota dels equips gestionats ja ha d'estar inclosa en l'oferta, tal com s'ha especificat en els apartats anteriors, volem aquí ressaltar unes tasques tècniques de suport, que podran ser en remot, i que es requeriran al licitador:

- Suport per posar en funcionament la nova connexió de fibra òptica pròpia de la que l'ajuntament ja disposa entre els centres CSE i Museu de Gavà:

  - *<text complet disponible a la versió confidencial>*

- Reubicació del «Fw_01.cse» a la seu de Gavà TV:

  - *<text complet disponible a la versió confidencial>*.

Aquestes tasques podran ser portades a terme en remot, amb el suport del personal municipal, i es gestionaran via peticions/tickets ordinaris de gestió i administració remota. Però es vol amb aquest apartat ressaltar aquestes tasques que modificaran en breu la topologia de la xarxa especificada a l'annex II.

1.7 Servei de documentació i inventariat

Generació i **actualització** de tota la documentació necessària per prestar el servei de gestió de la xarxa. El contractista s'haurà d'habilitar un accés permanent a través de Internet a tota la documentació actualitzada per l'Ajuntament:

➢ **Generació i actualització de la documentació de la instal·lació física i inventariat de la infraestructura del client:**

- Identificació i etiquetat del hardware al lloc de la instal·lació.
- Documentació fotogràfica de la disposició de hardware als armaris de comunicacions e identificació segons denominació en l'etiquetat.
- Identificació i registre del fabricant, model i números de sèrie dels components hardware.
- Identificació i registre del fabricant i codis de llicenciament dels components software.
- Versions de firmware/software/sistema dels dispositius.
- Dades d'accés i autenticació per la gestió de cada element de maquinari o programari, direccionament de xarxa, nom lògic i qualsevol altre dada requerida pels tècnics de l'Ajuntament.
- Inventariat de configuracions dels dispositius.

➢ **Generació i actualització de la documentació operativa i d'explotació pel servei de gestió remota:**

- Esquemes topològics de connexionat físic de xarxa per cadascun dels centres que la conformen i la relació entre ells.

- Detalls de les línies de comunicacions, incloent números administratius i lloc d'instal·lació.
- Diagrames de connexionat lògic dels dispositius.
- Esquemes lògics dels diferents components de programari implicats en la xarxa

➢ **Anàlisi i informes:**

L'anàlisi de la informació i indicadors proporcionats per la plataforma de monitorització i pel servei d'administració estableix una línia base de funcionament normal. Les desviacions d'aquesta normalitat seran analitzades i reportades periòdicament, i s'inclourà com a mínim:

- Informes mensuals:
  - Esquema topològic i inventari.
  - Diagrames i gràfiques dels indicadors monitoritzats acordats a incloure en els informes.
  - Evolució de l'entorn gestionat.
  - Incidències i actuacions preventives y correctives destacables realitzades sobre la infraestructura IT.
  - Conclusions i recomanacions.
- Checklist diari:

  En aquest informe es verifica diàriament de manera senzilla i clara l'estat operacional de serveis crítics a la infraestructura IT, executant els procediments acordats al observar-ne alguna desviació. S'enviarà cada dia a les 8:00 hores als e-mails que determini l'Ajuntament.
- Reporting Online:

  L'Ajuntament podrà accedir de forma remota a les següents informacions
  - Consulta del estat actual i històric de incidències.
  - Consulta del nivell de servei (SLA) real.
  - Reporting específic de la plataforma de monitorització.
  - Consulta de Documentació i Inventariat.

1.8 Servei d'assessorament tecnològic i seguiment del servei

Es farà un seguiment mensual del servei amb un gestor amb coneixements detallats del nostre entorn assignat pel contractista amb el responsable del sistemes i comunicacions de l'Ajuntament on s'avaluaran els aspectes següents:

- El funcionament del servei i el compliment dels nivells de servei establerts a l'annex I,

determinant-se les penalitzacions econòmiques que corresponguin per incompliment d'aquest, que seran aplicades a la següent factura.

- Estat de les incidències i sol·licituds en curs.
- Explicació dels informes periòdics.
- Propostes de millora sobre els actius hardware i software gestionats i administrats
- Propostes de possibles futurs projectes sobre els sistemes, equips i xarxa corporativa, que tinguin l'objectiu de millorar, actualitzar, enfortir, racionalitzar o qualsevol altre aspecte positiu la infraestructura TIC corporativa.
- Establiment de tasques planificades de manteniment o millora.

Clàusula 2. Coordinació del servei

L'adjudicatari nomenarà una persona de contacte que serà el coordinador/a de tots els assumptes relacionats amb la gestió i manteniment de la xarxa de l'Ajuntament i tots els serveis associats.

Aquesta persona haurà de tenir una visió global i integradora de la nostra xarxa i de les seves incidències i disposar de la capacitat tècnica suficient i suficient i elevats coneixements del funcionament dels actius gestionats És amb aquesta persona amb la que es faran les reunions mensuals de seguiment dels serveis, per proposar millores i resoldre els possibles conflictes.

Haurà d'estar sempre localitzable telefònicament (o comunicar expressament en cas de indisponiblitat, la persona que el substituirà), no per resoldre incidències que es farà a través de les vies de contacte normal, sinó per resoldre casos excepcionals d'atenció no satisfactòria.

La idoneïtat de la persona designada per l'empresa contractista com a coordinador/a («service manager») serà lliurement apreciada pel responsable del contracte que es designi per part de l'Ajuntament de Gavà, podent exigir en tot moment al contractista la seva substitució en ares a una bona execució del contracte.

Dins la coordinació del servei, està implícita la coordinació amb els fabricants als que l'adjudicatari contracti els manteniments i llicenciaments dels diferents elements administrats i gestionats, per tal de notificar avaries i, així, es procedeixi a la seva reparació o canvi en la major brevetat.

Clàusula 3. Nivell de servei, horaris i canals de comunicació

L'Ajuntament necessita que la xarxa municipal funcioni contínuament les 24 hores al dia els 365 dies de l'any. A efectes d'aquest servei es considera horari laboral normal el que va de dilluns a dijous de 8:00 a 18:00 hores i divendres de 8:00 a 15:00 hores. Tanmateix, la resta d'horari i dies també hi ha serveis funcionant, com per exemple els serveis policials:

- Quan a l'*Annex I* es parli de nivell de servei NBD (next business day), es referirà a que el serveis suportats per l'ítem hauran de restablir-se com a màxim al següent dia laboral. Tanmateix, el temps de resposta per a un SLA NBD davant de l'apertura de

la incidència s'haurà d'efectuar en els 30 següent minuts de la mateixa.

- Quan en el mateix *Annex* I es parli de 24x7, es refereix a que el servei s'atendrà 24 hores al dia, 7 dies a la setmana. I afegirem a continuació el nombre de hores en que ha de estar resolta la incidència. Per exemple, en el cas dels equips crítics serà 24x7x4h, es a dir, es referirà a que els serveis suportats per l'ítem hauran de restablir-se com a màxim en 4 hores per a tots els dies. Tanmateix, el temps de resposta a un SLA 24x7 davant de l'apertura de la incidència s'haurà d'efectuar en els 30 següent minuts de la mateixa.

Per cada component de la xarxa, s'estableix el seu nivell de servei a l'Annex I.

El servei de manteniment amb reparació o substitució de components avariats s'ha definit en aquest annex depenent de la criticitat de l'equip o component, i basant-nos també en la redundància disponible per mantenir el servei.

El servei automàtic de monitorització i alertes funcionarà en horari 24x7.

El servei de gestió atendrà peticions dels tècnics de l'Ajuntament, com a mínim, en l'horari laboral normal definit.

En quant a les volumetries del serveis de manteniment, gestió i administració remota dels actius, i tenint en compte que el personal tècnic propi de l'ajuntament té assolida prou autonomia en aquestes tasques com per resoldre per sí mateix gran part de les incidències o necessitats de canvi que es produeixen, l'adjudicatari haurà d'atendre la totalitat de les incidències/peticions/consultes que es generin durant tot el contracte sobre el seu servei, tenint com a referència que les volumetries aproximades actuals són de 250 incidències/peticions/consultes anuals aproximadament generades.

En el mateix annex I esmentat, s'identificaran els equips que donen servei a la telefonia, a l'accés a la troncal de comunicacions i a l'accés a Internet per als serveis centrals de la policia municipal, subjectes al tractament específic en els mecanismes de comunicació automàtica i/o humana de les avaries o incidències de funcionament que afectin a aquests serveis, i als mecanismes de resposta immediata establerts en l'apartat *2.4 Servei 24x7 per als serveis centrals de la policia*. Els SLA associats als equips dins aquesta consideració es defineixen amb la mateixa nomenclatura establerta anteriorment, i dins el mateix l'Annex I.

Es valorarà la millora en qualsevol dels paràmetres referents a SLA esmentats en aquest plec.

Clàusula 4. Posta en marxa del servei

La durada de la posta en marxa de la plataforma de monitorització i de la plataforma de ticketing no podrà ser superior a 1 mes després de la signatura del contracte.

A partir d'aquest moment es rebran els informes establerts, les alertes generades, i es tindrà accés a la plataforma de *tickets* per fer sol·licituds o incidències.

Clàusula 5. Devolució del servei

Durant l'últim mes previ a la finalització del contracte, en cas que l'empresa contractista que executa el contracte no resulti adjudicatària del nou servei, aquesta haurà de lliurar sota la supervisió de l'Ajuntament de Gavà, totes les dades administratives y tecnològiques que siguin necessàries a l'ajuntament per donar continuïtat a l'administració, gestió i manteniment de tots els equips programaris implicats en l'Annex I.

Com exemple d'aquestes informacions haurà de lliurar:

- Contractes de manteniment amb els fabricants.
- Accés a les plataformes de descàrrega de softwares i firmware dels fabricants d'elements gestionats.
- Inventaris d'equips hardware i plataformes software gestionades, que inclogui, entre d'altres informacions, el mètode d'accés, les credencials d'accés, certificats i credencials de certificats involucrats i , en general, qualsevol altra informació que es consideri rellevant per a poder donar continuïtat a la seva gestió i administració per part de l'ajuntament.
- Les còpies de seguretat del darrers 30 dies de les configuracions dels equips i programaris gestionats o mantinguts.
- Mapes lògics i físics descriptius de la xarxa i equips i programari associats
- En general, totes les dades i informacions que tinguin relació amb el conjunt d'equips i programaris administrats i gestionats en el contracte sortint, i que puguin ser necessaris en un futur al personal tècnic de l'ajuntament.

Clàusula 6. Memòria tècnica LOT 1

Els licitadors hauran de presentar en el SOBRE B per a la seva avaluació mitjançant judicis de valor, **una memòria tècnica, amb d'un màxim de 25 planes (Arial 11 interlineat senzill) sense comptar l'apartat d'Annexes, portada i índex,** amb el detall i contingut mínim següent:

1.Explicació del funcionament i gestió dels serveis.

Haurà d'incloure com a mínim l'explicació dels següents conceptes:

- Servei de manteniment: Com es durà a terme aquest servei, tipologia de contractes amb els fabricants, sistemes d'atenció, comunicació i seguiment de les incidències de manteniment...etc.

    - **Nota:** Es podrà fer referència per a aquesta explicació al contingut dels annexos que caldrà incloure amb la memòria (veure apartat «5. Annexes» d'aquest índex mínim per a la memòria tècnica), els quals documentaran gràficament (mitjançant fotografies) i documentalment (mitjançant un llistat en format PDF o EXCEL) l'inventari de maquinari en stock propi que podria utilitzar-se per resoldre avaries de maquinari en el cas especificat en el que el maquinari avariat ja no pugui estar en contracte de manteniment amb el

fabricant per obsolescència.

- Serveis de suport, serveis i sistemes de monitorització, servei de gestió remota.
- Serveis i mecanismes de documentació i inventariat.
- Servei de assessorament tecnològic i seguiment dels serveis, coordinació i interrelació entre tots els serveis.

2. Explicació del funcionament específic del servei de suport 24x7 per la policia municipal d'acord amb el que es demana als plecs tècnics.

3. Solució proposada per a la renovació tecnològica

- Equipament, llicenciaments inclosos, condicions del servei, planificació, metodologia, etc. Millores en components i/o prestacions de la solució de renovació tecnològica respecte al mínim especificat en el plec tècnic, si se'n ofereixen.

4. SLA proposat de cadascun del serveis

- Proposta dels SLA, a partir dels mínims establerts a l'Annex I del plec tècnic, i segons la nomenclatura definida a la clàusula 3 Nivell de servei, horaris i canals de comunicació de les prescripcions tècniques. Caldrà detallar o destacar en aquest apartat aquells punts on s'ofereixi una millora respecte als mínims requerits, ja sigui en temps de resposta i/o en temps de resolució, identificant sempre en quins dels ítems de l'Annex I s'aplicaria cada millora proposada.

5. Annexes

5.1 Document EXCEL o PDF amb el **llistat de l'stock propi** del que es disposi, per a l'atenció de possibles equips en EOL.

5.2 **Fotografies de l'stock propi** (del magatzem complet, o del materials que conforma l'stock de forma agrupada o individual,...etc.).

LOT 2. SERVEIS DE CIBERSEGURETAT (SIEM I SOC)

Clàusula 1. Descripció i abast del servei

<text complet disponible a la versió confidencial>

És objecte d'aquest lot la contractació dels serveis de desplegament, manteniment, gestió i administració d'una solució de SIEM (Gestió d'Esdeveniments i Informació de la Seguretat) corporativa, amb l'objectiu d'automatitzar al màxim possible la detecció, identificació i gestió dels esdeveniments de seguretat dels equips i sistemes corporatius, ser capaç de retenció d'evidències i logs de seguretat, efectuar l'anàlisi i correlació d'esdeveniments, generar alertes de seguretat a partir de l'anàlisi d'esdeveniments, i disposar de funcionalitats avançades com la detecció d'anomalies, l'anàlisi de comportament, capacitats d'automatització de la resposta davant incidents de seguretat, entre d'altres.

Per altra banda, tot i que els tècnics IT municipals responsables dels sistemes mantenen la seva responsabilitat sobre la seguretat de la xarxa i els sistemes corporatius, també són responsables de la direcció i/o execució de projectes IT, de part del servei de resolució d'incidències i peticions ordinàries als usuaris, del manteniment i la gestió del canvi de tots els sistemes i equips corporatius, de la coordinació i seguiment dels contractes actius sobre aquests sistemes i equips, o de la participació en projectes liderats per d'altres unitats i departaments corporatius. La ciberseguretat corporativa requereix d'esforços continuats i no pot dependre només d'esforços puntuals que l'equip IT pugui dedicar en la seva planificació.

Per tant, es fa necessària la contractació d'un servei per a gestionar la seguretat corporativa – gestió conjunta amb els tècnics IT municipals, però liderada pel propi servei de SOC - que faci possible l'anàlisi continuat de l'estat actual de la seguretat corporativa, l'optimització d'aquesta seguretat, així com controlar les amenaces detectades pel SIEM. Per tant, aquest servei ha d'estar suportat per un equip que tingui la «expertise» del sistema SIEM corporatiu i el coneixement profund de la seva integració amb els sistemes i equips municipals.

Per tant, és igualment objecte principal d'aquest lot la contractació dels serveis de SOC (Centre d'Operacions de Seguretat), que implementi els serveis esmentats en el paràgraf anterior, i tots els serveis propis d'un SOC. Aquests serveis inclouen, per exemple, l'anàlisi, auditoria i assessorament en la seguretat corporativa i en els actius implicats; el desplegament i optimització de la solució SIEM amb tots els requeriments propis de l'eina especificats més endavant; el disseny, implementació i integració de la monitorització de la seguretat dels actius implicats en l'eina en el SIEM; el disseny, implementació i integració dels casos d'ús, correlacions i workbooks; l'adopció de l'explotació del XDR corporatiu com un actiu més; les tasques de vigilància continua sobre la seguretat corporativa, mitjançant l'equip humà que implementi el servei de SOC i mitjançant l'eina SIEM desplegada; el servei de supervisió i monitorització 24x7 d'alertes del SIEM; l'execució d'operatives acordades (tiqueting i escalat), com poden ser tasques preventives, de detecció i de resposta; els automatismes que puguin ser integrats i oportuns per millorar la pro-activitat d'aquesta vigilància; la creació d'informes i propostes de millora en quan a la seguretat de forma regular; evolució, creació i millora constant dels workbooks a implementar; el servei de resposta completa a un ciberincident greu/disruptiu en les condicions establertes més avall, el servei d'auditories i tests de seguretat, que sempre aportaran conclusions i indicacions per

implementar les mesures correctives que se'n derivin de les seves conclusions; i, en general, totes aquells serveis propis d'un servei de SOC que es considerin adients i que el licitador ofereixi, més enllà dels esmentats i els requerits en l'apartat específic de servei SOC.

Què entenem per «cas d'ús» i per «workbook»:

- Un «cas d'ús» es defineix com allò que l'organització considera – de forma prèviament pactada amb el SOC - un «positiu» referent a ciberseguretat.
    - Exemple de cas d'ús: «es detecta múltiples intents fallits d'inici de sessió en un sistema crític»
    - Exemple de cas d'ús: «el XDR corporatiu detecta una alerta en un EndPoint»
- Definim «workbook» (o també anomenat «runbook») com un procediment per mitigar i donar resposta a un cas d'ús concret.

  Un exemple d'un workbook podria ser aquest:
    - Pas 1. Automàticament el SIEM detecta el positiu d'un cas d'ús pactat amb el client, i reporta una alerta pels mecanismes establers amb el SOC.
    - Pas 2. L'operador del SOC obra la fitxa del workbook, i determina/analitza l'incident.
    - Pas 3. Si escau, l'operador disposa d'un procés de reacció establert en el workbook (aquesta reacció pot ser automatitzada o manual).

Tots aquests serveis són crucials per protegir la infraestructura de tecnologia de la informació i les dades sensibles de l'ajuntament.

Clàusula 2. Desplegament, manteniment, gestió i administració d'una solució de SIEM

L'Ajuntament de Gavà te la necessitat d'implementació d'un nou SIEM com a pla estratègic de seguretat corporativa.

Els licitadors a la memòria tècnica a presentar en el sobre B i que serà objecte d'avaluació mitjançant judicis de valor, hauran d'optar per implementar qualsevol de les propostes, que s'indiquen a continuació, que hauran de complir els següents requeriments:

<u>CAS 1. SI EL LICITADOR PROPOSA UNA SOLUCIÓ SIEM BASADA EN SW COMERCIAL</u>

Aquesta solució comercial haurà de complir els següents requeriments específics:

- L'eina SIEM comercial ha de ser líder en el mercat degut a la criticitat de la seguretat corporativa:
    - Líder en l'últim quadrant de Gartner de SIEM disponible.
    - Líder en l'últim quadrant de Gartner en eines d'observabilitat (2023).

- Líder en els últims 5 quadrants de Gartner de SIEM.

- L'eina SIEM comercial haurà de servir-se en modalitat SaaS, optimitzant així el suport, actualitzacions i manteniment, facilitat la implementació i escalabilitat.
- El *tennant* SaaS i el llicenciament ha de ser propietat de l'Ajuntament de Gavà, garantint així la independència entre serveis de Partners i l'eina SIEM , permeten així donar continuïtat a totes les tasques evolutives i casos d´us implementats sense cap tipus de migració a noves plataformes SIEM.
- L'eina SIEM comercial ha d'estar catalogada com a Qualificada en ENS nivell ALT dins del Catàleg de seguretat de les TIC del CCN CERT (aprovat pel Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica)
- L'eina SIEM SaaS comercial ha d'estar llicenciada amb capacitat d'ingesta mínima de 20GB/dia de Logs
- La plataforma es lliurarà en mode servei CLOUD SaaS nadiu on el fabricant de la solució assumeix la totalitat del servei.
- El *tennant cloud* proporcionat pel servei de SIEM, serà dedicat exclusivament per a l'Ajuntament de Gavà, i es lliurarà directament per part del fabricant, on la propietat i la titularitat serà de l'Ajuntament.
- La plataforma tindrà replicació de les dades per tal de garantir la disponibilitat de les mateixes.
- El servei SaaS haurà de donar-se amb un acord de nivell de servei o SLA del 100% de disponibilitat.
- La solució SaaS disposarà d'un servei de còpia de seguretat de la configuració i les dades més enllà de la replicació.
- Implementi Schema on read per a les dades ingestades.
- Capacitat d'ingestar dades de xarxa mitjançant una sonda, que permeti extreure dades de més de 25 protocols de xarxa: IP, TCP, UDP, ICMP, HTTP, DNS, etc.
- Compti amb un market o repositori amb més de 2000 connectors ja fabricats i disponibles per facilitar la normalització i càrrega de les dades a la futura plataforma SIEM de l'Ajuntament de Gavà.
- Catàleg de casos d'ús de ciberseguretat amb més de 1000 regles predeterminades disponibles per a la seva implementació.
- Que els connectors disponibles al market tinguin suport directe dels fabricants tercers de les solucions a connectar o pel propi fabricant de la solució de SIEM.
- Disposi ja implementats almenys 20 algorismes de Matching Learning mantinguts pel propi fabricant.
- El servei proporciona capacitats de xifratge en trànsit i xifratge opcional en repòs.

CAS 2. SI EL LICITADOR PROPOSA UNA SOLUCIÓ SIEM BASADA EN SW DE CODI OBERT I LLIURE

Aquesta solució basada en «open source» haurà de complir els següents requeriments específics:

- Anàlisi i indexació de registres universals (ULPI).
- Realitzar l'inventari automatitzat del sistema.
- Generar alertes de compliment normatiu.
- Detecció de vulnerabilitats sense necessitat de llicències addicionals.
- Capacitat de supervisió de trucades al sistema.
- Capacitat de monitorització i generació d'alertes sobre la integritat dels fitxers a temps real.
- Integració amb el servei al núvol VirusTotal.
- Suport 8x5 del desenvolupador.
- Compti amb un conjunt de regles pre-definides que apliquin a tecnologies de forma transversal, com per exemple: Postfix, Nginx, Apache, MySQL, entre d'altres.
- Seguiment del compliment: Suport al compliment dels requisits reglamentaris alineant les alertes amb marcs de compliment com ara PCI DSS, GDPR i NIST, proporcionant una pista d'auditoria clara per a la verificació del compliment.
- Taulers de control personalitzables: ha d'incloure eines que permeten als usuaris crear i personalitzar taulers de control adaptats a les seves necessitats operatives. Aquesta personalització s'estén a la visualització de dades tals com els intents de connexió SSH amb informació geogràfica detallada o la monitorització de les activitats de la base de dades i dels dispositius de xarxa.

Per a qualsevol de les dues opcions presentades (solució comercial o solució basada en open source) l'eina SIEM ha de complir TOTS els següents requeriments, característiques, capacitats i funcionalitats base generals especificats a continuació i fins el final d'aquest apartat «*Desplegament, manteniment, gestió i administració d'una solució de SIEM*»:

Que el fabricant/desenvolupador de la solució SIEM proposta tingui reconeguts i registrats un mínim de 10 partners a l'estat espanyol. Es demanarà acreditar amb un document, certificat o link a la web del fabricant/desenvolupador que acrediti aquests mínims partners.

Que la solució SIEM proposta ofereixi de forma nativa una eina que permeti mapejar directament alertes de ciberseguretat amb el compliment del framework de ciberseguretat MITRE ATT&CK.

Ha de permetre una anàlisi de la situació a múltiples ubicacions des d'un punt de vista unificat que facilita la detecció de tendències i patrons no habituals.

A més, la solució SIEM desplegada ha de combinar les següents funcions i requeriments:

- Sistema de gestió d'informació de seguretat
- Encarregat de l'emmagatzematge a llarg termini de la informació de seguretat. Gestió

de les obligacions legals de custòdia d'evidències.

- Anàlisi i comunicació de les dades de seguretat. Ha de permetre/facilitar la comunicació d'incidents en els terminis establerts.
- Gestió d'esdeveniments de seguretat.
- Encarregat de la monitorització en temps real dels esdeveniment de seguretat.
- Correlació d'esdeveniments en temps real.
- Notificacions i quadres de comandament de la informació de seguretat significativa.
- Ha de permetre la automatització de respostes davant esdeveniments, per protegir de forma automàtica els sistemes IT de les amenaces detectades (automatitzacions mitjançant integració directe de SIEM i els sistemes corporatius, o mitjançant eines d'orquestració tipus SOAR).

A més, la solució SIEM desplegada ha de permetre integracions tecnològiques ràpides, oferint múltiples integracions i casos d'ús preconfigurats (natives o via syslog) per a dispositius físics i virtuals, amb recol·lecció centralitzada de traces d'auditoria dels diferents sistemes, com per exemple els següents:

- *<text complet disponible a la versió confidencial>*

Es valorarà que la mateixa eina doni funcionalitats de visibilitat sobre el rendiment dels sistemes i serveis corporatius.

Es valorarà que la mateixa eina doni funcionalitats d'anàlisi de vulnerabilitats dels sistemes i serveis corporatius sense que calgui llicenciament de tercers. Es valorarà que el projecte de desplegament inclogui el desplegament d'aquesta funcionalitat.

Si no es dona la característica anterior, també es valorarà que l'eina pugui integrar-se amb solucions de anàlisi de vulnerabilitats de tercers, com per exemple OpenVAS o NESSUS, entre d'altres. Anàlogament al cas anterior, es valorarà que el projecte de desplegament inclogui el desplegament d'aquesta integració i/o es valorarà que la oferta inclogui el llicenciament d'aquesta solució de tercers, en cas que es requereixi llicenciament.

Es valorarà que l'eina permeti, i el projecte inclogui, la integració de la solució SIEM proposada amb les eines pròpies del Centre Criptològic Nacional per a la gestió de la seguretat (microCLAUDIA, LUCIA, etc) i/o amb els sistemes de informació de la xarxa nacional de SOCs.

A més, de tot l'anterior, la eina SIEM proposada ha de tenir aquestes característiques de la seva arquitectura:

- Arquitectura escalable sense límits d'escalat.
- La plataforma ha de ser capaç i estar dimensionada per processar un mínim de 20 Gb d'ingesta al dia sense estar limitada a un màxim d'esdeveniments per segon o eps.
- La plataforma disposarà de capacitats de recopilació de dades segures i d'alt rendiment per a dispositius *NIX (incloent-hi AIX, Solaris i z/linux), MacOS i Windows.

Aquests agents seran molt lleugers i utilitzaran els recursos mínims (<2% sobre el rendiment del servidor).

A més, de tot l'anterior, la eina SIEM proposada ha de tenir aquestes capacitats i funcionalitats base:

- L'eina haurà de garantir la retenció dels logs en temps real («en calent») dels darrers 90 dies.
- En el cas que l'eina proposada sigui OnPrem, l'eina haurà de garantir la gestió de l'històric de Logs dels darrers 2 anys.
- Altrament, si l'eina proposada és al Cloud, l'eina haurà de garantir, al menys, la gestió de l'històric d'incidents dels darrers 2 anys.
- Capacitat d'ingerir qualsevol dada basada en text, preservar l'esdeveniment original amb total integritat i proporcionar un esquema de dades flexible per a una extracció fàcil de camps en temps de cerca.
- Capacitat d'admetre la ingesta de dades mitjançant agent o agentless. suportant les tècniques més comunes de recol·lecció de dades sense agent incloent: TCP, UDP, WMI, recursos compartits de fitxers de xarxa, JDBC, ODBC, JMS, SNMP, captures de trànsit de xarxa, APIs, FIFO o dades provinents de scripts personalitzats.
- Funcionalitat de normalització de la dada basada en un format estàndard, no propietari.
- Proporcioni un model de dades comú com a estàndard de normalització que faciliti a l'anàlisi de les dades.
- No depengui de connectors personalitzats subministrats per tercers per ingerir dades de diferents fonts.
- Permeti la creació i extensió de la gamma de visualitzacions personalitzades (que no es limiti als informes fixos i preestablerts).
- Els informes i quadres de comandament de la plataforma incloguin capacitats de *drilldown* que permetin als usuaris aprofundir en la informació que la plataforma posa a la disposició mitjançant clics.
- Es valorarà que l'eina permeti casos d'ús més enllà de la ciberseguretat i del acompliment normatiu, que possibiliti la col·laboració entre serveis diferents als de la ciberseguretat o fins i tot serveis no IT, al permetre l'ús de la mateixa eina per a la gestió i control d'altres serveis o actius de la corporació, diferents als de la ciberseguretat.

A més, de tot l'anterior, la eina SIEM proposada ha de tenir les següents capacitats i funcionalitats específiques en seguretat:

- Proporcioni actualitzacions – si pot ser automàtiques - de contingut de seguretat lliurades directament per l'equip de recerca d'amenaces per ajudar a mantenir el servei al corrent de les amenaces noves i emergents.

- Ofereixi funcionalitats que ajudin en totes les fases de la pràctica de ciberseguretat:

- Monitorització de la postura de seguretat:
    - Analitzi en temps real el risc, alertes i compliance.
    - Monitorització continua i completa dels actius.
- Compliance:
    - Analitzi l'estat de compliment segons RGPD o CIS amb les dades recollides.
- Detecció d'Amenaces Avançades:
    - Detecti els sistemes i usuaris compromesos.
    - Determini les activitats associades amb usuaris i atacants.
    - Trobi indicadors i artefactes associats als sistemes compromesos.
- Investigació d'incidents i forense:
    - Visibilitat mitjançant una única plataforma d'anàlisi que ajudi a detectar i investigar ràpidament les possibles amenaces de seguretat reduint així els seus MTTD i MTTR.

Clàusula 3. Servei SOC

3.1 Requeriments del servei SOC

L'Ajuntament de Gavà te la necessitat d'un servei gestionat de SOC (Centre d'Operacions de Seguretat) que digui a terme les següents tasques i funcions, i amb els següents requeriments:

➢ En la **fase d'adopció del servei**, el SOC, com a mínim, ha d'executar les següents tasques i funcions:

- Anàlisi de l'estat de la ciberseguretat de l'Ajuntament de Gavà.
- Anàlisi pràctic (empíric i real) dels vectors seguretat crítics.
- Anàlisis de l'estat d'infecció i seguretat, mitjançant validació i anàlisis de connexions externes (C&C, malware, bots,....). Es desplegaran eines per tal d'analitzar l'estat de la corporació cap i des de internet, i el risc digital de l'Ajuntament de Gavà.
- Anàlisis de fonts d'identitat de l'Ajuntament: privilegis, permisos i activitats, mitjançant eines especialitzades per a identificar aspectes com: Shadow Admin Threat, Política de contrasenyes, Configuració errònia, Abús de Privilegis, Emmagatzematge de credencials no segures, Amenaces d'ús de comptes locals, etc.
- Anàlisis i definició de proposta de millora dels sistemes de BackUp i proposta de quina seria la arquitectura adient per poder suportar un DRS en Cloud.

➢ En la **fase d'integració al servei (onboarding),** el servei ha de preveure, com a mínim,

aquestes tasques i funcions:

- Direcció de projecte
- Desplegament i implementació de l'eina SIEM, dels Forwarders, Instal·lació d'agents, desplegament de configuracions tipus Syslog en els equips que així ho requereixin (o, com mínim, suport a la configuració de sistemes syslog que requereixin la instal·lació d'enes de tercers, com podrien ser pluguins, redirecció de logs, entre d'altres)
- Configuració d'ingesta de les fons (mínim de 20 GB/dia de logs)
- Identificació, creació i configuració d'un mínim de 15 WorkBooks crítics de forma inicial, personalitzats i adaptats sobre els serveis crítics existents a l'Ajuntament de Gavà, així com pla d'evolució sobre els mateixos.
    - La implementació d'aquests durant els primers 3 mesos del contracte.
- Definició i implementació de metodologia de priorització de casos d'ús.
- Optimització de la plataforma SIEM:
    - Configuració de correlacions i casos d'ús per a la detecció.
    - Confecció d'informes i Dashboards de visibilitat i seguretat seguretat.
    - Confecció de Dashboard normatiu basat en estat de compliment de l'ENS.
- Definició de processos personalitats per la anàlisis.
- Confecció o validació de respostes automàtiques i procediments.
- Incorporació al servei de SOC de la gestió i la explotació de la solució XDR de seguretat de l'EndPoint (*<text complet disponible a la versió confidencial>*) ja desplegada i en explotació a la corporació, a banda de la seva òbvia integració amb el SIEM. El servei de SOC haurà d'operar sobre el XDR corporatiu els canvis necessaris de reconfiguració que sorgeixin de necessitats de operació del SOC o projectes IT corporatius: configuració d'excepcions, perfils específics per grups de màquines o màquines concretes, analítiques, automatització, optimització, revisió i gestió de polítiques, tunning, suport i gestions pròpies del servei de SOC referents a l'explotació del XDR en general, etc.
- Es valorarà com a millora el desplegament de Honeypots, incloent la seva gestió i la seva integració amb la solució SIEM.
- Com s'ha esmentat en la secció «Desplegament, manteniment, gestió i administració d'una solució de SIEM» d'aquest mateix Lot 2, es valorarà que el projecte presentat tingui previst que es configuri i posi en explotació la funcionalitats d'anàlisi de vulnerabilitats dels sistemes i serveis corporatius que incorpori la mateixa solució SIEM o, si l'eina no inclou tal funcionalitat, que el projecte tingui previst la integració de l'eina SIEM amb solucions de anàlisi de vulnerabilitats de tercers, com per exemple OpenVAS o NESSUS, entre d'altres.
- Com s'ha esmentat en la secció «Desplegament, manteniment, gestió i administració d'una solució de SIEM» d'aquest mateix Lot 2, es valorarà que projecte tingui prevista la integració de la solució SIEM proposada amb les eines pròpies del Centre Criptològic Nacional per a la gestió de la seguretat (microCLAUDIA, LUCIA, etc) i/o amb els sistemes de informació de la xarxa nacional de SOCs.

➢ En la **fase d'explotació continuada (ongoing),** el servei ha de preveure, com a mínim, aquestes tasques i funcions:

- Direcció del servei mitjançant Service Manager (punt únic d'interlocució)
- Creació i generació d'informes mensuals de seguretat i de servei.
- Sessió semestral de propostes d'evolució i millora.
- Servei de supervisió i monitorització 24x7 d'alertes del SIEM segons els casos d'ús definits, incloent de validació de l'alerta i recopilació d'informació. Execució d'operatives acordades (tiqueting i escalat):

    - Tasques preventives: gestió de quadres de comandament i KPIs de Seguretat.
    - Tasques de Detecció: gestió del SIEM, monitorització 24x7, gestió Logs i casos d'us, compliment normatiu.
    - Tasques de Resposta: gestió de alertes i coordinació d'incidents amb 3ers.
    - Eines: Gestió, operació i manteniment del SIEM.

- Es valorarà si el servei inclou també tasques de cacera d'atacs complexos (*Thread Hunting*).
- Evolució i millora dels WorkBooks definits durant el servei.
- Creació de nous WorkBooks fins a un màxim de 30 a l'any segons necessitats i ecosistema (fonts d'ingesta, atacs detectats, vulnerabilitats...).
- Servei de resposta davant d'incidents:

    - El servei inclourà la resposta davant un ciberincident de qualssevol actiu monitoritzat pel servei de SIEM/SOC considerat de baixa o mitja gravetat i/o que no afecti a dades personals municipals i/o que no afecti al desenvolupament del treball habitual dels serveis i personal corporatius. Aquesta resposta de baixa granularitat podrà consistir en:
        - Alertes (supervisió i atenció)
        - Adopció polítiques o configuracions de seguretat adients.
        - Implementació de les mesures de contenció o correcció necessàries.
        - Comunicació de l'incident.
        - Suggeriments d'actuació per part de IT
    - La oferta també ha d'incloure inclou 1 resposta anual davant un ciberincident greu/disruptiu durant la durada del contracte, en totes les seves fases. En aquest sentit:
        - La gravetat del ciberincident i/o la seva afectació a dades personals gestionades per l'ajuntament i/o la seva afectació al desenvolupament del treball habitual dels serveis i personal corporatius, i sempre per decisió consensuada entre l'adjudicatari i el responsable de ciberseguretat de l'ajuntament de Gavà, determinarà la utilització

d'aquest servei de resposta davant un ciberincident considerat greu/disruptiu.

- Si no s'utilitza el servei en un període anual, la utilització del servei de resposta anual davant un ciberincident greu/disruptiu queda acumulat per al següent període anual dins el contracte.
- La resposta a un ciberincident d'aquestes característiques podrà requerir la actuació «in situ», en cas que així es requereixi, en menys de 4 hores. Aquest procés de resposta haurà de preveure, com a mínim, les fases i accions següents, que s'ampliaran i/o es detallaran a la memòria tècnica:
    - Detecció
    - Contenció
    - Resolució
    - Investigació i anàlisi forense
    - i totes les que l'adjudicatari consideri necessàries a banda
- **A banda d'aquest serveis de resposta ja inclosos en oferta, en els criteris automàtics de valoració d'aquest lot, els licitadors hauran d'oferir el cost econòmic que tindria la resposta addicional a un ciberincident greu/disruptiu**, per preveure el cas que s'hagi consumit l'actuació anual prevista i inclosa en el contracte, i es necessités la contractació d'un segon, tercer... servei de resposta davant d'un nou ciberincident greu/disruptiu dins el mateix període anual.

  El preu ofertat, no ha de tenir cap tipus de limitació, ni en tipus de perfil que atendria el ciberincident greu/disruptiu addicional, ni tampoc limitacions de desplaçament ni d'horaris (laborables, caps de setmana i fora d'horari laboral). Els ciberincidents d'aquestes característiques poden deixar incomunicades les seus i/o serveis en qualsevol moment i dia."

3.2 Servei específics d'auditories i tests de seguretat pròpies del servei SOC

Es requereix que l'empresa contractista del servei de Ciberseguretat (SIEM i SOC) efectuï unes mínimes auditories de seguretat (algunes d'elles necessàries fins i tot per a les primeres fases del projecte:

Tipus d'auditoria o test de seguretat	Quantitat o freqüència mínima requerida
Auditories del Directori Actiu	1 en la fase d'adopció del projecte
Auditories del firewalling	1 durant el primer any del servei d'explotació
Auditories de segmentació de xarxa i comunicacions	1 durant el primer any del servei d'explotació
Auditories de seguretat en l'eina de correu electrònic i de l'eina de seguretat	1 durant el primer any del servei d'explotació

perimetral del correu electrònic	
Auditories de vulnerabilitats	Freqüència anual durant la durada del contracte
Pentest intern	Freqüència anual durant la durada del contracte
Pentest extern	Freqüència anual durant la durada del contracte

Taula 1. Auditories/test de seguretat

A banda d'aquestes tipologies i quantitats d'auditories requerides, el licitador podrà incloure en la seva oferta una quantitat superior de les esmentades auditories o d'altres tipus d'auditories o accions no esmentades en aquests llistat de mínims que, al seu criteri, siguin necessàries/adequades/recomanables per el bon desenvolupament de tot el projecte de desplegadament del SIEM i/o pel correcte funcionament del servei de SOC i/o per a la millora de la ciberseguretat corporativa en general.

En general, per a tots els tests i auditories de seguretat, tant per a les obligatòries com per a les opcionals que s'ofereixin, i una vegada efectuades aquestes auditories i tests de seguretat, l'adjudicatari haurà de generar un informe executiu i un informe complet.

En general, per a tots els tests i auditories de seguretat, tant per a les obligatòries com per a les opcionals que s'ofereixin, i una vegada efectuades aquestes auditories i tests de seguretat, l'adjudicatari haurà de documentar – en algun d'aquests informes - les accions correctives sobre els elements i sistemes analitzats, sempre i quan aquestes actuacions puguin ser implementades amb els hardware i software de xarxa i seguretat contractats i gestionats pel licitador, amb l'objectiu de resoldre els problemes de seguretat diagnosticats en aquestes proves. Si els resultats d'aquests test fessin palesa la necessitat de noves adquisicions de hw o sw addicional, o de la contractació de nous serveis, no inclosos en aquesta licitació, l'adjudicatari no tindrà l'obligació d'aportar aquestes solucions addicionals, però sí haurà d'incloure's, en l'informe de resultats dels tests de seguretat, el diagnòstic detectat i una relació de possibles solucions de mercat al problema detectat, a efectes d'assessorament tecnològic.

Tots els processos d'aquests tests de seguretat es realitzaran amb la supervisió i control del procés per part d'un Consultor especialista en Seguretat IT.

Pel que fa a les auditories obligatòries esmentades a la *Taula 1. Auditories/test de seguretat*, es valorarà la metodologia de les mateixes i les característiques de la documentació generada. Per a aquestes auditories obligatòries esmentades, també es valorarà si la oferta inclou millores respecte a les quantitats mínimes requerides de cada auditoria en aquesta taula, i la idoneïtat o justificació d'aquesta millora.

Pel que fa a les auditories, test o accions addicionals que el licitador inclogui a la seva oferta (com podrien ser, per exemple, campanyes de fishing ètic, hacking de PC local, auditories i/o hacking del servei WiFi, accions o recursos per fomentar la sensibilització en ciberseguretat del personal corporatiu, o qualsevol altre que el licitador consideri apropiades), es valorarà tant la metodologia d'aquestes accions, les característiques de la documentació generada, la quantitat d'aquestes accions, i la idoneïtat o justificació d'aquesta millora.

Clàusula 4. Coordinació del servei

L'adjudicatari nomenarà una persona de contacte que serà el coordinador de tots els assumptes relacionats amb la gestió i manteniment de la solució SIEM i la coordinació dels serveis de SOC.

Aquesta persona haurà de tenir una visió global i integradora del nostre escenari tecnològic i de les necessitats que poden derivar-se del servei de SIEM i SOC, així com disposar de capacitat tècnica suficient i elevats coneixements de la solució SIEM i serveis SOC a gestionar. És amb aquesta persona amb la que es faran les reunions periòdiques de seguiment dels serveis, per proposar millores i resoldre els possibles conflictes.

Haurà d'estar sempre localitzable telefònicament (o comunicar expressament en cas de indisponiblitat, la persona que el substituirà), no per resoldre incidències que es farà a través de les vies de contacte normal, sinó per resoldre casos excepcionals d'atenció no satisfactòria.

La idoneïtat de la persona designada per l'empresa contractista com a coordinador/a («service manager») serà lliurement apreciada pel responsable del contracte que es designi per part de l'Ajuntament de Gavà, podent exigir en tot moment al contractista la seva substitució en ares a una bona execució del contracte.

Dins la coordinació del servei, està implícita la coordinació amb els fabricants als que l'adjudicatari contracti els manteniments i llicenciaments dels diferents elements administrats i gestionats, per tal de notificar avaries i, així, es procedeixi a la seva reparació o canvi en la major brevetat.

Clàusula 5. Nivell de servei i horaris

Els sistemes d'informació corporatius estan funcionant 24 hores donant serveis a la ciutadania, amb el que, per aquest condicionant, com també per la pròpia naturalesa de la gestió de la ciberseguretat, el servei ha de contemplar mecanismes de cibervigilància en 24x7. Per això, el servei de supervisió i monitorització d'alertes del SIEM, incloent la validació de l'alerta, la recopilació d'informació i la resposta necessària ha de ser un servei en 24x7.
Pel que fa al manteniment, administració i gestió del canvi de l'eina SIEM, el licitador proposarà un SLA que es valorarà a la fase de puntuació de la proposta.
Pel que fa al servei de SOC, com ja s'ha esmentat en els requeriments del servei SOC, la resposta d'avant d'incident que es consideri com a «greu/disruptiu» de forma consensuada, haurà de ser "in situ" en cas necessari, en menys de 4 hores, i en 24x7. Pel que fa a la resta de tasques d'anàlisi, de respostes automatitzades o manuals, pròpia del servei de SOC, l'adjudicatari haurà de complir amb el mateix SLA de 24x7x4, en remot sempre que sigui possible o, «in situ» si fora imprescindible.
El personal que assisteixi a les actuacions «in situ» derivades del servei, ha de tenir alguna de les capacitacions tècniques establertes per al personal prestador del servei, i sempre ha de ser personal propi de l'adjudicatari.

Clàusula 6. Devolució del servei

Durant l'últim mes previ a la finalització del contracte, en cas que l'empresa contractista que executa el contracte no resulti adjudicatària del nou servei, aquesta haurà de lliurar sota la supervisió de l'Ajuntament de Gavà, totes les dades administratives y tecnològiques que siguin necessàries a l'ajuntament per donar continuïtat a l'administració, gestió i manteniment de tota la solució SIEM desplegada**.**

Com exemple d'aquestes informacions:

- Contractes de manteniment amb els fabricants.
- Accés a les plataformes de descàrrega de softwares dels fabricants d'elements gestionats.
- Inventaris d'actius implicats en el la plataforma SIEM gestionada, que inclogui, entre d'altres informacions, el mètode d'accés, les credencials d'accés, certificats i credencials de certificats involucrats i , en general, qualsevol altra informació que es consideri rellevant per a poder donar continuïtat a la seva gestió i administració per part de l'ajuntament.
- Còpia de seguretat de la darrera configuració estable de tots els elements configurables de la solució SIEM desplegada.
- En general, totes les dades i informacions que tinguin relació amb el conjunt sistemes i programaris administrats i gestionats de la solució SIEM, i dels components addicionals relacionats en el contracte sortint, i que puguin ser necessaris en un futur al personal tècnic de l'ajuntament.

Clàusula 7. Memòria tècnica LOT 2

Els licitadors hauran de presentar en el SOBRE B per a la seva avaluació mitjançant judicis de valor, **una memòria tècnica, amb d'un màxim de 45 planes (Arial 11 interlineat senzill) sense comptar l'apartat d'Annexes, portada i índex,** amb el detall i contingut mínim següent:

1. Arquitectura de la solució SIEM proposada

1.1. Descripció i presentació de l'arquitectura, funcionalitats i prestacions de l'eina proposada

NOTA IMPORTANT:

- *Dins aquest apartat, caldrà quedar palès si la solució proposada es basa en software comercial o en programari lliure. S'haurà de fer explícit el nom del fabricant o del codi obert lliure de la solució, versions, etc., per suposat, a banda de la resta d'informació sobre l'arquitectura, funcionalitats i prestacions de l'eina proposada.*

1.2 Dimensionat i tipologia dels recursos hardware i/o software corporatius «on premise» que aquesta arquitectura i el projecte requerirà de l'ajuntament de Gavà.

NOTA IMPORTANT:

- *Si s'opta per solucions «On premise», cal especificar en aquest apartat quins recursos hardware i software proporciona la oferta, i quins es requerirà que siguin aportats per la corporació.*
- *Si s'opta per aquestes solucions al Cloud, la corporació no posarà cap recurs al Cloud (ni SaaS, ni IaaS, ni Paas). Aquests recursos de Cloud hauran de ser íntegrament dotades pel proveïdor, i el tennant cloud proporcionat serà dedicat exclusivament per a l'Ajuntament de Gavà, i es lliurarà directament per part del fabricant, on la propietat i la titularitat serà de l'Ajuntament. Tots els costos d'aquests serveis al Cloud han d'estar inclosos en l'oferta econòmica. L'ajuntament de Gavà no haurà de fer-se càrrec de cap cost econòmic més enllà dels derivats d'aquesta licitació durant tota la durada del contracte.*

1.3 Anàlisi vulnerabilitats dels sistemes i serveis corporatius

NOTA IMPORTANT:

Caldrà incorporar un subapartatat on s'exposi tant si la solució SIEM preveu aquesta funcionalitat de forma nativa sense que calgui llicenciament de tercers, com si la solució té la possibilitat d'integrar-se amb eines de tercers com OpenVAS o NESSUS, entre d'altres. Altrament, no caldrà incorporar aquest subapartatat.

1.4 Possibilitat d'explotació de la mateixa eina per a gestió d'altres serveis o actius diferents als de la ciberseguretat

NOTA IMPORTANT:

Només caldrà incorporar aquest subapartat descriptiu en el cas l'eina proposada permeti casos d'ús més enllà de la ciberseguretat/acompliment normatiu, que possibiliti l'aprofitament de la mateixa eina per a la gestió d'altres serveis o actius de la corporació, diferents als de la ciberseguretat.

2. Metodologia de desplegament de la solució SIEM

NOTA IMPORTANT:

Caldrà en aquest apartat descriure la metodologia d'implantació de la solució proposada, incloent la informació referent a la implantació dels casos d'ús, dels workbooks, de la optimització de la plataforma, de generació d'informes i dashboards, i tots els aspectes de projecte i metodologia que es cregui necessari, sempre de forma general, sense entrar encara en casos d'ús o workbooks concrets, que s'abordaran en un altra apartat.

3. Avant-projecte de classificació i priorització d'actius, i d'avant-proposta ende quins seran els actius que s'incorporaran a l'eina SIEM

NOTA IMPORTANT:

Els actius IT corporatius (equips i sistemes) amb els que treballa la corporació estan comptabilitzats i categoritzats a grans trets en l'annex «Annex III. Actius candidats a integrar

en la cibervigilància». Aquests actius poden ser candidats, a criteri del licitador, a ser incorporats o no en el projecte d'integració per a la seva cibervigilància mitjançant l'eina SIEM i la seva supervisió en el servei de SOC. En aquest apartat de la memòria tècnica, per tant, serà obligatori incloure un especificació - a mode d'avant-proposta – que inclourà ***tres informacions, com a mínim****, relacionades amb els esmentats actius:*

- *Classificació a criteri del licitador de tots els esmentats actius de l'annex en crítics, primaris, secundaris o d'altres no candidats.*
- *Selecció, a criteri del licitador, de quins seran els actius que la oferta del licitador preveu incorporar en el projecte de integració amb el SIEM, i quins actius quedaran fora de l'abast del projecte. Poden identificar-se per la categoria assignada, o de forma individual, com el licitador consideri.*

  Ara bé, independentment de la classificació i selecció que el licitador faci, el requisit mínim serà que el projecte inclogui, com a mínim, la integració en el SIEM de tots els elements de seguretat perimetral, de seguretat de l'EndPoint, del directori actiu corporatiu, del correu electrònic, de l'eina de seguretat perimetral del correu electrònic, i dels serveis DNS en xarxa interna corporativa.

- *Quina serà la planificació en temps, dins els anys de contracte, amb els que el licitador preveu incorporar els elements seleccionats en el punt anterior.*

NOTA IMPORTANT:

S'entén que és una avant-projecte i que, pern tant, una vegada iniciada la fase d'adopció, podrà ser redefinit segons necessitats i condicionants concrets del projecte. Però es demana aquí un avant-projecte per poder valorar la correctesa i la viabilitat del projecte proposat, a priori, amb les dades publicades en aquest plec tècnic.

4. **Avant-projecte de workbooks**

NOTA IMPORTANT*:*

Serà obligatori incloure - a mode també d'avant-proposta – una especificació/previsió de quins podrien ser els mínims workbooks que es crearien i implementarien a la fase de «onboarding» del projecte, indicant la seva complexitat i tipologia, o si la proposta inclouria una quantitat superior als 15 mínims exigits en aquesta fase (i independentment dels que el projecte ja preveu en fases posteriors; el projecte preveu un mínim de 30 addicionals anuals ja en la posterior fase d'ongoing, que es definiran durant el contracte. Aquí valorem només els workbooks de la fase inicial).

5 Detecció de vulnerabilitats

Subapartat específic que especifiqui si el projecte de desplegament preveu les tasques de desplegament de les funcionalitats pròpies de detecció de vulnerabilitats; o bé si el projecte preveu les tasques d'integració amb eines de detecció de vulnerabilitats de tercers com per exemple OpenVAS o NESSUS, i/o si la proposta inclou els llicenciaments d'aquestes eines de tercers.

6. Metodologia, funcions i serveis inclosos en el servei de SOC

6.1 Metodologia de la gestió, la coordinació i el seguiment del servei

6.2 Servei de gestió, operació i manteniment de la solució SIEM

NOTA IMPORTANT:

Tant en el cas d'una eina comercial, com en el d'una eina Open Source, es requereix que hi hagi un contracte de suport i manteniment professional amb el fabricant, que també caldrà descriure en aquest apartat, a banda de la descripció dels serveis propis de gestió, operació i manteniment oferts pel licitador com a partner de la solució.

6.3 Metodologia de servei de supervisió i monitorització 24x7 d'alertes del SIEM segons els casos d'ús definit, incloent validació de l'alerta i la recopilació d'informació, i d'altres serveis propis

6.4 Metodologia en execució d'operatives/tasques preventives, de detecció, de resposta, i d'altres tipus rellevants

6.5 Proposta i metodologia de respostes automatitzades davant incidents de seguretat, i d'altres automatismes

6.6 Metodologia de resposta davant un ciberincident greu/disruptiu: detecció, contenció, resolució, investigació i anàlisi forense, i qualsevol altre fase o tasca involucrada

6.7 Proposta i metodologia de tasques de cacera d'atacs complexos, si aquest concepte s'inclou en l'oferta (apartat opcional, si el licitador la inclou en la proposta)

6.8 Proposta de desplegament de Honeypots, la seva gestió i la seva integració amb la solució SIEM (apartat opcional, si el licitador la inclou en la proposta)

6.9 Proposta d'integració de la solució SIEM proposada amb les eines pròpies del Centre Criptològic Nacional per a la gestió de la seguretat (microCLAUDIA, LUCIA, etc) i/o amb els sistemes de informació de la xarxa nacional de SOCs (apartat opcional, si el licitador la inclou en la proposta)

6.10 Auditories i test de seguretat obligatoris

NOTA IMPORTANT

Cal descriure la metodologia, les característiques de la documentació generada i, si el licitador millora/incrementa la quantitat o la freqüència en algun dels tipus d'accions obligatòries, la justificació/idoneïtat d'aquesta millora.

6.11 Auditories i test de seguretat no obligatoris

NOTA IMPORTANT

Cal descriure la tipologia, metodologia i quantitat de les accions addicionals a les obligatòries requerides a l'oferta, les característiques de la documentació generada per cada cas, així com la justificació/idoneïtat tant del tipus d'acció com de la quantitat prevista en l'oferta

7. Proposta de SLA per als serveis de manteniment, administració i gestió del canvi de l'eina SIEM

8. Annexes:

8.1 Document amb captures exemple de dashboards, informes, i qualsevol altre eina o document gràfic propi del servei SOC o de l'eina SIEM.

8.2 Enllaç a la web fabricant/desenvolupador o document del fabricant/desenvolupador on s'acrediti que es tenen reconeguts i registrats un mínim de 10 partners a l'estat espanyol per la solució/producte SIEM amb el que es presenta la oferta.

LOT 3. RENOVACIÓ DEL SISTEMA DE SEGURETAT XDR PER ALS END POINT

L'Ajuntament de Gavà, en una anterior contractació licitada a l'any 2020, va contractar – entre d'altres serveis – la posada en funcionament i els serveis associats a una nova solució de seguretat de l'End Point. Es pretenia superar les solucions de prevenció clàssiques (antivirus basat en signatures contra el malware conegut) per evolucionar cap a una protecció i prevenció eficaç contra atacs no coneguts i complexos, que assolissin els següents requeriments-objectius:

- Prevenció de «exploits», tant coneguts com desconeguts (Zero-Day).
- Prevenció de «malware», tant conegut com desconegut.
- Recull d'informació forense per a la seva anàlisi posterior.
- Capacitats de Detecció i Resposta integrades en el mateix agent.
- Reporting sobre les amenaces detectades.

Els requisits funcionals que havia de tenir la implementació d'aquest nivell de seguretat del punt final per a assolir aquests objectius, a grans trets, eren els següents:

- Prevenció de diversos mètodes contra el malware
- Intel·ligència sobre amenaces (a més de fonts d'informació de tercers, afegir un grau d'immunitat col·lectiva a tots els usuaris dels endpoints, xarxes i aplicacions al núvol).
- Anàlisi local mitjançant aprenentatge automàtic (anàlisi local amb ajuda de tecnologia de Machine Learning determinar si es pot executar l'arxiu, fins i tot abans de rebre un veredicte de la inspecció).
- Inspecció i anàlisi en Sandbox (a més de l'anàlisi local, l'agent podria enviar els arxius desconeguts al servei d'anàlisi, utilitzant tècniques d'anàlisi estàtic mitjançant aprenentatge automàtic, anàlisi dinàmic i anàlisi de hardware.
- Altres funcionalitats de prevenció:
    - Protecció exhaustiva de processos secundaris: per defecte, l'agent ha de poder detectar i prevenir els atacs basats en scripts i sense arxius gràcies a uns exhaustius controls preparats per utilitzar sobre l'obertura d'aplicacions legítimes, com a motors de script i shells d'ordres.
    - Protecció davant el ransomware basada en el comportament.
    - Escaneig amb accions automatitzades.
    - Polítiques de cancel·lació de permisos d'administrador.
    - Quarantena per malware.
    - Classificació de greyware.
    - Restriccions de l'execució (com per exemple, evitar l'execució d'un tipus de fitxer concret emmagatzemat en una unitat USB)
    - Bloqueig sobre dispositius USB (total, temporal d'alguns tipus de dispositius USB, parcial segons llista blanca de dispositius USB, etc).

- Prevenció de «exploits » de diversos mètodes (contenir el nombre limitat de tècniques -o, si ho prefereix, eines- que tot atac basat en «exploits» ha d'utilitzar per manipular una vulnerabilitat de programari):

    - Protecció prèvia enfront de «exploits»: prevenir les tècniques de generació de perfils de vulnerabilitat que fan servir els kits de «exploits» abans que llancin atacs.
    - Prevenció de «exploits» basada en tècniques: evitarà que apareguin vulnerabilitats conegudes, de dia zero i sense actualitzar bloquejant les tècniques d'explotació que utilitzen els atacants per manipular aplicacions.
    - Prevenció de «exploits» de nucli: previndrà els «exploits» que s'aprofiten de les vulnerabilitats de el nucli dels sistemes operatius per a crear processos amb privilegis escalats a nivell de sistema, i noves tècniques d'exploits que executen càrregues malicioses, com per exmple WannaCry, NotPetya, Ryuk, BitPaymer, o d'altres tipus Ransomware.

- Prevenció d'entorns Windows, Mac i Linux

En l'adjudicació, va resultar guanyadora la solució *<text complet disponible a la versió confidencial>*.

Clàusula 1. Descripció del servei

Donat el bon rendiment de la solució actualment desplegada als equips corporatius, *<text complet disponible a la versió confidencial>*, aquest lot només té com objecte la renovació per al període de 2 anys de 450 llicències de protecció XDR de l'End Point amb *<text complet disponible a la versió confidencial>*.

Actualment es disposa de 600 llicències, però només es vol renovar-ne 450. Es valorarà que hi hagi un increment en les llicències ofertes.

La gestió i explotació de l'eina serà duta a terme per l'adjudicatari del lot 2 i pel personal propi del departament IT de l'ajuntament. Per tant, l'objecte del contracte és només la renovació de les llicències amb el fabricant i, el suport amb el mateix, en la modalitat mínima de *<text complet disponible a la versió confidencial>*.

Ara bé, es valorarà que el licitador ofereixi algun servei addicional, que sempre haurà d'estar relacionat directament amb la gestió, administració, explotació, tunning, optimització, gestió del canvi, o serveis tipus SOC específic a l'esmentada eina XDR.

Clàusula 2. Memòria tècnica LOT 3

Els licitadors hauran de presentar en el SOBRE B per a la seva avaluació mitjançant judicis de valor, **una memòria tècnica, amb d'un màxim de 5 planes (Arial 11 interlineat senzill) sense comptar portada i índex,** amb el detall i contingut mínim següent:

1.Serveis de suport inclosos:

S'exposarà el nivell o programa del servei de suport amb el que el personal IT de

l'ajuntament de Gavà podrà obrir casos de suport sobre l'eina XDR amb el partner i/o amb el fabricant. Quin seria el tipus de nivell o programa de suport inclòs en la oferta, que ha de ser com a mínim de tipus *<text complet disponible a la versió confidencial>*. S'especificarà quins serà el horari d'atenció i els SLA oferts (temps de resposta, temps de resolució, etc.) en el cas del servei amb el partner així com quins en el cas que s'inclogui serveis directes amb el fabricant.

2. <u>Serveis addicionals inclosos</u>:

Descripció dels serveis que el licitador ofereix en la oferta, referents a gestió, administració, explotació, tunning, optimització, gestió del canvi, o serveis tipus SOC específic a l'esmentada eina XDR, o qualsevol altra relacionada amb aquest producte, i que vagin més enllà de la simple renovació per a 2 anys del llicenciament/manteniment dels eina XDR per als End Points amb el fabricant, que és el concepte mínim exigit en aquest lot.

ANNEXOS:

Annex I. Inventari de programaris i equips de seguretat i de comunicacions, condicions de manteniment, gestió i SLA *<text complet disponible a la versió confidencial>*

Annex II. Gràfic d'enllaços Ajuntament de Gavà*<text complet disponible a la versió confidencial>*

Annex III. Actius candidats a integrar en la cibervigilància*<text complet disponible a la versió confidencial>*

El coordinador de Sistemes, Infraestructures, Comunicacions
i Ciberseguretat de l'Ajuntament de Gavà